



POLICY NO: CCC032

POLICY FOR ENTERPRISE RISK MANAGEMENT FRAMEWORK

May 2018

| | |
|--------------------------------|--|
| AUTHORITY | NAME & TITLE |
| AUTHOR | Stephen Bignill, Project Manager |
| MANAGER | James Taylor, Acting Unit Manager Governance and Business Services |
| EXECUTIVE LEADER | Shane Sullivan, Acting Executive Manager Governance |
| CHIEF EXECUTIVE OFFICER | Brian Glendenning, Acting Chief Executive Officer |

History of Revisions:

| Version | Date | Reason | TRIM Doc. # |
|----------------|--------------|--|--------------------|
| 1 | May 2018 | Creation of Policy | |
| 2 | January 2019 | Minor amendments to policy following internal feedback | D13443402 |

Table of Contents

| | |
|--------------------------------|-------------------------------------|
| SUMMARY | 4 |
| POLICY BACKGROUND | 4 |
| POLICY STATEMENT | 4 |
| PURPOSE | 5 |
| BREACHES | 7 |
| DEFINITIONS | 7 |
| RELATED RESOURCES..... | <i>Error! Bookmark not defined.</i> |

SUMMARY

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.

POLICY BACKGROUND

2. 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.
3. 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.

POLICY STATEMENT

Jurisdiction

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

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.

PURPOSE

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 will enable:
 - a) formal, structured approach to risk management that is appropriate to CCC's activities and operating environment; and
 - b) risk management approach consistent with the principles of AS ISO 31000:2018.
13. CCC's current risk appetite statement 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.
14. 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; and
 - h) is dynamic, iterative and facilitates continual improvement.
15. Council is ultimately responsible for committing to this risk management policy and fully considering risk management matters contained in Council reports.

- 16.** 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.
- 17.** The Executive Leadership Team is responsible for considering urgent, sensitive and/or complex risk management issues that cannot be resolved by staff.
- 18.** 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.
- 19.** 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.
- 20.** The Section Manager Insurance and Risk 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; and
 - g) ensuring a consistent approach to ERM throughout Council
- 21.** 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; and
 - f) facilitating the formal review and update of the ERM Framework.

- 22. 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.
- 23. This policy will be reviewed within 12 months of the completion of the Enterprise Risk Management Framework Project, and two years thereafter, or more frequently in the event of a material change in circumstances.

BREACHES

- 24. Suspected breaches or misuse of this policy are to be reported to the Chief Executive Officer.
- 25. 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.

DEFINITIONS

- 26. Code of Conduct means the Code of Conduct adopted by Council
- 27. Council means Central Coast Council
- 28. Act means the Local government Act
- 29. Council staff means employee of Council and includes the Chief Executive Officer
- 30. Mayor means the person elected as the Mayor of the Council
- 31. Values and Behaviours mean the common set of Values and Behaviours adopted by Council. There are five Values and fourteen supporting Behaviours.

| | |
|---------|--|
| Serve | Deliver amazing services through empowering people; and Pursue collaborative partnerships for better community outcomes. |
| Improve | Look for better ways of doing things; and Encourage participation and new ideas. |

| | |
|--------------|---|
| Collaborate | Build relationships based on mutual trust; Share ideas, talent, skills and knowledge; Actively listen to find the best overall outcome; and Demonstrate care and respect for ourselves and each other. |
| Be Your Best | Strive to be your best every day; Promote self-awareness and development; Open to continual learning and improvement; and Take personal responsibility for actions and decisions. |
| Be Positive | Celebrate having a go; and Build one team spirit. |



- 32.** Risk is the effect of uncertainty on objectives – it can be positive or negative
- 33.** 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.
- 34.** ERM means Enterprise Risk Management
- 35.** Enterprise Risk Management is the management of all risks within council, not just insurable risks or occupational health and safety (DLG Internal Audit Guidelines, September 2010).
- 36.** 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.
- 37.** 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.
- 38.** Risk Tolerance is the organisations or stakeholders readiness to bear the risk after risk controls are in place in order to achieve its objectives;

- 39.** Regulatory compliance involves adherence to laws, regulations, guidelines and specifications relevant to an organisation's or individuals activities.

RELATED RESOURCES

- 40.** Legislation:

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

- 41.** Associated Documents:

- a) Code of Conduct;
- b) Procedures for the Administration of the Code of Conduct; and
- c) Equity, Diversity and Respect Policy.