CBB Risk Policy Model

*Guidance note: This Risk Policy provides the overarching document and philosophy regarding risk for the Board to approve.*

*The list of areas for the risk register/s to (as appropriate) is based on the NDIS Practice Standard – so this list could look different in other organisational contexts. Organisations using this model document should review what applies to them.*

*This risk policy references and relies upon the international standard for risk management which is ISO31000. We recommend that you get a copy of this standard, read/review it before using this model policy/procedure. There are many free resources online which include extracts of and guidance about the standard.*

## Purpose

[Organisation] views effective risk management as being integral to achieving its strategic objectives. This policy provides the framework to govern and manage the risks associated with achieving these strategic objectives. It is designed to identify, assess, prioritise, monitor and manage the different types of risk that the organisation encounters – in order to both mitigate risks and maximise opportunities.

## Scope

This policy applies across the organisation from the Board through management to service delivery and functional support areas. Refer also to the Risk Framework, Risk Appetite and Risk Procedure.

## Definitions

*Risk* is the effect of uncertainty on achieving the organisation’s objectives. It may be a positive or negative deviation to what is expected. It includes, but is not limited to, risks relating to:

* Service delivery
* Physical environment – e.g. health, safety and environment
* Finance and cashflow
* Reputation and image
* Legal, regulatory and statutory requirements.

Refer to *AS/NZS ISO 31000 Risk management - Principles and guidelines* for other definitions.

## Policy Statement

[Organisation] aims to make risk management a part of the organisation’s culture which is integrated into its philosophy, practices and business plans. The risk culture is driven from the top down and is recognised as the responsibility of everyone.

By having a structured approach to risk management, [Organisation] aims to have:

* More effective decisions and transparency in decision making
* Effective delivery of services
* High standards of service and safety for customers, employees, volunteers and the general community
* Effective allocation and use of resources
* High standards of accountability
* Creativity and innovation in management practice
* Consideration of legal issues and compliance with the law, funding requirements and any other formal requirements.

[Organisation] recognize that AS/NZS ISO 31000 Risk management - Principles and guidelines has become the model by which most organisations seek to follow in the risk management process of identifying and managing risk. [Organisation] subscribes to the process, methodology and definitions in this standard.

Risks of the organisation shall be documented and reviewed in the form of a risk register/s. Once created, the risk register should be a live document that’s dynamically updated, following incidents and complaints. Such risk register/s shall consider the following areas as appropriate:

* Incident management
* Complaints management
* Work health and safety
* Human resource management
* Financial management
* Information management
* Governance.

Within the context of this Risk Policy, the organisation will consider other external requirements on the organisation as appropriate, including in relation to NDIS Practice Standards, Aged Care Quality Standards, other accreditations and insurance.

We recognise that part of the organisation’s core activities and purpose involves working with vulnerable people, and that risk related processes will consider the needs of those vulnerable individuals and groups in ascertaining what risk mitigations and treatments to apply.

Management shall develop and put in place a Business Continuity Plan in accordance with requirements of the Risk Procedure, and test this at least annually.

Other organisational policies and procedures shall be developed using a risk-based approach such that these policies/procedures are a key tool in mitigating and minimising risk to the organisation.

The organisation shall ensure that appropriate insurances are in place through at least an annual process of review, as part of the insurance policy renewals.

*Organisations should consider whether to include specific reference to other practices, processes or requirements here based on the organisational context – e.g. (not exhaustive) restrictive practices, medication, behaviour supports, vulnerable people groups.*

## Responsibilities

The Board, with the assistance of the CEO, is responsible for overseeing the establishment and implementation of risk management systems and reviewing their effectiveness.

The Board, with support of its [name of Board Committee which Risk is part of}, provides oversight of the organisation’s risk management activities through review/approval of this risk policy and appetite, fostering the risk culture, reviewing insurance coverage, reviewing and overseeing strategic risks and monitoring emerging risks.

The Board and CEO will work together to ensure consideration of risk and opportunity is a part of the strategic planning and budgeting processes.

The CEO report to the Board shall include a section on risk which includes updates on:

* Extreme and key strategic risks at each Board meeting
* High, Medium and Low risks at least once a year
* New and emerging risks to the organisation.

It is the responsibility of the CEO to ensure that:

* Effective risk management procedures are in place, applicable to all parts of the organisation
* Risk management procedures are reviewed regularly
* Recommendations arising out of the risk management process are evaluated and implemented
* Employees and volunteers are made aware of applicable risks and are familiar with the organisation’s risk management procedures
* Risk management analyses are carried out for all parts of the organisation
* Copies of up-to-date risk registers are maintained.

The Risk Coordinator will support the CEO with:

* Review and updates to the risk register, risk plans and business continuity plan
* Reporting on risk including new and emerging risks
* Guidance and accountability to business units and support functions in managing risks.

It is the responsibility of all employees and volunteers to ensure that they:

* Are familiar with the organisation’s risk management procedures applicable to their section
* Observe those risk management procedures
* Inform their supervisor if they become aware of new or emerging risks, and any risk not covered by existing procedures.

## Review of Policy

The Board of [Organisation] will review this policy annually or as often as it determines necessary and will make any changes it determines necessary or desirable.

*Organisations will often have a standard format for policies/procedures and sections such as this. For this and any other relevant sections or structure, you should consider using whatever your organisational norms are.*