Policy 6	RISK MANAGEMENT

Record of policy development		
Version	**Date approved**	**Date for review**
3.1	December 2020	October 2022
3.0	October 2020	October 2022
2.2	May 2019	January 2021
1.2	October 2017	October 2020

Policy purpose: Coastlink actively works to identify and address potential risk, to ensure the safety of clients, staff and the organisation.

Policy: The governing body is committed to ensuring the organisation has effective risk management in place. The governing body has ultimate responsibility for safeguarding the organisation and its employees, clients and other clients, students, as well as the organisation's services, reputation and finances from unnecessary injury, loss or damage relating to the business and activities in which it is involved.

Risk management processes are designed in order to prevent injury or harm to individuals, to protect the assets and interests of the organisation and to limit the impact of any unavoidable risk.

Relevant Standards

NSW Disability Service Standards:

1. Rights
2. Participation & inclusion
3. Individual outcomes
4. Feedback & Complaints
5. Service Access
6. Service Management

NDIS Practice Standards:

1. Rights and Responsibilities
2. Provider Governance and Operational Management
3. Provision of Supports
4. Support Provision Environment
5. High Intensity Daily Personal Activities
6. Specialist Behaviour Support
7. Implementing Behaviour Support Plans
8. Early Childhood Supports
9. Specialised Support Coordination
10. Specialist Disability Accommodation

Aged Care Quality Standards	
1. Consumer dignity and choice 2. Ongoing assessment and planning with consumers 3. Personal care and clinical care 4. Services and supports for daily living	5. Organisation's service environment 6. Feedback and complaints 7. Human resources 8. Organisational governance

Related Legislation & References
Aged Care Act 1997 (Cth), Schedule 2 User Rights Principles 2014. Charter of Rights and Responsibilities – Home Care Aged Care Quality & Safety Commission Better Practice Guide to Complaints Handling in Aged Care Services (2013) Children and Young Persons (Care and Protection) Act 1998 Commonwealth Home Support Programme Guidelines Commonwealth Privacy Act 1988 National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018 National Disability Insurance Scheme (Quality Indicators) Guidelines 2018 National Disability Insurance Scheme Act 2013 National Disability Insurance Scheme Code of Conduct NDIS Quality and Safeguards Commission United Nations Convention on the Rights of Persons with Disabilities

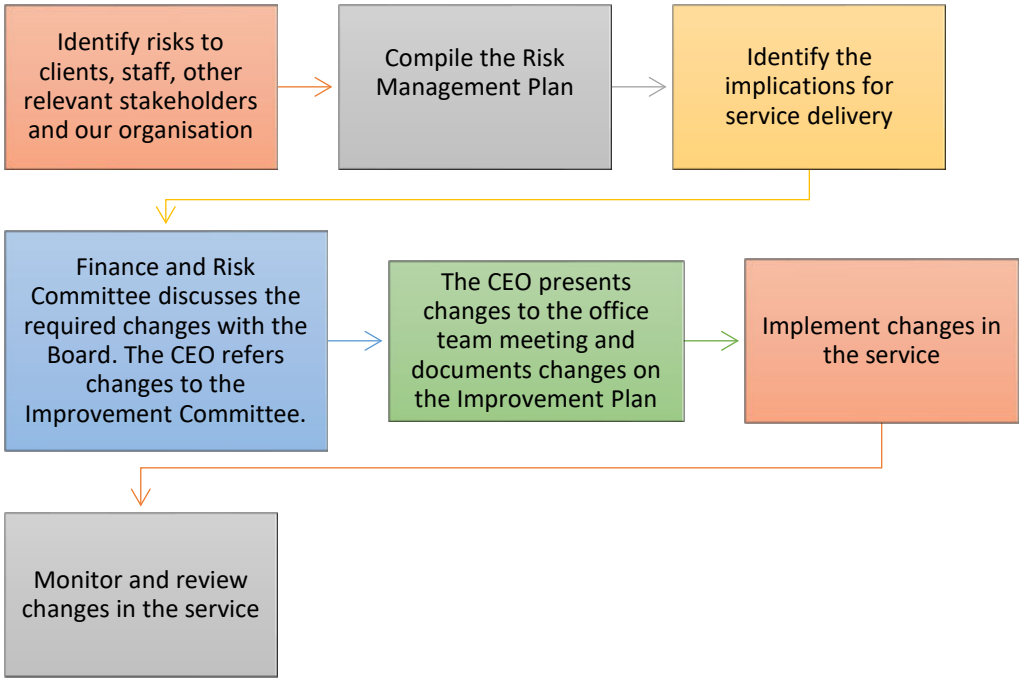
Related Procedures	
Documents/Forms	
Minutes of Meetings	Finance Risk and Audit Committee minutes held by CEO Other minutes held in Common Drive

Risk Management Plan	CEO, office personnel and Improvement Committee
Improvement Plan	CEO and Common Drive

Responsibilities and delegations	
This policy applies to: Clients Employees/volunteers	**It will be distributed through:** Client handbook, Coastlink website, Coastlink brochures Employee/volunteer handbook, common drive
Policy approval	Board

Definitions
Refer to Definitions list at front of Coastlink Policy and Procedure Manual

RISK MANAGEMENT PROCEDURE OVERVIEW



RISK MANAGEMENT GUIDELINES

6.1 Risk Management Overview

COASTLINK identifies and manages risks appropriate to our organisation, based on a simplified application of the AS/NZS 31000:2009 Risk Management Standards. Our risk management process is an ongoing process based on:

- Regular six monthly (or more often if required) reviews of previously identified risks (on risk management plan) to improve the strategies to minimise the risk and plans for responding to the risk if it occurs;
- Rolling internal audit of all risks, risk controls and risk outcomes (from incidents or trials);
- Rolling three-year external audit of all Corporate Risks as approved by the Board;
- The continuous identification of new risks and strategies to control the risks;
- Processes to ensure service continuity, such as the development of Business Continuity Plans at a corporate level, and Activity Continuity Plans as recommended by the Commonwealth Home Support Programme.[1]

The Board have endorsedthe following Risk Appetite Statement for guidance on all risk assessments and controls:

> *To deliver sustainable, high quality Disability and Aged Care services, to innovate, adapt and grow the Coastlink Board and Leadership accept that some level of risk is required. This statement outlines the risk appetite at Coastlink.*
>
> ***Seizing Growth Opportunities***
>
> *To take advantage of growth opportunities we understand and accept that a moderate level of risk is required to innovate, adapt and grow. We will explore and test opportunities aligned with our Key Focus Areas.*
>
> *The Board, together with Senior Leaders will rigorously analyse all relevant facts to understand, address and mitigate potential risks and inform decision-making.*
>
> ***Organisation Operations***

[1] Commonwealth Home Support – Programme Manual 2018

Coastlink has no risk tolerance regarding workplace safety, financial controls and probity, privacy of clients' personal information and quality of care.

Operational risks are monitored, addressed and mitigated through adopted organisational policy and regular reporting against the adopted organisational risk matrix.

6.1A Risk Management and Clients

All clients will be assessed for risks to their lifestyle, health, safety and wellbeing from the initial assessment and through the periods of time in which they receive COASTLINK services.

- Have a risk profile completed;
    - Coastlink's client risk profile contains specific questions relating to the managing risks associated with clients living alone and being supported by a sole support worker;
    - Where such a risk is identified, Policy 11 – Support Planning and Delivery maintains processes including service agreements, and internal processes for monitoring these individuals;
- Where risks are identified have a risk management plan developed;
- Management plans (including Health Plans and Support Plans) will be regularly reviewed by professionals (note: be aware of potential 6-8 month wait for professional behavioural clinicians and other allied health professionals);
    - Behaviour Support Plans and the management of restricted practices is managed through Policy 19 – Protection and Promotion of Huan Rights, which specifically deals with restrictive practices)
- COASTLINK is required to meet our work health and safety obligations to provide maximum safety for clients, staff and others;
- Work health and safety obligations are met in a manner that allows clients to take reasonable risks in their daily lives and without placing staff and others at risk of harm;
- Risks are identified, assessed, controlled and monitored to minimise risks to clients and staff as part of a risk management approach;
- Clients risk assessment and management are fundamental components of the individual planning process and the health care planning process;
- Clients Risk Profiles and Clients Risk Management Plans are incorporated into Individual Plans and are subject to regular review as part of the individual planning review process.

6.2 Risk Management and Continuous Improvement

Our organisation has integrated the risk management process into the continuous improvement process by:

- The Board delegating responsibility for risk management to the Finance, Risk and Audit Committee, an advisory Committee to the Board;
- Delegating operational responsibility for risk management operational review to the Continuous Improvement Committee (CIC);
- Including the identification and discussion of risks on the agenda for the CIC;
- Identifying risks and improvements by capturing incident, hazard and observation information in ProSIMS and reporting through the Work Health and Safety Committee or the CIC as appropriate;

- Including improvements to reduce or control risks through improvement processes and capturing these improvements in the Improvement Plan;
- Ensuring a risk approach is maintain in development of the Business Continuity Plan;
- Ensuring service continuity for clients as they transition from the younger to older age cohort.

6.3 Risk Management Plan

A Risk Management Plan is maintained and includes the following information:

- *The specific risk identified (risk source)*: these are the risks identified by the organisation;
- *What can go wrong (possible loss or adverse result):* details of what can go wrong in relation to the risk;
- *Consequence*: the consequence of the risk, using the risk rating matrix in 6.6 Risk Rating Matrix and below:
    - 1= Insignificant
    - 2= Minor
    - 3= Moderate
    - 4= Major
    - 5= Extreme

- *Likelihood*: the likelihood of the risk occurring using the risk rating matrix in 6.6 Risk Rating Matrix and below:
    - 5: Highly likely
    - 4: Likely
    - 3: Possible
    - 2: Highly unlikely
    - 1: Unlikely

Inherent and residual risk levels are calculated for both the likelihood and the consequence.

This allows effective risk controls to be identified and improves the understanding of risks in context with the controls in place.

- *Current controls to reduce risk*: the controls or strategies in place to control or reduce the risk;
- *Date reviewed:* Date the risk and controls were reviewed to identify improvements;
- *New controls:* Additional controls necessary to control or reduce risk or changes to existing controls.

6.4 Identifying Risks

In identifying risks, the Improvement Committee considers:

- Minutes from the WHS Committee;
- Staff and client feedback;
- Input from the annual planning day (see 1.14.2 Annual Planning Day);
- Staff Accident Incident Reports;
- Client Critical Incident Reports;
- Hazards and maintenance information;
- Information captured in ProSims
- Review of policies and procedures and processes;
- Management knowledge and understanding of service delivery and work processes.

Where appropriate, different staff groups are involved directly in the risk management process either through attendance at part of the CIC meeting or through a CIC member consulting directly with staff.

For example, in identifying in-home service delivery risks an improvement committee member may meet directly with in-home service delivery staff to discuss and identify potential risks and ways to control the risks and report these back to the Improvement Committee.

6.5 Identifying Controls

Controls are strategies to manage risk, balanced against the cost and inconvenience of the control. Common controls include:

- Staff training;
- Provision of information;
- The use of safe or safer equipment;
- Changes in procedures or practices;
- Personal checks including referee checks, driver's licence, motor vehicle registration, professional registration, criminal history check;
- The development of plans for dealing with risks that occur.

6.5.1 Recording Improvements

Improvements implemented as a result of risk management reviews and planning, are recorded in the Improvement Plan, as well as in the Risk Management Plan, to ensure that they are implemented, monitored and evaluated (see Section 5: Continuous Improvement).

6.6 Risk Rating Matrix

The Risk Rating Matrix is used to determine the status of each risk based on the likelihood, and consequences of the risk. The Improvement Committee judges the likelihood and consequences of the risk to identify the rating. The Risk Rating Matrix is also included at the bottom of the Risk Management Plan.

Figure 6.1: Risk Management Rating Matrix

The following tables are from Section 6 – Risk management from the Coastlink Policies and Procedures, and are to be used in order when assessing risk.

1. Assess Control Effectiveness

○ Control Effectiveness Rating	○ Description / Guide
○ Fully Effective	○ Controls are well designed, largely preventive and address the root causes. Controls are effective and reliable at all times. Reactive controls only support the preventative controls. No more to be done except ongoing monitoring and periodic review of the existing controls.
○ Substantially Effective	○ Most controls are well designed, preventive and operating effectively. More can be done to improve control effectiveness, pro-activity and/or reliability.
○ Partially Effective	○ While the design of the controls may be good, they are not adhered to or effective in practice. Alternatively, controls are effective but not well designed or do not address root causes. There may be an over-reliance on reactive controls.
○ Largely Ineffective	○ There are significant gaps in the controls present. The controls may not address root causes, may not be preventive in nature, or may not be effective.
○ Totally Ineffective	○ The risk is not controlled. What control, if any, that does exist is ineffective in preventing risk events from occurring or mitigating their effects.

2. Assess Consequence (reasonable worst case)

The **reasonable worst case consequence** considering the existing controls and their overall effectiveness (as rated at step 1).

Negative Consequence Table							
Rating	**Health & Safety Impact***	**Business Capability**	**Client Impact**	**Environmental Impact**	**Financial Impact**	**Reputational Impact**	**Legal/Regulatory/ Compliance Impact**
5 Extreme	Multiple fatalities and/or injuries with widespread medical attention required.	Loss of key service delivery requiring extended external assistance >1 week.	Client impact severe and lasting >1 week; or multiple clients impacted.	Long term (>5 yr) significant environmental damage or clean up costs > $5 million	Financial loss or unrecompensed expense of >$0.5 million. Fraud >$0.250m.	Damage to corporate reputation at national or state level. Major loss of community support.	Government Agency scrutiny/major government intervention. Significant prosecution, fines or class action. Imprisonment of responsible officers. Major loss of income.
4 Major	Single fatality, serious injuries or occupational illnesses with potential acute or chronic disabilities	Loss of key service delivery requiring external assistance between 1 day and 1 week.	Client impact on functioning for a period of up to one week.	Medium term (1-5 yr) significant environmental damage or clean up costs $1 to $5 million	Financial loss or unrecompensed expense of $0.1-0.5 million Fraud >$100,000.	Damage to corporate reputation at regional or state level. Significant decrease in community support.	Minor government intervention. Requires external legal assistance Prosecution by regulator. Litigation. Responsible officers charged with offence. Loss of income.

3 Moderate	Medical treatment required with potential for short term absence <1 week with no fatalities or serious long-term disabilities.	Loss of service delivery causing disruption of up to 1 day.	Normal client functioning with some inconvenience for 24 or 48 hours.	Short term (<1 yr) environmental damage or clean up costs up to $1 million	Financial loss or unrecompensed expense of $0.05-$0.1 million Fraud >$10,000.	Damage to corporate reputation at local or regional level. Moderate decrease in community support.	Regulatory breaches with investigation or report to authority with prosecution powers. Requires intervention by Board or CEO. Fines possibly incurred.
2 Minor	Minor injuries only, medical treatment required. Sick leave not required.	Loss of service delivery causing disruption of less than half a day.	Some client disruption for less than 24 hours.	Small and short-term environmental damage requiring less than $250,000 to clean up	Financial loss or unrecompensed expense of $0.01 to $0.05 million Fraud >$2,000.	Damage to corporate reputation at local level. Minor decrease in community support.	Minor policy non-compliances or regulatory breaches, managed at CEO level.
1 Insig-nificant	On-site first aid may be required.	Inconsequential loss of service delivery. No impact on operations.	Inconsequential disruption to the community.	Small environmental impact, clean up on-site managed within normal operating budget.	Financial loss or unrecompensed expense of less than $10,000 Fraud <$2,000.	Local awareness of an issue exists but there is no public concern.	Minor compliance issues.

**Includes impacts on staff, contractors, clients and the public*

3. Assess Likelihood (of the reasonable worst case)

The likelihood of the **reasonable worst case consequence** (as rated at step 2),

e.g. the likelihood of tripping and sustaining a serious injury (not the likelihood of tripping).

Likelihood Table	
5 **Highly Likely**	• Strong likelihood of re-occurring, with much opportunity and means to occur. • The consequence is expected to occur in most circumstances (monthly) • High level of known incidents (records/experience)
4 **Likely**	• Considerable opportunity and means to occur. • The event will probably occur in most circumstances (annually) • Regular incidents known (records/experience)
3 **Possible**	• Some opportunity and means to occur. • The event should occur at some time over (2 to 5 years) • Few infrequent, random occurrences recorded/experienced
2 **Unlikely**	• Little opportunity or means to occur. • The event could occur at some time (5 to 15 years) • No known incidents recorded or experienced
1 **Highly Unlikely**	• Almost no opportunity to occur. • The event may occur only in exceptional circumstances (15+ years) • Not known to have ever occurred

4. Rate the Risk

Risk Rating Table – Negative Consequences						
LIKELIHOOD	CONSEQUENCE					
		INSIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	EXTREME 5
	HIGHLY LIKELY 5	Low -L7	Medium -M4	High -H4	Critical -C4	Critical -C1
	LIKELY 4	Low -L8	Medium -M5	High -H5	High -H2	Critical -C2
	POSSIBLE 3	Low -L9	Low -L4	Medium -M3	High -H3	Critical -C3
	UNLIKELY 2	Low -L10	Low -L5	Low -L2	Medium -M2	High -H1
	HIGHLY UNLIKELY 1	Low -L11	Low -L6	Low -L3	Low -L1	Medium -M1

5. Risk Tolerance and Escalation Levels

Risk tolerance determines at what level of authority a risk is to be managed. Where a risk cannot be treated at the organisational level where it is identified, it shall be escalated to the appropriate management level.

Risk Tolerance and Escalation Levels	
RISK RATING	**ACTION REQUIRED**
Critical	**Escalate to Board through chain of command** ▪ Allocate a risk Action Plan Lead and implement a detailed action plan to address the risk. ▪ Include on appropriate business plan as needed.
High	**Escalate to Executive Officer through chain of command** ▪ Allocate a risk Action Plan Lead and implement a detailed action plan to address the risk. ▪ Include on appropriate business plan as needed.
Medium	**Specify management accountability and responsibility** ▪ Monitor trends and plan for potential improvements. ▪ Implement a risk Action Plan if appropriate.
Low	**Manage by routine procedures** ▪ Monitor trends; review costs and effectiveness. ▪ Implement a risk Action Plan if appropriate.

6.7 Monitoring the Risk Management Process

Risk management processes and systems are regularly audited (per 6.1) as part of our audit program and staff, clients and other stakeholders are encouraged to provide ongoing feedback on issues and areas where improvements can be made (see Corporate Calendar and Section 5: Continuous Improvement).

The CEO will provide a Corporate Risk Matrix to every Board Finance, Risk and Audit Committee (FRAC) meeting. The FRAC will also be provided a reviewed copy of the Risk Management Plan every six months, with additional controls and risk identified by the CIC, CEO or through the WHS Committee.

The FRAC will approve the risk audit schedule annually. There are two components of the risk audit:

- An internal review of all risks, their controls and potential residual risk outcomes (inherent risk les controls = residual risk)
- An external audit and review of all Corporate Risks as determined by the Board.