Risk Management Framework & policy

Purpose and Scope
The Board is committed to risk management through the development and implementation of this Risk Management Framework and Policy (the Framework) that provides the necessary foundation and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management. This Framework aligns with the best practice guide AS/ NZS ISO 31000:2009 Risk Management Standard to integrate risk management into processes to assist in achieving business objectives. 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. The Board has ultimate responsibility for safeguarding the organisation and its employees, customers, clients, NDIS participants 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. The Framework addresses both strategic and operational risks. We will use our skills and expertise to identify risks across the organisation and will also identify operational controls in place which manage risk.

Responsibilities and delegations	
This policy applies to	The scope of this Framework and Policy applies to the Access 4 U Board, Executives, managers, other staff, all committees, consultants, contractors. The level of success in managing risks relies on everyone enacting the risk management approach outlined in this document. It is therefore a requirement to comply with this Framework to promote sound organisational culture, governance and accountability arrangements and decision making. The Framework will be communicated to all Board members and staff as part of their induction
Specific responsibilities	**The Board –** Responsible for ensuring adequate resources are made available within the budget to implement all risk management processes. The Board delegates the monitoring and reporting of risk management to the CEO. **The CEO** Responsible for the day-to-day implementation of risk management procedures and for ensuring that all staff are aware of these procedures. **Staff –** Responsible for understanding the policy and implementing the intent and procedures of the policy where applicable in their work.
Policy approval	CEO / Chair

Policy context – this policy relates to:	
Standards	National Disability Insurance Scheme Quality and Safety Framework AS/NZS ISO 31000:2009 Risk Management
Legislation	National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018 National Disability Insurance Scheme Act 2013 Disability Discrimination Act (DDA) 1992

	The Disability Services Act SA 1993
Contractual obligations	NDIS Code of Conduct
Organisation policies and procedures	Sharing Information Guidelines; Human rights Policy; Service Access Policy Worker Screening Policy; Children and Vulnerable Persons Safe Environment Policy Critical Incident Policy; Incident Management Policy and Procedure
Forms, record keeping, other documents	Risk Matrix, Risk Register, Risk Assessments, Board Meeting Minutes, Team Meeting Minutes

Contents

1. Introduction

1.1 Risk Management Defined

The AS/NZS ISO 31000:2009 Risk Management standard defines:

- Risk - as the effect of uncertainty on objectives.
- Risk management - as the coordination of activities to direct and control an organisation with regard to risk.

Risk and risk management are best explained in an organisational context. All activities in an organisation are targeted towards achieving business objectives that are often reflected in strategic, operational, project and activity plans. The ability to achieve these objectives is affected by uncertain internal and external factors, otherwise known as risks. Examples include industry standards, government policies, legislation, financial constraints and effectiveness of internal controls.

Management of risks requires a consistent process that involves establishing the context, identification, analysis, evaluation, treatment, monitoring and regular communication and consultation of risk with stakeholders.

Not all risks have a negative impact. From time to time, internal and external factors may give rise to opportunities. From a “glass half empty” perspective, the risk comes from not taking advantage of arising opportunities. As business objectives vary risk management should be context specific. For example, a negative risk in one organisation may be an opportunity in another.

1.2 Benefits of Risk Management

Risk management when implemented effectively contributes to improved performance by:

- Encourages proactive rather than reactive management;
- Ensures compliance with relevant legal, regulatory, industry standards and requirements;
- Improves governance and controls;
- Establishes a reliable basis for decision making and planning;
- Effectively allocates and uses resources for risk treatment;
- Improves operational effectiveness and efficiency;
- Enhances health and safety performance as well as environmental protection;
- Improves loss prevention and incident management.

The framework for managing risk will form an overarching management foundation upon which other management frameworks can be implemented, such as: planning, reporting and budgeting processes, quality and compliance program, business continuity management program, occupational, health and safety program.

2. Risk Culture

Risk culture refers to the behaviours that impact on how individuals within an organisation consider and manage risk. Developing a positive risk culture involves supporting employees to grow and increase their capability to make consistent and appropriate risk decisions. The 3 components for a positive risk culture are:

(1) Accountability

The Board, CEO AND Executive take leadership for risk management and how it is communicated and managed.

(2) Awareness

Risk management roles, responsibilities and ownership is understood and accepted.

(3) Attitudes

Risk management is viewed as 'everyone's responsibility and acknowledged for the value it creates for the organisation.

3. Governance

- Access4u will engage with our stakeholders to identify risks to our operations and to communicate risk management strategies.
- The level of risk for Access4u and its operations will be assessed by considering the probability and impact and our purposes and objectives. Risks will be ranked in order of importance.
- A Strategic Risk Register will be developed and maintained. This plan will identify how risk is managed.
- Risk assessment will be conducted as part of major projects and business decisions.
- When planning for future events and/or short-term projects, a risk assessment will be conducted.

3.1 Risk Governance

Effective risk governance will:

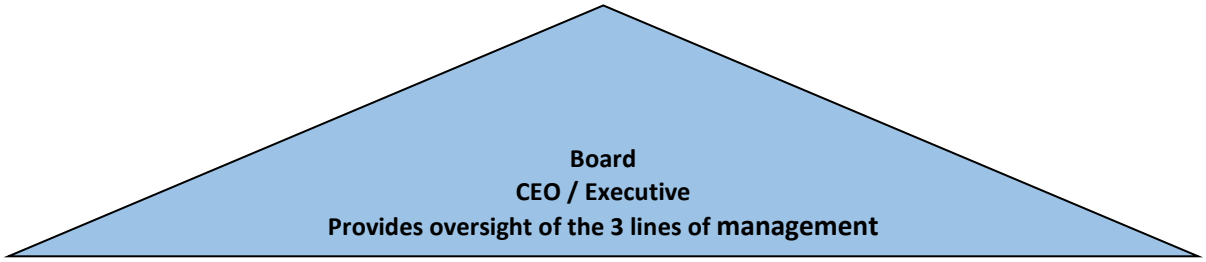
- Guide required risk management behaviours
- Establish consistent processes
- Drive informed decision making

3.2 Risk Appetite Statement

The Board accepts that to be the progressive organisation of choice for people with disability, supporting them to live a life of their choosing, a level of risk taking will be involved. Decisions at Board level will require measured risk taking and informed decision making within defined risk tolerance ranges.

3.3 The levels of Risk Management

This approach identifies three distinct lines of management as depicted below.



First Line are Key to Success	Second Line Support the Business	Third Line Provide Assurance
Frontline Management	Risk Management, Quality and Compliance	Internal & External Audit
People, Systems & Culture	Tools, advice, training and testing	Control, Detection and Correction

3.4 Roles and Responsibilities

The Board

Overall responsibility and accountability to ensure risks are effectively managed, provide leadership, establish the risk appetite and foster a risk aware culture. Through its oversight function receives information and assurance that:

- The Risk Management Framework and Policy requirements are implemented and reviewed
- The necessary steps are taken to foster a risk aware culture across the organisation
- Risk Information is available for consideration in the decision making process

Chief Executive Officer (CEO)

The CEO has overall accountability to the Board for ensuring that there are effective systems for identifying and managing risks. The CEO will oversee the development, implementation and monitoring of the Strategic Risk Register for the organisation. The Strategic Risk Register will cover all aspects of the organisation's activities and involve:

- With support from the management team, ensures the requirements of the risk management framework and policy is being adhered to by establishing the tone from the top;
- Embeding risk management into business and planning processes
- Ensure resources are available to support risk management
- Consider risks that have been escalated by the management team including risk treatment plans
- Embedding risk into strategic discussions and analysis at the managerial levels.
- Ensure documentation of all potential risks and their risk rating
- Identification of actions to manage risk, time frames for any tasks and responsibility. This will include ensuring compliance checks are conducted.
- Monitoring and reviewing of the plan
- The CEO will report to each meeting of the board about critical risk incidents that have occurred and their management
- The CEO will review and report to the governing body at least every six months about the management of risk and will include any changes to the Risk Register and Management Plan
- The CEO will provide a report against the Strategic Risk Register to the Board
- The CEO will review the Strategic Risk Register on an annual basis

Senior Managers

Each Senior Manager has responsibility to manage risks in their portfolio. Collectively the Senior Management team provides assistance to the CEO to manage risk from an organisational perspective including:

- Providing ongoing assurance to the CEO to ensure risks are being management effectively
- Ensuring the effective integration of risk management into planning, reviewing and reporting processes
- Championing the risk management culture and supporting the enhancement of risk management practices
- Conducting assurance activities (compliance audits, operational audits and performance reviews)
- Ensuring the risk register is a live document and maintained on a continuing basis
- Ensuring risk mitigation strategies are identified and implemented
- Considering risks in decision making.

Support Leaders/ Managers / Team Leaders / Coordinators

In collaboration with their team, support leaders, managers, team leaders and coordinators have responsibilities that include:

- project and programs risk assessments
- Consideration of risks in decision making and planning processes
- Overseeing the implementation and effectiveness of key controls; and
- Work Health and Safety and Human Resources programs and initiatives.

All employees, consultant, contractors

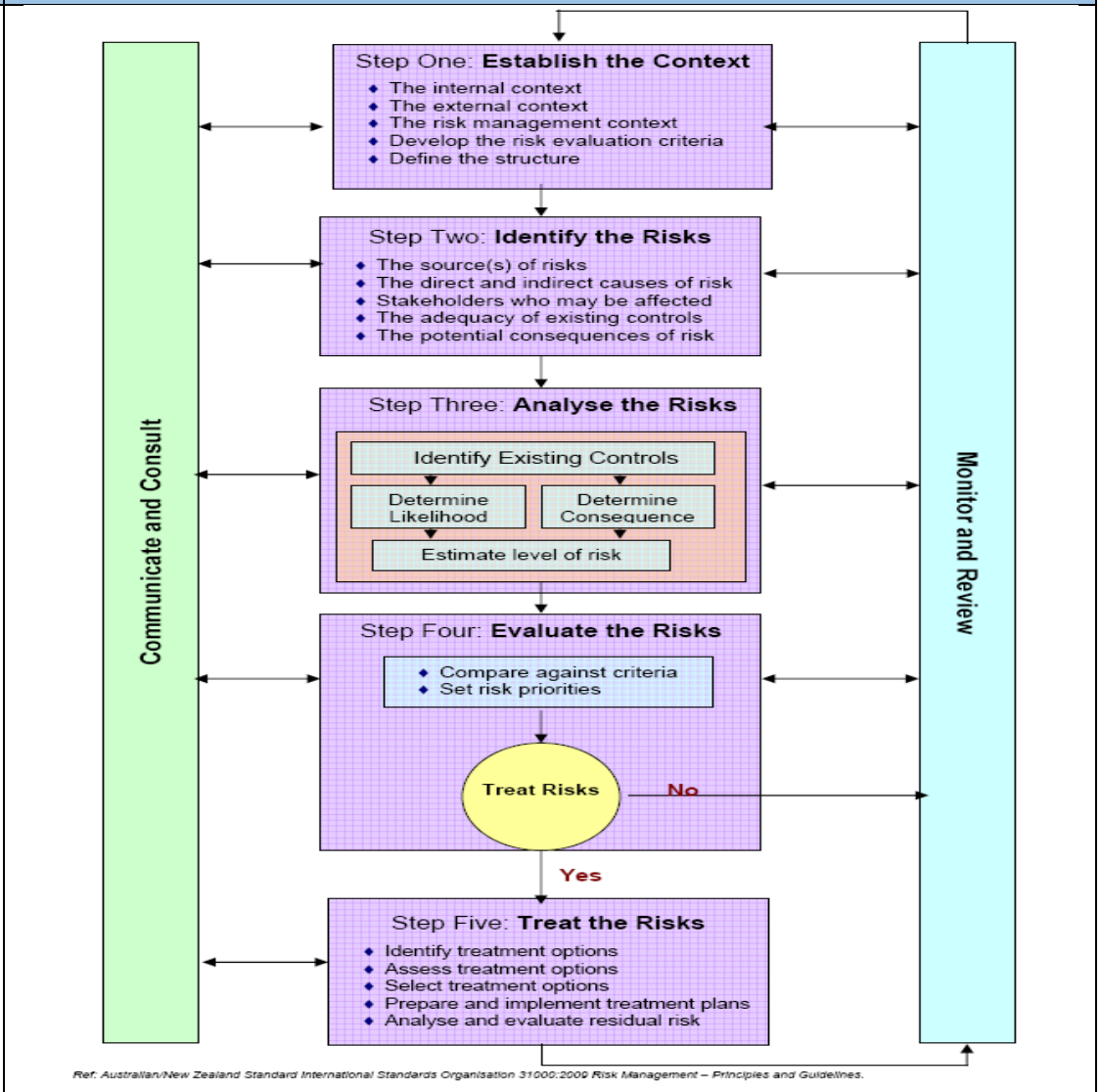
Risks should be considered in all activities conducted by employees, consultant and contractors including:

- Reporting any perceived hazards, risks or issues of concern regarding safety in their area of work to their line manager
- Reporting all incidents/accidents and near misses using the recognised process
- Comply with all Access 4 U policies, procedures, regulations and instructions to protect the health, safety and welfare of anyone affected by the business; and
- Where appropriate, take part in risk assessments.

4. Framework for Managing Risk

4.1 The Risk Principles, Framework and Process

The AS/ NZS ISO 31000/2009 Risk Management Standard is the best practice guide for risk management. This standard is a generic principle based guide that requires risk practitioners to tailor the guidelines to suit the uniqueness of their organisations. While the adoption of this standard is not mandatory, Access4U has implemented the generic risk management processes outlined in the standard; however, established its own descriptor for likelihood, consequences and risk categories to best suit Access4U requirements.

Principles for managing Risk	Framework and Process for managing risk
(1) Creates value (2) Integral part of organisational processes (3) Part of decision making (4) Explicitly addresses uncertainty (5) Systematic, structured and timely (6) Based on the best available information (7) Tailored (8) Takes human and cultural factors into account (9) Transparent and inclusive (10) Dynamic, iterative and responsive to change (11) Facilitates continual improvement and enhancement of the organisation	 *Ref: Australian/New Zealand Standard International Standards Organisation 31000:2009 Risk Management – Principles and Guidelines.*

5. Risk Assessment

Risk assessment in the context of the risk management process for managing risk hs three sequential steps, namely ***Risk Identification, Analysis*** and ***Evaluation.***

5.1 Risk Assessment Requirements

Board and CEO

Regular review of Strategic Risks

- Undertake an annual risk assessment workshop to:
- Examine in detail risks record on the current Strategic Risk Appetite and Risk Register
- Consider the external and internal environment to attempt to identify emerging risk to the organisation.

Senior Managers and Leads

Undertake an annual risk assessment workshop with relevant employees to:

- Examine in detail risk recorded on the Current Risk Register
- Consider the external and internal environment to attempt to identify any emerging risks to their specific function / service
- Risk assessments are require when considering new programs or services, when significant changes occur or opportunities arise that need to be considered
- Project / Program leads undertake regular risk assessments on a t lease a quarterly basis through the life cycle of the project.

5.2 Risk Assessment Outputs

Three separate outputs may be produced as a result of a risk assessment:

(1) Risk Profile

High level summary documents that include risk descriptions, risk and control rating

(2) Risk Register

Detailed summaries for each risk recorded on the Risk Profile. Details recorded include the underlying risk causes, the possible impacts to the organisation as well as existing controls. Required risk treatment action is also summarised.

(3) Risk Treatment Plan

Detailed action plan summaries for each risk treatment recorded in the risk register. These plans will require ongoing monitoring until fully implemented to achieve the necessary reduction in the level of risk.

6. Risk Reporting

6.1 Strategic Risk Profile and Risk Register

Risks associated with the organisation as a whole:

- Issues of strategic importance
- Strategic risk relating to services and system and how they contribute to achieving strategic objectives
- Accountability to external stakeholders to deliver results and conform with legal responsibility

While most risks recorded on the Strategic Risk Register will result from the Board / CEO risk assessments and risk workshop, some risks requiring high level attention may be included due to the escalation of risk from within the business.

Where risks are identified during the course of business, the CEO will consider if a strategic response is required and if this is the case then the risk will be included on the Strategic Risk Register.

6.2 Risk identification

All areas of the organisations will be addressed, and can be grouped according to the following broad categories:

- Service Delivery / Quality
- Financial Management
- Workforce
- Culture / Reputation
- Governance / Regulatory

6.3 Risk Assessment

A risk matrix is used to assess risk. This includes an estimation of both the likelihood of the risk occurring and the impact it may have to the organisation.

6.4 Services Risk Profile and Risk Register

Risks specifically related to the service areas. The risk profile and risk register is dynamic and must be reviewed and updated periodically to take into consideration new information, changes in the operating environment and completion of actions from risk treatment plans.

Service areas will maintain their own service risk registers (where appropriate). The Senior Manager / Manager for the service is responsible for monitoring the risk register and a copy is to be provided on a quarterly basis or when the register is substantially changed to the CEO. This also applies to project / program specific risk registers.

The CEO will review all service area specific risk registers and report the key findings in updates to the Board on a quarterly basis.

7. Risk Treatment

7.1 Planning Principles

When considering the need for risk treatment for risks identified as requiring mitigation, the following principles are to be observed:

Legal:	Any risk identified that breaches legal and or regulatory obligations – resolve
People Safety:	Any risk to our customers, our employees, contractors or the community - **ALARP**, which stands for "as low as reasonably practicable". The **ALARP principle** is that the residual risk shall be reduced as far as reasonably practicable
All other Risks	Cost Benefit Analysis – The business case supports the proposed action

7.2 Risk treatment Planning Options

Risk treatment planning consists of the identification of feasible but cost effective risk treatments. A combination of control treatment options may be appropriate in treating risks including:

- ***Avoiding the risk*** – Where the level of risk is unacceptable and the means of risk control are either not viable or not worthwhile or not actionable, risk could be eliminated by not proceeding with the activity that could generate the risk.
- ***Changing the risk likelihood*** – Undertake actions aimed at reducing the probability of the risk occurring. This can be redesign of the services to optimise the processes to mitigate the risk.
- ***Changing the risk consequence*** – undertake actions aimed at reducing the impact of the risk.
- ***Retaining or accepting the risk*** – Accept the risk as it is. This is appropriate where the rating of a risk is sufficient to justify other potential risk treatment options, or when it is not possible or uneconomic to treat the risk, or when the risk level is within risk tolerance.
- ***Sharing the risk*** – Responsibility for treating the risk can be transferred or allocated to parties best able to manage it. (using insurers or contractors or entering into joint venture or partnership).

8. Risk Management Assurance Activities

The risk governance structure ensures risks identified are reported to relevant people and the Board.

Reporting of risks in it self does not provide assurance that controls implemented are actually being lived. To address this issue, three types of assurance activities occur throughout the year.

As part of the assurance program, it is essential that the risk register - risk treatment plans and subsequent monitoring of progress are assigned to the appropriate person.

The frequency of the monitoring should be dictated by the level of risk and cost-benefit for doing so.

(1) Monitoring and Review

- Access4u will monitor, report and review its management of risks regularly and after any incident. Monitoring is how you continually check, supervise, and track the progress of an activity so you know whether it is happening as you expect. This checking will be done against assessed risk, agreed measures, objectives or an expected level of performance.
- The Board will consider the review of the Risk Management Policy, after input from the CEO and other stakeholders. The review of the relevant Strategic Risk Register should be completed each year to re-evaluate all the risks, taking into account the changes in the environment, stakeholders and other factors, as well as the plans and processes to manage risks.
- If there has been an incident not covered by the Risk Register, or if other factors have changed, this will trigger a review of the risk and where appropriate the development of a Strategic Risk Register.
- When there is an incident or an event that did not go as planned or that exposes a new area of risk, it is important to review the causes. After the review there may be a need to consider the activities to prevent the identified risk from happening again, and to update the relevant Strategic Risk Register.

(2) Internal Audits

Internal audits are conducted in accordance to the annual audit plan. The annual audit plan aligns with the risk profile.

Assurance Activity	Frequency
Client satisfaction survey	3 yearly
Policy review	3 yearly
Currency and adequacy of insurance cover	Annual
Compliance with contractual arrangements and funding agreements	Annual
Equipment maintenance	Annual
Occupational, health and safety audit	6 monthly
Annual Human resource or personnel file audit	Annual
Client feedback, complaints and compliments audit	Annual
Annual Performance appraisal audit Professional development / training audit	Annual
Compliance with regulatory body requirements	Annual
Incident, near miss audits	Annual

(3) Control Self Assessments

Control self assessments is a technique used to assess control adequacy and effectiveness. In contrast to internal audit, the tests are performed by staff whose normal day to day responsibilities are within the business unit being assessed. Where practicable, tests are conducted on an area by staff that do not work there but have sound knowledge of its operations. Self assessments allow management to address control issues on a continuing basis to promote continuous improvement.

Control self-assessments are generally related to compliance with funding agreements (grants), industry specific legislative and regulatory requirements, and where relevant code of practice.

Senior Managers are responsible for managing control self-assessments. Results are reported from the Senior Managers to the CEO who provides advice and assistance to Senior Managers on how to address the findings. The benefits of control self-assessments include compliance issues are addressed on a continuing basis to assist meet obligations and deal with the rigor of external audits; and

(4) External Audits

External audits refer to independent audits conducted by external parties. Examples include audit of the financial reports, NDIS audits.

Appendix 1 Key Definitions

Risk	In the context of the generic Australian / New Zealand / International Standard: AS/NZS ISO 31000:2009, risk is defined as "the effect of uncertainty on objectives."
Strategic Risk	Risk which could affect the achievement of Strategic Objectives outlined in the Strategic Plan
Operational Risk	Risk which can affect the day to day operations
Risk Owner	Person or entity with the accountability and authority to manage the risk (AS/NZS ISO 31000:2009)
Risk Management Process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk (AS/NZS ISO 31000:2009)
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation (AS/NZS ISO 31000:2009)
Risk Appetite	A measurement of the tendency or inclination for risk taking or risk aversion
Risk Tolerance	The predetermined level of risk the organisation, whilst not accepting it, is prepared to take to achieve its corporate objectives. The higher the risk tolerance, the more risk the organisation is prepared to take.
Risk Opportunity	"The Risk Management process can be used to identify and prioritise opportunities (*i.e. 'positive' risks*) with little change to the process." *Risk Management Guidelines - HB 436:2004 p58*
Risk Profile	Description of any set of risks (AS/NZS ISO 31000:2009) A risk profile is an evaluation of an individual's willingness and ability to take risks. It can also refer to the threats to which an organisation is exposed. A risk profile is important for determining a proper investment asset allocation for a portfolio.
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk (AS/NZS ISO 31000:2009)
Risk Treatment	Accept and monitor low-priority risks (*risks rated moderate and low*). For other high-priority risks (*risks rated high and extreme*), develop and implement a specific treatment management plan for each risk, which includes consideration of resource and funding requirements. The risk treatment process ensures that managers take responsibility to identify all options available to treat the risk by assessing / evaluating those options, selection of the most appropriate method available, and the development and implementation of a treatment plan.