



Enterprise Risk Management Framework **Policy**

April 2021

Policy No: CCC 032

| | |
|---------------------|--|
| Policy owner: | Governance and Risk, Corporate Affairs |
| Approved by: | David Farmer, Chief Executive Officer |
| Date of approval: | 19/04/2021 |
| Policy category: | Internal |
| Content Manager No: | D14582043 |
| Review date: | 01/04/23 |



Contents

| | |
|---|---|
| Purpose | 3 |
| Scope | 3 |
| Background | 3 |
| General | 3 |
| Review | 6 |
| Compliance, monitoring and review | 6 |
| Records management | 6 |
| Definitions | 6 |
| Related resources | 7 |
| History of revisions | 7 |

Purpose

1. The purpose of this Enterprise Risk Management (ERM) Policy is to communicate Council's commitment to managing enterprise-wide risks and to establish clear expectations to ensure that all staff are aware of their responsibilities for identifying and managing risk.

Scope

2. This Policy covers personnel employed by Council; any person or organisation contracted to or acting on behalf of Council; and any person or organisation employed to work on Council premises or facilities and all activities of the Council.
3. This policy does not confer any delegated authority upon any person. All delegations to staff are issued by the Chief Executive Officer.

Background

4. Central Coast Council (CCC) acknowledges that significant risk events, should they occur, have the potential to adversely impact the achievement of its strategic, operational, financial, regulatory and other objectives.
5. Risk management thought processes, principles and practices will support the achievement of objectives, helping Council deliver quality services, improving decision-making, establishing priorities, promoting safety, minimising the impact of loss, and ensuring regulatory compliance.

General

6. Amendment to this policy will occur in accordance with the procedure for Organisational Policy establishment.
7. It is the personal responsibility of all CCC employees and agents thereof to have knowledge of, and to ensure compliance with this policy.
8. CCC is committed to the formal, systematic, structured and proactive management of risks across the organisation.
9. Whilst risk is inherent in all CCC's activities, the management of risk is intelligent business practice, creates value, is integral to good corporate governance and, in some instances, a mandatory legal requirement.

10. Effective risk management:
 - a) supports decision-making and planning;
 - b) increases the likelihood of achieving objectives; and
 - c) identifies opportunities.
11. CCC is committed to maintaining an effective, efficient and tailored risk management framework that consists of this policy, an enterprise risk management strategy, and supporting policies that complement risk management such as fraud prevention, internal audit, business continuity, environmental and WHS management systems and the Code of Conduct.
12. The ERM framework enables:
 - a) formal, structured approach to risk management that is appropriate to CCC's activities and operating environment
 - b) risk management approach consistent with the principles of AS ISO 31000:2018.

CCC's current risk management framework is contained in a separate document and is broadly based on a low tolerance to risk, particularly where it may affect the safety of staff and/or the community, financial viability and regulatory compliance.
13. CCC is committed to ensuring that a strong risk management framework is in place that:
 - a) integrates risk management with existing planning and operational activities
 - b) allocates sufficient funding and resources to risk management activities
 - c) provides staff with appropriate training in risk management principles and processes
 - d) assigns clear responsibilities to staff at all levels for managing risk
 - e) embeds controls to manage risks into business processes
 - f) establishes mechanisms for measuring and reporting risk management performance
 - g) communicates risk management policies, plans and issues to staff and other stakeholders
 - h) is dynamic, iterative and facilitates continual improvement.
14. Council is ultimately responsible for committing to this Risk Management Policy and fully considering risk management matters contained in Council reports.
15. The Chief Executive Officer is responsible for leading the development of an enterprise risk management culture across the organisation and ensuring that this Policy and the enterprise risk management framework are being effectively implemented.
16. The Executive Leadership Team is responsible for considering urgent, sensitive and/or complex risk management issues that cannot be resolved by staff.
17. Directors and Executive Managers are responsible for ensuring that this Policy and the risk management strategy are being effectively implemented within their areas of responsibility.
18. Unit Managers are required to create an environment where the management of risk is accepted as the personal responsibility of all staff, volunteers and contractors. Managers are accountable

for the implementation and maintenance of sound risk management processes, structures and outcomes within their areas of responsibility in accordance with Council's risk management framework.

19. The Enterprise Risk Manager is responsible for ensuring that all requirements necessary for the implementation and operation of the risk management strategy across Council are in place, including:
 - a) reporting to Executive Team on business, risk plans for major projects and undertakings, and new and emerging risks relevant to Council
 - b) reporting to the ERM Committee on ERM Framework development needs
 - c) implementing directions of Executive Team relating to the ERM Framework
 - d) contributing to Council's risk policy, risk appetite, and strategic, operational and project risk planning
 - e) assisting managers in understanding the interrelationships between various types and sources of risk
 - f) creating a risk-aware culture
 - g) ensuring a consistent approach to ERM throughout Council.

20. The ERM Management Team is responsible for periodically reviewing the ERM Framework and for:
 - a) planning and facilitating the progressive implementation of the ERM Framework and the development of a risk-aware culture
 - b) establishing and monitoring key performance indicators for the implementation and operation of the ERM Framework
 - c) reporting quarterly to the Executive Team regarding the performance of the ERM Framework, including recommendations to achieve performance targets
 - d) identifying training and development needs to achieve the required risk management competencies across CCC
 - e) coordinating resources to support the implementation of the ERM Framework
 - f) facilitating the formal review and update of the ERM Framework.

21. Staff are always required to act in a manner which does not place at risk the health and safety of themselves or any other person in the workplace. Staff are responsible and accountable for taking practical steps to minimise Council's exposure to risks including financial, legal, environmental, reputation and conduct insofar as it is practicable within their area of activity and responsibility, and for notifying potential hazards and opportunities.

Review

Compliance, monitoring and review

22. This policy will be reviewed every three years, or more frequently in the event of a material change in circumstances.
23. Suspected breaches or misuse of this policy are to be reported to the Chief Executive Officer. Alleged breaches of this policy shall be dealt with by the processes outlined for breaches of the Code of Conduct, as detailed in the Code of Conduct and in the Procedures for the Administration of the Code of Conduct.

Records management

24. Staff must maintain all records relevant to administering this policy in the Content Management system

Definitions

25. In this policy:

Code of Conduct means the Code of Conduct adopted by Council.

Council means Central Coast Council.

Act means the Local Government Act.

Council staff means employee of Council and includes the Chief Executive Officer.

Mayor means the person elected as the Mayor of the Council.

Risk is the effect of uncertainty on objectives – it can be positive or negative.

Risk Management is a systematic process that involves establishing the context for risk management, identifying and analysing risks, treating and controlling risks, periodically monitoring and reporting on risks and treatments, communicating and consulting about new and emergent risks, and sharing experiences so that the overall process improves.

ERM means Enterprise Risk Management.

Enterprise Risk Management is the management of all risks within council, not just insurable risks or occupational health and safety.

Enterprise Risk Management Framework is a set of components that provides the foundations and organisational arrangements for designing, implementing, undertaking, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk Appetite is the amount and type of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time. It is expressed in the form of a risk appetite statement that covers Council's critical risk categories.

Risk Tolerance is the organisations or stakeholders readiness to bear the risk after risk controls are in place in order to achieve its objectives.

Regulatory compliance involves adherence to laws, regulations, guidelines and specifications relevant to an organisation's or individual's activities.

Related resources

26. Legislation:

- a) Local Government Act 1993; and
- b) Local Government (General) Regulations 2005.

27. Associated Documents:

- a) Code of Conduct;
- b) Procedures for the Administration of the Code of Conduct; and
- c) Equity, Diversity and Respect Policy.
- d) AS ISO 31000 2018 Standard for Enterprise Risk Management

History of revisions

| Amendment history | Details |
|--|---|
| <p>Original approval authority details</p> <p>May 2018</p> | <p>Acting Chief Executive Officer</p> <p>The purpose of this Enterprise Risk Management (ERM) Policy is to communicate Council's commitment to managing enterprise-wide risks and to establish clear expectations to ensure that all staff are aware of their responsibilities for identifying and managing risk.</p> |
| <p>January 2019</p> | <p>D13443402</p> <p><i>Minor amendments to policy following internal feedback</i></p> |
| <p>April 2021</p> | <p>D14582043</p> <p><i>Standard Review, minor amendments and update to current policy format</i></p> |