# *Capricorn Citizen Advocacy*

## RISK MANAGEMENT FRAMEWORK

| | | | |
|---|---|---|---|
| **Policy number:** | 1.3.6 | **Approved by Management Committee:** | 27th March 2024 |
| **Version:** | 4.0 | **Signed off by Executive:** | 27th March 2024 |
| **Responsible person:** | Coordinator | **Scheduled Review Date:** | 27th March 2027 |

## Purpose

All activities of organisations involve risk.  Organisations manage risk by understanding, anticipating and deciding whether to treat the risk.  This process involves communication with stakeholders and monitoring controls and treatments of risks.

This policy explains Capricorn Citizen Advocacy's risk management framework which is based on *AS ISO 31000:2018 Risk Management Guidelines.*

## Policy

**1.  What is a Risk Management Framework?**

**A risk management framework** coordinates activities to direct and control an organisation's activities with regard to minimising or eliminating risk.

**Risk -** is an internal or external factor that causes uncertainty for an organisation being able to meet its objectives. The effect of risk is to deviate from what is expected, either in a positive or negative way.

**Objectives -** are statements of intent in particular areas.

**Consequences** - of poor risk management for foreseeable events may include:

1.  Physical or psychological injury to ourselves or others.
2.  Loss or damage to property and services.
3.  Reputational loss
4.  Legal action being taken against us for things we either do, or fail to do.

## 2. Integrated Risk Management

Organisations should integrate risk management into everyday strategy and planning, governance, financial management, operations, projects, reporting, policies and organisational culture. Risk management is not an isolated function that exists within the agency.

Integrated risk management therefore requires an ongoing assessment of potential risks and opportunities impacting CCA at every level. The results of our ongoing assessments should inform our level risks, facilitate priority setting and improve our decision making.

Clear links should be established between risk management, Government policies and priorities, our objectives (vertical integration), and our policy and operations (horizontal integration).

## 3. Risk Management Framework Principles

Principles for Managing Risk (*AS ISO 31000:2018 Risk Management - Clause 4*)

Risks, risk profile, risk management capability and systems, and the risk environment are all constantly changing and evolving. The principles of effective risk management will assist organisations deal with a dynamic environment;

1. Creates value
2. Integral part of organisation's processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Systematic, structured and timely
6. Based on best available information
7. Customised
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

## 4. Managing Risk

*AS ISO 31000:2018* gives a list in order of preference on how to deal with risk:

1. Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk
2. Accept or increase the risk in order to pursue an opportunity
3. Remove the risk source
4. Change the likelihood
5. Change the consequences
6. Share the risk with another party or parties (including insurance contracts)
7. Retain the risk by informed decision

## 5. What does **AS ISO 31000 2018 Risk Management** do?

Capricorn Citizen Advocacy's risk management framework is based on *AS ISO 31000:2018*. The objective of the standard is to provide guidance to enable public, private or community enterprises, groups and individuals to achieve:

1.  A more confident and rigorous basis for decision-making and planning
2.  Better identification of opportunities and threats
3.  Gaining value from uncertainty and variability
4.  Pro-active rather than re-active management
5.  More effective allocation and use of resources
6.  Improved incident management
7.  Reduction in loss and the cost of risk, including commercial insurance premiums
8.  Improved stakeholder confidence and trust
9.  Improved compliance with relevant legislation
10. Better corporate governance

## 6.  Factors which lead to Poor Risk Management

Factors that inhibit effective risk management in organisations and which may impact on CCA include:

1.  Lack of support for a risk management culture from staff and Management Committee
2.  A lack of time and resources allocated to risk management
3.  Difficulty in identifying and assessing emerging risks
4.  Lack of independent assurance over the effectiveness of the risk framework
5.  Lack of clarity over risk ownership and the responsibility for risk management
6.  Over or under treatment of risks, and
7.  Unnecessarily complex risk documentation.

## 7.  Risk Management Process (AS ISO 31000 2018 Risk Management - Clause 6)

Effective risk management enables organisations to have increased confidence that they can deliver the required services, manage risks and threats to an acceptable degree, and make informed decisions about opportunities and challenges they face. Capricorn Citizen Advocacy endorses the process for managing risk as set out in *AS ISO 31000:2018.*

While the steps are shown separately within this process, the risk management process is continually occurring. The processes can be undertaken in any sequence and some processes overlap or fall in a different order. Further detail on this framework is provided below;

- Establish the Risk Context
- Risk Assessment
    - o Risk Identification
    - o Risk Analysis
    - o Risk Evaluation
    - o Risk Treatment
- Communication and Consultation
- Monitoring and Review

### a.  Establish the Risk Context

Capricorn Citizen Advocacy will regularly review its risk matrix and responsibilities.

A risk matrix combines the likelihood of the risk occurring and the consequence should such a risk occur.  This results in the risk rating for treating and/or monitoring the risk.  Parameters are set for each likelihood and consequence in the risk matrix. For example, the likelihood of a risk occurring may be classified as 'unlikely' if it is expected to occur less than 5% of the time, or once in a year.

Each possibility within a matrix is defined and the necessary action documented for each possibility.  The matrix is reviewed with the internal and external environments to determine the relevance to the risks.

|  | Consequence | |
| --- | --- | --- |
| **LIKELIHOOD** | **Minor** | **Moderate** |
| **Unlikely** | Low | Low |
| **Possible** | Low | Medium |
| **Likely** | Medium | High |

## b. Risk Identification

Once the context is established, the next stage is to identify individual risks.  The aim is to generate a comprehensive list of threats and opportunities based on events that create, enhance, degrade, delay or prevent the achievement of CCA's strategic objectives.

A common method used to identify emerging risks is environmental scanning.  An environmental scan is a powerful risk management and strategic planning tool that entails careful monitoring of an agency's internal and external environments to detect early signs of challenges and opportunities that may influence the agency's current and future plans.

It involves obtaining both factual and subjective information on potential challenges and opportunities to increase the CCA's awareness of the key risks it faces, including;

- Type of risk – political, legal, economic, environmental, socio-cultural or technological
- Source of risk – external (political, economic) or internal (reputation, security, knowledge management)
- Impacts of the risk – type of exposure (people, reputation, program results, priorities, funding, assets), and
- Level of control – the degree to which the agency can influence, affect or manage the risk.

It is vital that relevant and up-to-date information is used, and that people with appropriate knowledge are involved in the risk identification process.

## c. Risk Analysis

Risk analysis involves exploring the impact of any challenge or opportunity using the risk matrix, starting with an assessment of the consequences as well as the likelihood of a risk occurring.

Where Capricorn Citizen Advocacy considers the risk analysis process to be relatively straight-forward, then categorisation of the risk as high, medium or low is sufficient. CCA will use critical judgement to determine the level of analysis that is required based on what is appropriate and reasonable.

Once risks have been identified and analysed, CCA will use a simple table to summarise the assessment:

| Risk | | |
| --- | --- | --- |
| **Low** | **Medium** | **High** |
| **1.** | | |
| **2.** | | |
| **3.** | | |

### d. Risk Evaluation

Once CCA has identified and analysed its risks, the risks will be evaluated to determine which risks are to be treated and the priority for treatment implementation.

This process is known as risk evaluation. Treatment options are outlined in the 'Risk Treatment' - section (e) below.

The highest priority will be given to those risks that are evaluated as being the least acceptable. High priority risks should be given regular attention, review and evaluation.

Over time, specific risks and risk priorities will change, and CCA will review and evaluate its prioritisation process.

### e. Risk Treatment

Once risks have been evaluated, Capricorn Citizen Advocacy will determine the appropriate risk treatments. Any action taken to address a risk becomes part of CCA's internal risk controls. Risk treatment options include:

(a) **Treat the Risk.** This approach enables the activity or action to continue within the agency, but action is available to reduce the risk to an accepted level. The 'treat' option can be further dissected into four different types of controls:

- **preventative controls** – designed to limit the possibility of an undesirable outcome being realised. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement preventive controls. Examples include separation of duties, installing security cameras to deter criminal activity etc.
- **corrective controls** – designed to correct undesirable outcomes which have been realised. Examples of corrective controls include audit review

of preventative and detective controls, or a change of management procedures.

- **directive controls** – designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, particularly in the area of health and safety. An example is a requirement for protective clothing or equipment to be worn.

- **transfer the risk.** Risk transfer may be achieved by buying insurance to facilitate financial recovery against the realisation of a risk. Risk may be wholly transferred, or partly transferred (that is, shared).

- **terminate the risk.** Some risks may only return to acceptable levels if the activity is terminated.

- **accept the risk.** It may be appropriate to accept the risk rather than treat the risk. A risk may be accepted because:

  - the probability or consequences of the risk is low, or minor
  - the cost of treating the risk outweighs any potential benefit
  - the risk falls within our established risk appetite or tolerance levels

CCA may prepare **risk treatment plans** if necessary to document how the chosen treatment/action will be implemented. The following points will be addressed:

- person assigned to implement the plan
- proposed actions and timeframes
- physical resource requirements to implement the actions
- performance indicators to measure, review and evaluate the effectiveness of the treatment/action, and
- ongoing monitoring and reporting requirements

## f. <u>Monitoring and Review</u>

Monitoring and review processes may be undertaken as part of a formal periodic process, or performed on an ad hoc basis.

Monitoring and reviews will determine whether risks still exist, whether new risks have arisen, whether the likelihood or impact of risks have changed and to reassess the risk priorities.

Monitoring and reviews provide important feedback regarding the efficiency and effectiveness of controls.

## g. <u>Communication and Consultation</u>

In order to ensure the effectiveness of the risk management process, CCA has a reporting structure wherein the Coordinator reports regularly to the Management Committee regarding the status of the risks currently on the risk register.

Reporting must be timely and will address the following points:

♦ the adequacy and effectiveness of the internal controls in place to treat risk
♦ identification of any new risks that may have arisen, and
♦ implementation of new controls to address key risks.

## Related Documents

1. *1.3.6.1    Risk Management Plan & Risk Register*
2. *4.3.0        Workplace Health and Safety Policy*
3. *4.7.0        Child and Youth Risk Management Strategy*
4. *4.7.0.1     Handling Disclosures or Suspicions of Harm, including Reporting Procedure*

## References

1. *AS ISO 31000:2018 Risk Management Guidelines*
2. *HB 266:2010 Guide for Managing Risk in Not-For-Profit Organisations*
3. *A Guide to Risk Management, July 2011; The State of Queensland (Queensland Treasury)*

---

### Ratification

**This policy was adopted by Capricorn Citizen Advocacy's Management Committee at its meeting held on 27 / 03 / 2024.**

**SIGNED:**  .....................................…     **SIGNED:**  .....................…………….…
**President**                                               **Secretary**

**27 / 03 / 2024**                                **27 / 03 / 2024**
**(Date)**                                             **(Date)**

---