



## Croydon Shire Council

# Risk Management Policy

### Document Control

**Version Number:** 2

**Next Scheduled Review Date:** September 2022

**Author:** Finance Manager

**Council Approval Required:** Yes

**CEO Approval:**



Resolution Number	Date	Reason/Comment
04/11/2016	13 October 2016	Legislation
05-12/2020	19 November 2020	Review, updated definitions and reference to amended standards

## 1. Purpose

Croydon Shire Council recognises that as a public authority it is exposed to a broad range of risks which, if not managed, could adversely impact on the organisation achieving its strategic objectives. Therefore Council will implement a systematic risk management methodology to identify and address, where practical, areas of potential risk within Council. Any methodologies adopted will be consistent with AS ISO 31000:2018 Risk management - Guidelines.

The intent of this policy is to create an environment where Council, management and staff assume responsibility for risk management, through consistent risk management practices.

## 2. Scope

This policy applies to all Councillors and officers of Croydon Shire Council who are involved in the identification and management of all risks associated with the performance of Council functions and the delivery of Council services.

Contractors, committees and volunteers engaged in the provision of Council services, or the management of Council facilities and assets, are also required to comply with this policy.

## 3. Definitions

### **Risk**

Risk is defined by the Australian Standard for Risk Management as “effect of uncertainty on objectives”. An effect is a deviation from the expected. It can be positive, negative or both and can address, create or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

### **Risk Management**

Risk Management is the coordinated activities to direct and control an organisation with regards to risk. Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

### **Enterprise Risk Management (ERM)**

Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by Council’s business functions and activities with identified risks.

### **Risk Register**

The risk register lists identified and assessed risks.

## 4. Objectives

The objectives of this policy are:

- Align Council activities to and support business objectives identified in Council's corporate and operational plans;
- Maintain and improve reliability and quality of service provided by Croydon Shire Council;
- Minimise or eliminate adverse impacts from Council's services or infrastructure on the community, visitors and the environment;
- Capitalise on opportunities identified for Croydon Shire Council;
- Safeguard Council's employees, contractors, committees, volunteers, assets, financial sustainability, property, reputation and information;
- Promote risk management principles as a strategic tool to ensure better informed decision making throughout Council; and
- Create a culture of risk management across the Council.

## 5. Principles

The following principles will be adopted to ensure that the objectives are achieved:

- Apply a risk management framework which is consistent with the current *AS ISO 31000:2018 Risk management - Guidelines* for making decisions on how best to identify, assess and manage risk throughout all departments of Council;
- Evaluate identified risks and implement treatments progressively based on the level of risk assessed and the effectiveness of the current treatments;
- Integrate risk management with existing planning and operational processes, including the Corporate Plan;
- Take into account relevant legislative requirements and political, social and economic environments in managing risks;
- Create a culture of risk awareness throughout the organisation through training, induction, promotion and risk review and reporting mechanisms; and
- Ensure resources and operational capabilities are identified and responsibility for managing risk is allocated.

## 6. Roles and Responsibility

<b>Council</b>	Council is responsible for adoption of this policy and ensuring sufficient resources are applied to managing the risks identified.
<b>Chief Executive Officer</b>	Council's Chief Executive Officer is responsible for identifying, evaluating and managing risk in accordance with this policy through a formal enterprise-wide risk management framework.
<b>Leadership Team</b>	<p>Council's Leadership Team will perform the function of the Risk Management Committee which has oversight of developing the risk management framework and monitoring risk treatment.</p> <p>The Leadership Team will ensure the risk management framework identifies high level strategic risks and aligns with the Internal Audit Plan.</p> <p>The Leadership Team will ensure that the results of its reviews are provided to Council for update of the Council's risk profile as appropriate.</p> <p>The Leadership Team will ensure periodic reviews of the risk management framework are carried out by Internal Audit pursuant to the Internal Audit Plan.</p> <p>Council's Leadership Team is responsible for the accuracy and validity of risk information reported to the Council. In addition, it will ensure clear communication throughout the Council of the Council's and senior management's position on risk.</p>
<b>Employees including casual staff, contractors and volunteers</b>	<p>All employees are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans.</p> <p>Employees will be responsible for the timely completion of activities conducted routinely to ensure that employees are familiar with risk management and how it is applied within Croydon Shire Council.</p>
<b>Risk Monitoring</b>	<p>Council utilises a number of functions, including Internal Audit, to perform independent and objective monitoring over its risk areas, including if necessary, conducting reviews over Council's operations and risk areas by external agencies.</p> <p>The scope of the work undertaken by all of these functions and the reviews by external agencies, will be considered in conjunction with Council's risk profile at least annually. This will assess the independent monitoring of key risk areas within Council's risk profile.</p>

## **7. Implementation**

The implementation of this policy is the responsibility of the Chief Executive Officer.

## **8. Policy Review**

This Policy will be reviewed when any of the following events occur:

- Audit reports relating to risk management activities being undertaken by Council indicate that a policy review from a legislative, compliance or governance perspective is justified;
- Relevant legislation, regulations, standards and policies are amended or replaced; and
- Other circumstances as determined from time to time by the Chief Executive Officer or through a resolution of Council.

**Notwithstanding the above, this policy and Council's risk management framework will be reviewed at least every two years by Council's Executive Leadership Team to review its effectiveness and to ensure its continued application and relevance.**