City of Newcastle

Policy

Enterprise Risk Management

March 2019

PO Box 489, Newcastle NSW 2300
Ph: 4974 2000 Fax: 4974 2222
Email: mail@ncc.nsw.gov.au
www.newcastle.nsw.gov.au

City of Newcastle

Table of Contents

Part A Preliminary

1 Commitment and mandate

1.1 CN's CEO and ELT are committed to good corporate governance and creating a positive organisational culture that promotes risk management acceptance, communication and management of appropriate risk at all levels of the organisation.

1.2 CN's approach to risk is integrated into the organisation's core business and embedded within planning and decision-making processes and operational procedures. CN requires a strong risk culture to enable it to deliver its vision and purpose. All staff are responsible for the proactive identification, escalation and management of risk.

2 Background and introduction

2.1 CN faces significant internal and external factors and influences that create uncertainty. This uncertainty can impact on the extent that we achieve our objectives in delivering services for our community. The effect this uncertainty has on our objectives is referred to as 'risk'.

2.2 CN recognises that risk management is an integral part of good governance and management practice with the organisation needing to provide assurance to the community that it is operating effectively and efficiently. Managing risk is iterative and assists CN in setting strategy, achieving objectives and making informed decisions. CN's operations span a wide spectrum of disciplines, fields and environments. This diversity of activity creates an equally diverse and complex range of risks as well as a wealth of opportunities for CN. To ensure that we are achieving our objectives, we need to monitor our risks and their controls in a consistent and systematic manner.

2.3 CN's ERM Framework provides a foundation for responding to uncertainty through a structured and consistent approach. This approach facilitates risk-informed decision making aligned with our strategic, operational and project-specific objectives. The ERM Framework integrates the processes for managing risks and controls into CN's overall governance, strategy and planning, performance improvement, reporting processes, policies, values and culture. The ERM Framework takes into account the internal and external context in which CN operates. The ERM Framework compromises:

2.3.1 **This Policy**: to formally outline policy principles and commitment.

2.3.2 **Risk Management Guideline and supporting tools**: designed to be read in conjunction with this Policy and to guide, direct and assist everyone to better understand the principles of risk management and to adopt consistent processes for managing risks.

2.3.3 **Risk Register**: principle repository for risks across CN. The Risk Register enables areas to analyse risks, monitor controls and prioritise treatment actions. The Risk Register is captured in an online database which also facilitates standardised reporting of risks.

2.3.4 **Governance and Risk Executive Committee**: responsible for oversight of risk management across CN.

3 Context

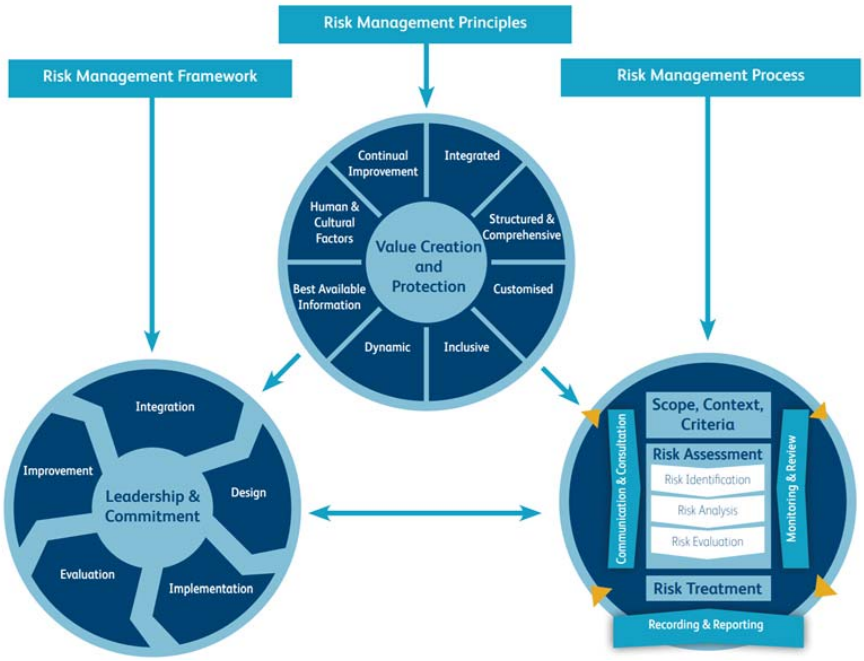
3.1 CN's approach to risk management is aligned to the AS/NZS ISO 31000:2018 Risk management – Guidelines. The three key components within the standard for managing risk are as follows:

3.1.1 Principles that need to be satisfied before risk management is effective;

3.1.2 A framework that integrates the principles for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture; and thirdly.

3.1.3 An effective process that can be applied across an entire organisation, to its many areas and management levels, as well to specific functions, projects and activities.

3.2 The inter-relationship between the three components is illustrated in the diagram below.



.

4 Purpose

4.1 The purpose of this Policy and the ERM Framework is to:

4.1.1 support a consistent, effective and structured approach to the management of risk at CN; and

4.1.2 support CN to achieve its objectives and embed risk management in all strategic and operational processes.

4.2 This in turn provides a framework for:

4.2.1 encouraging understanding by staff of the implications of risk as well as risk management opportunities;

4.2.2 Councillors and staff at CN making informed business decisions based on appropriate risk assessments and established risk appetite;

4.2.3 everyone at CN applying risk management to their day to day work activities;

4.2.4 defining and documenting responsibilities, processes and reporting lines;

4.2.5 risks being identified, prioritised and managed in a coordinated manner;

4.2.6 improvements to strategic planning processes as a result of a structured consideration of risk;

4.2.7 compliance with relevant legislation; and

4.2.8 resources being safeguarded (for example: people, finance, property and reputation).

5 Scope

5.1 Risk management applies and incorporates risk responsibility into all areas of the CN's operations.

This policy does not apply to the management of individual work, health and safety risks (WHS) which are managed within CN's WHS system.

6 Principles

6.1 The standard AS/NZS ISO 31000:2018 Risk management - Guidelines states that the purpose of risk management is the creation and protection of value. The principles provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The eight principles identified in the standard are illustrated in the following diagram;

6.2 CN commits itself to the following principles which provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose.

Principle	Description

Integrated	Risk management is an integral part of all CN activities and supports evidence-based decision making.
Structured and Comprehensive	CN's ERM Framework has a structured and comprehensive approach to risk management (supported by integrated software) which contributes to consistent and comparable results.
Customised	The ERM Framework is customised taking into account CN's external and internal context relative to core objectives.
Inclusive	Appropriate and timely involvement of all areas of CN enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
Dynamic	Risks can emerge, change or disappear as CN's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
Best Available Information	The inputs for risk management are based on historical and current information as well as future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
Human and cultural factors	It is acknowledged that human behaviour and culture significantly influence all aspects of risk management at each level and stage.
Continual Improvement	Risk management is continually improved through learning and experience.

6.3 The effectiveness of risk management depends on its active integration of all aspects of the organisation into decision making. The standard AS/NZS ISO 31000:2018 Risk management - Guidelines provides that the components of leadership, integration, design, implementation, evaluation and improvement are needed to deliver effective risk-based decision-making capability as illustrated in the following diagram:

6.4 CN is committed to these components which are described below:

Leadership & Commitment	ELT and risk oversight committees (for example - Governance and Risk (Executive) Committee) ensure that risk management is integrated into all organisational activities and should proactively demonstrate risk leadership and commitment to the organisation.
Integration	Integrating risk management into CN is a dynamic and iterative process, and is customised to CN's needs and culture. Risk management is part of, and not separate from, CN's organisational purpose, governance, leadership and commitment, strategy, objectives and operations.
Design	The ERM Framework is designed to: examine and understand its external and internal context articulate risk management commitment assign appropriate organisational roles and responsibilities facilitate the appropriate allocation of resources establish communication in order to support the framework and facilitate the effective application of risk management
Implementation	The ERM Framework ensures that the risk management process is a part of all activities throughout the organisation including decision making and that the changes in external and internal contexts will be adequately covered.
Evaluation	CN will periodically measure performance against its purpose, objectives and implementation plans.
Improvement	CN will continually improve and adapt the ERM Framework to ensure that risk management is continually enhanced.

7 Integration with Strategic and Business Planning

7.1 Risk is fundamentally linked to the objectives and processes in our strategic and business planning. Through identification, assessment, evaluation and, where

appropriate, additional treatments to controls, opportunities can be maximised whilst also minimising the severity of adverse consequences. Failure to incorporate risk management in the integrated planning and reporting process (IP&R) significantly reduces its effectiveness.

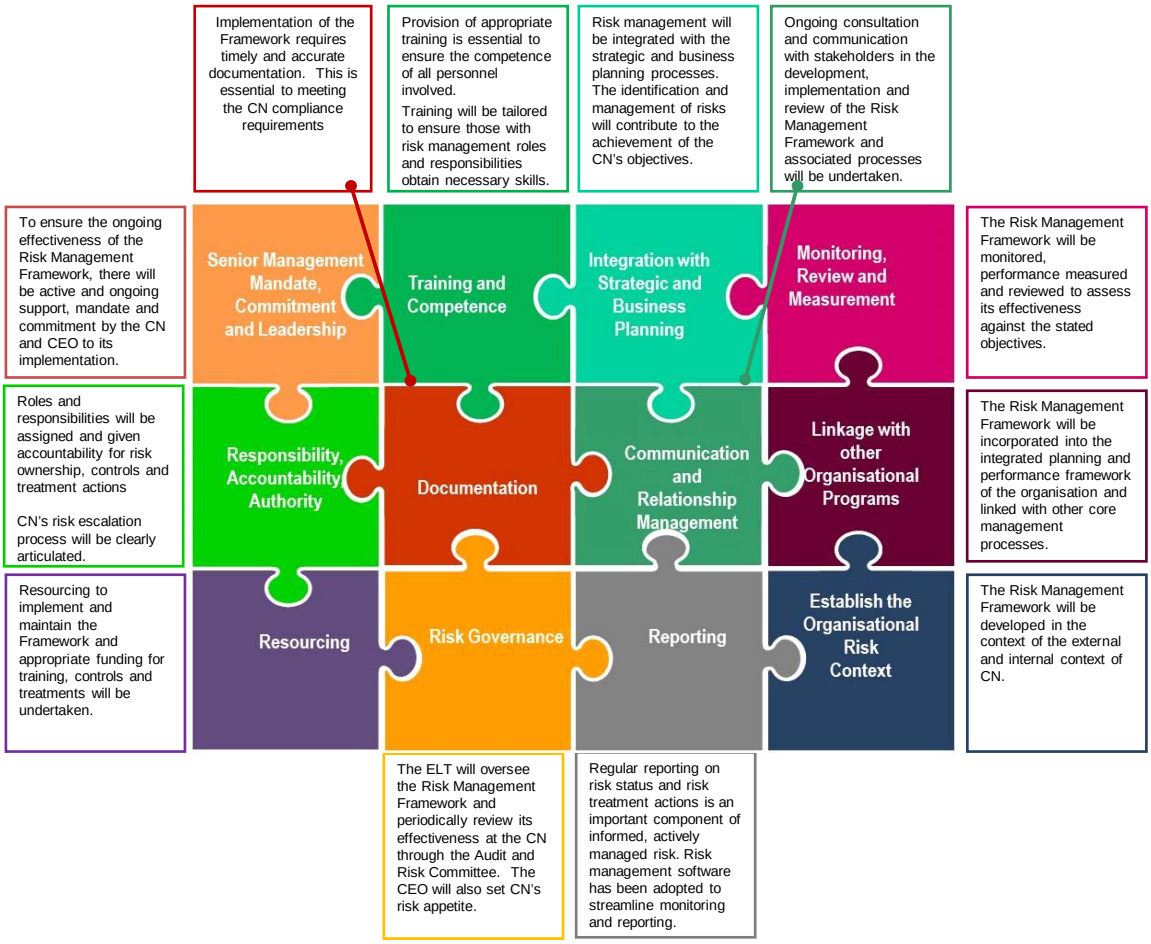
7.2 CN has a tiered structure of externally and internally focused plans and strategies that align with the IP&R framework. These documents include plans for the community, resourcing strategies, delivery and operational plans, service unit and project plans and many other strategies and plans to facilitate CN's capability and capacity to serve the community.

7.3 Through managing risk associated with these strategies and plans in accordance with the ERM Framework, CN is better positioned to deliver to our community.

Part B CN's Risk Management model

8 Integrated approach

8.1 CN's approach to risk management is integrated:



9 Risk culture

9.1 Embedding risk management into the organisational culture is fundamental to achieving integrated risk management. This will be accomplished by:

9.1.1 Directors and Managers championing risk management behaviours and actions;

9.1.2 Promoting the view that all staff are managers of risk;

9.1.3 Encouraging staff to develop knowledge and skills in risk management;

9.1.4 Ensuring policies and procedures incorporate risk management at all stages;

9.1.5 Including risk management in our induction program, and ongoing training program; and

9.1.6 Providing targeted training and support to staff so that risk management practices are effectively incorporated into their everyday roles and responsibilities.

9.2 We recognise that a proactive risk management culture is necessary to effectively respond to unexpected events. Therefore, successful risk management requires

involvement by all staff. An organisational culture that supports effective risk management is one where:

9.2.1 A “no surprises” rather than “no risks” philosophy is encouraged;

9.2.2 Individuals are encouraged to identify and respond to risks without fear of retribution;

9.2.3 Individuals are encouraged to challenge and debate risk responses in a respectful and constructive manner; and

9.2.4 There is a common risk language that facilitates clear and consistent discussion of risks affecting CN.

10 Risk types

10.1 CN recognises that there is the potential for risks in various aspects of operations. However, it is also important to consider the potential opportunities or benefits that can be achieved. The ERM Framework describes the process for managing risk. It provides a structure for a consistent approach to identifying and categorising risk.

The ERM Framework accommodates strategic, operational, fraud and corruption and project risks.

10.1.1 **Strategic risks** are those risks that apply to CN as a whole and could adversely affect the achievement of our strategic outcomes and/or damage CN’s reputation. These risks are managed by ELT.

10.1.2 **Operational risks** relate to the risks that may impact delivery of specific services and programs and are managed by the relevant Service Unit.

10.1.3 **Fraud and corruption risks** relate to dishonest or fraudulent behaviour. CN is committed to deterring and preventing such behaviour with control measures set out in its Fraud and Corruption Control Plan. The risks are managed by ELT.

10.1.4 **Project risks** may affect the delivery of a project on time, within budget, or within acceptable quality parameters. They are managed by the project manager in consultation with the project sponsor. CN’s Project Management Policy includes risk assessment and management criteria, and all projects have a Risk Register that is documented during the planning phase, monitored during program development and reviewed at the project finalisation stage.

11 Risk management process

11.1 The risk management process, as defined by AS/NZS ISO 31000:2018 Risk management – Guidelines involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

This process can be represented by the diagram below.

11.2 The process involves:

11.2.1 **Communication and consultation** – a consultative approach involving all relevant stakeholders will help to better define the context for the risk assessment and provide greater confidence that all risks are identified. It will promote ownership of the risk assessment, an appreciation of the benefits of the risk controls, and support for the risk assessment plan.

Effective risk communication will ensure that those responsible for implementing risk management and those with a vested interest, understand the basis on which risk management decisions are made and why particular actions are required.

11.2.2 **Establishing the scope, context and criteria** – establish the external, internal, and risk management context in which the rest of the risk management process will take place. By establishing the context, scope and criteria CN articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. In defining its ERM Framework and risk management approach, CN has considered its:

Internal context:

- governance, organisational structure, roles and accountabilities;
- policies, objectives, and strategies;
- resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- relationships with and perceptions and values of internal stakeholders;
- organisational culture;
- information systems, information flows and decision-making processes (both formal and informal);
- standards, guidelines and models adopted by CN; and
- form and extent of contractual relationships.

External context:

- social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment (international, national, regional and local);
- key drivers and trends which impact on CN's objectives; and
- relationships with, perceptions and values of the community and its stakeholders.

11.2.3 **Risk assessment** – risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

11.2.4 **Risk identification** – the aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Risk identification is the process of identifying risks having an effect on the achievement of our objectives. Comprehensive identification using a well-structured systematic process is critical, because a risk not identified at this stage may be excluded from further analysis.

11.2.5 **Risk analysis** – risk is analysed by determining consequences and their likelihood, and other attributes of the risk. It provides an input to risk evaluation, decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

11.2.6 **Risk evaluation** – involves comparing the level of risk with risk criteria and making decisions about which risks need treatment, and the priority for treatment implementation, taking into account CN's agreed risk appetite.

11.2.7 **Risk treatment** – risk treatment involves selecting one or more options for modifying risks and implementing those options. When implemented, treatments provide or modify the controls.

11.2.8 **Monitoring and review** – risks and the effectiveness of controls and risk treatments need to be monitored, reviewed and reported to ensure changing context and circumstances do not alter priorities.

11.2.9 **Recording and Reporting** - consistent, comprehensive and timely risk reporting is critical to provide management with the opportunity to monitor risks, and to inform decision making

12 Risk register

12.1 CN maintains a Risk Register to record key risk events that would likely impact the achievement of objectives.

12.2 All risks, controls and treatments will be assigned risk owners within the Risk Register.

13 Risk appetite

13.1 The ISO Guide 73:2009, Risk Management – Vocabulary defines Risk Appetite as "*The amount and type of risk that an organisation is willing to pursue or retain*".

13.2 For this reason, the risk appetite for residual risk has been identified for each Impact Category for CN.

13.3 The level of risk CN is prepared to accept in each risk category is detailed on Appendix E of the ERM Guideline.

14 Escalation of risks

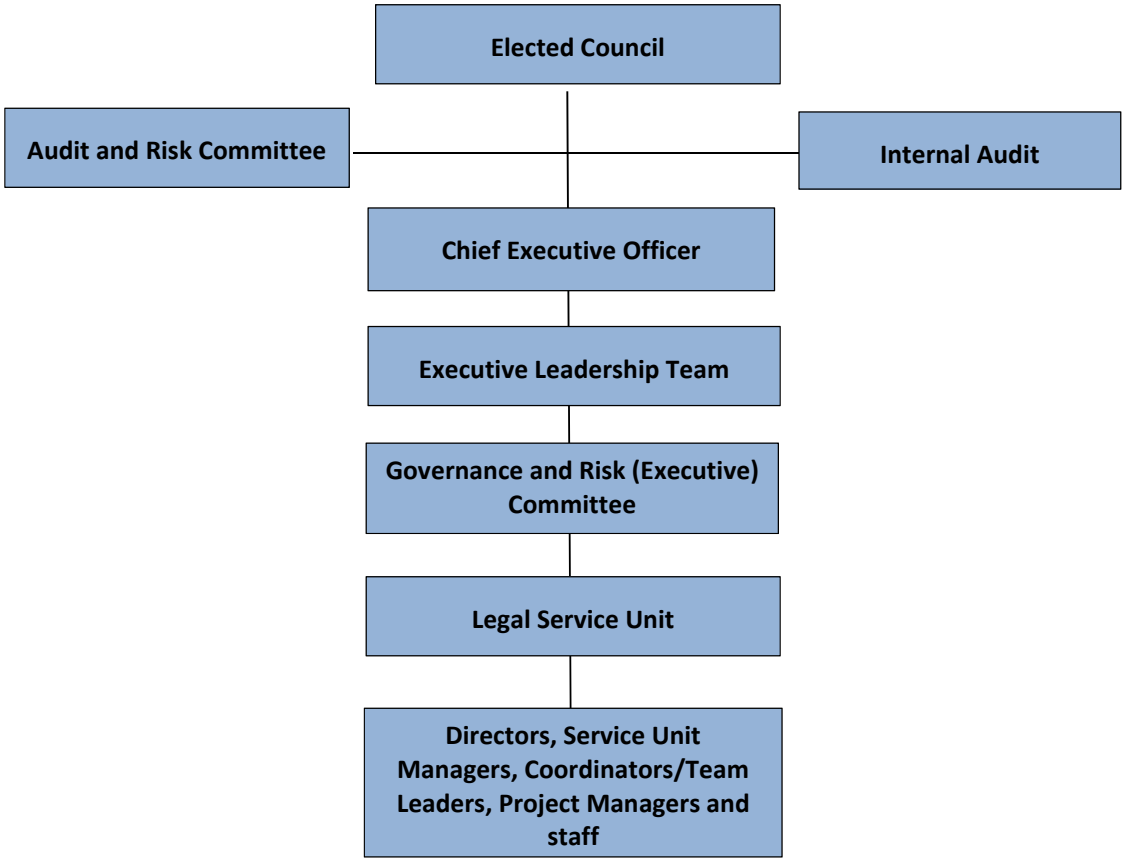
14.1 Risk Owners may manage risks where the residual risk falls within the agreed risk appetite.

14.2 Risks will be escalated in accordance with the CN Risk Escalation table and process detailed in Appendix G of the ERM Guideline.

Part C Roles, responsibilities and resourcing

15 Roles, responsibilities, accountability and authority

15.1 Risk management is considered an integral part of all management and decision-making functions:



The following table summarises the key risk management roles and responsibilities in the organisation.

Role	Responsibilities
Elected Council	Consider risk as an integral part of decision making consistent with its functions under the Local Government Act 1993.
Audit and Risk Committee	Provide independent assurance, advice and assistance to CN on risk management, control, governance, and external accountability responsibilities as defined in the Audit and Risk Committee Charter.
Internal Audit	Plan, perform and oversee the delivery of the CN's Internal Audit Program. Monitor and track the status of Agreed Management Actions and report on these to the Audit and Risk Committee / ELT. Consult and collaborate across CN to ensure the ERM Framework is applied in a consistent and effective way. Continually promote a positive "no blame" risk culture aware across CN. In consultation with the Risk Management Coordinator, review the CN Risk Register to ensure risks are appropriately articulated and assessed, and that treatments are sufficiently defined with risk owners and due dates. Facilitate sharing of risk management "best practices" across CN.
CEO (Level 1)	Lead the development of a 'no-blame' risk aware culture across CN. Set CN's risk appetite and tolerance levels. Approve this Policy and the ERM Framework. Monitor and receive reports on CN's risks and their management.
ELT	Lead the development of a 'no-blame' risk aware culture across CN. Champion, participate in, communicate and demonstrate support for risk management. Communicate CN's risk appetite and tolerance. Assess and manage strategic risks, including the assessment of emerging strategic risks within CN and the local government sector to ensure that appropriate action is being taken. Provide direction regarding responses to strategic, operational and project risks, as required. Monitor risks associated with strategic projects.

Role	Responsibilities
	Provide direction to the Governance Risk (Executive) Committee (GREC) Provide direction in response to reports and recommendations provided by the GREC where appropriate. Resolve urgent, sensitive, complex or CN-wide risk management issues that cannot be resolved by staff.
Governance and Risk (Executive) Committee (GREC)	Facilitate the implementation and priority setting of the ERM Framework and the development of a 'no blame' risk aware culture. Oversight of the effective implementation and operation of CN's ERM Framework. Facilitate training and development needs to achieve the required risk management competencies across CN where appropriate. Facilitate the formal review and update of the ERM Framework. Sponsor initiatives to support the ERM Framework across CN.
Legal Service Unit	Lead the development of a 'no-blame' risk aware culture across CN. Provide specialist risk management support and training to staff to ensure a consistent risk management approach across CN. Facilitate the progressive implementation of the ERM Framework and the development of a risk-aware culture. Promote the communication of risks within and between our various Service Units and Directorates. Maintain our Risk Register in a consistent and accessible form – providing quality information as a basis for effective risk management across CN. Review the CN Risk Register to ensure risks are appropriately articulated and assessed, and that treatments are sufficiently defined with risk owners and due dates. Identify opportunities for improvement of the ERM Framework. Review ERM Framework implementation and operational effectiveness and provide associated reports and recommendations to the GREC. Collaborate with Emergency Management during significant events that impact on the ERM Framework. Provide Risk Status Reports to the Audit and Risk Committee. Develop strategies for the management of emergency and disaster risks and document these.

Role	Responsibilities
Directors (Level 2)	Lead the development of a 'no-blame' risk aware culture across CN. Ensure the ERM Framework is being effectively implemented and operated within their areas of responsibility. Participate in strategic, operational and project risk assessments including collaboration with Emergency Management during significant events. Manage operational risks within their Directorate. Promote a culture that encourages the open and transparent discussion of risk. Escalate extreme risks to the CEO as appropriate in accordance with the established risk appetite.
Service Unit Managers (Level 3)	Lead the development of a 'no-blame' risk aware culture across CN. Ensure that the ERM Framework is being effectively implemented and operated within their areas of responsibility. Participate in operational and project risk assessments including collaboration with Emergency Management during significant events. Manage risks (including controls and control effectiveness) within the Service Unit and accordance with established risk appetite. Develop strategies for the management of applicable operational risks and document these strategies in the Service Unit Plan. Report quarterly on operational risks to their Director. Escalate medium/high risks to the Director as appropriate in accordance with the established risk appetite.
Coordinators and Team Leaders (Level 4 and 5)	Lead a culture of 'no-blame' risk awareness across CN. Manage risks (including controls and control effectiveness) within the Service Element and accordance with established risk appetite. Escalate risks to the Service Unit Manager as appropriate in accordance with the established risk appetite.
Project Managers	In accordance with the Project Management Policy: • Develop strategies for the management of project risks and document these strategies in the project plan. • Include project-specific risk management requirements and methodology in the project plan.

Role	Responsibilities
	• Ensure the effective management of risks within the project team to support the achievement of project objectives. • Escalate risks to the Project Control Group, the Project Sponsor or the ELT (where required).
People and Culture	Facilitate a risk management training program
Staff	Proactive identification, escalation and management of risk in accordance with this Policy and the ERM Framework.

16 Resourcing

Risk management is adequately resourced as follows:

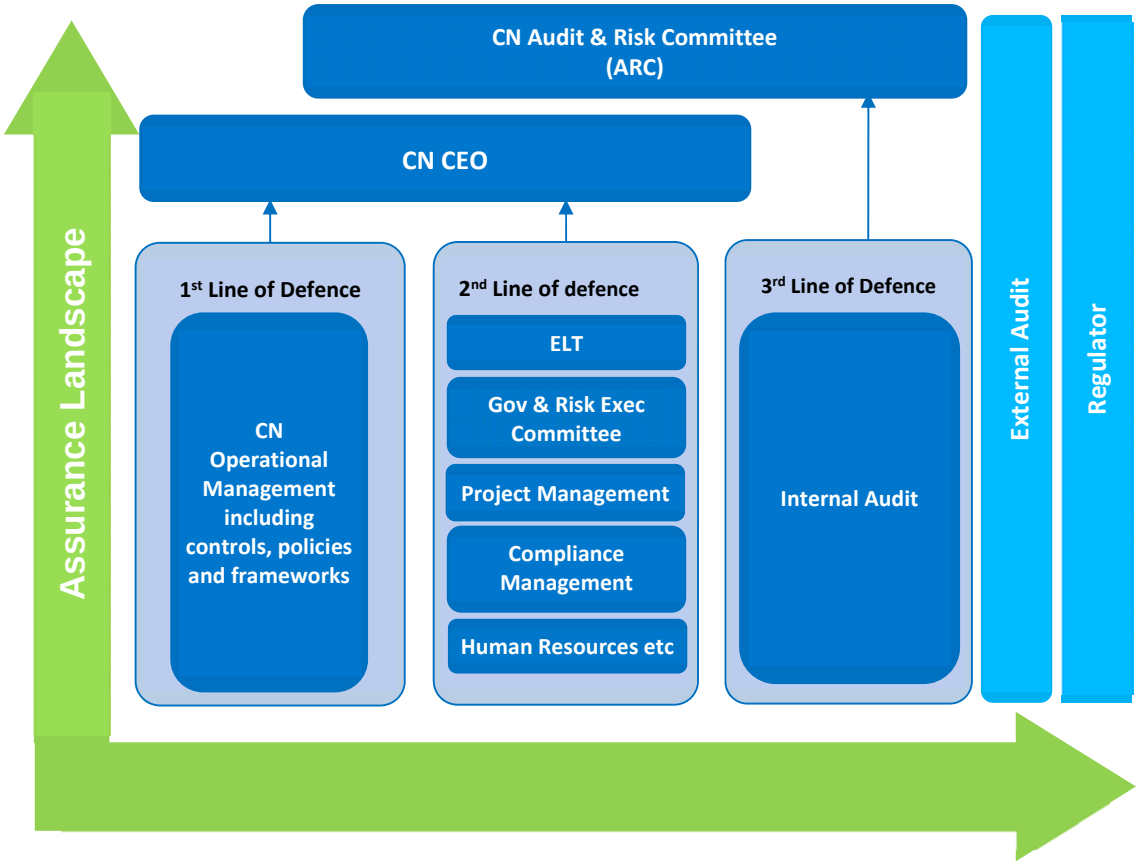
Area	Resource Requirements	Budget
Risk Treatment Actions	Internal Resources	Operational and Capital Budgets
Risk Management Training	External and Internal Training Resources	Operational Budget
Risk Management Framework Audit	External Provider	Operational Budget
Risk Management System	Internal and External Providers	Operational Budget

Part D Assurance/defence

17 Lines of assurance/defence

17.1 The community, all at CN and other stakeholders need assurance that CN is managing its threats and leveraging its opportunities to achieve objectives. A robust ERM Framework ensures these threats and opportunities are addressed in a methodical and consistent way.

17.2 Assurance over the robustness of the ERM Policy and Framework is achieved through the 'three lines of assurance' model maintained by CN as part of its framework of internal controls, as follows:



Part E Definitions

CEO means Chief Executive Officer of the City of Newcastle and includes their delegate or authorised representative.

References to the Chief Executive Officer are references to the General Manager appointed under the Local Government Act 1993 (NSW).

City of Newcastle (CN) means Newcastle City Council.

References to City of Newcastle are references to Newcastle City Council as prescribed under the Local Government Act 1993 (NSW).

ELT means Executive Leadership Team.

ERM Framework means Enterprise Risk Management Framework.

Risk Owners means staff members assigned within the Risk Register as responsible for risk/s. Risk may only be assigned to Management Levels 1- 5.

Unless stated otherwise, a reference to a section or clause is a reference to a section or clause of this Policy.

Document Control

Policy title	Enterprise Risk Management Policy
Policy owner	Director Governance / Manager Legal
Policy expert/writer	Risk Management Coordinator
Associated Procedure Title (if applicable)	NIL
Procedure owner (if applicable)	NIL
Prepared by	Governance
Approved by	CEO
Date approved	14/03/2019
Policy approval form reference	ECM# 5909005
Commencement Date	14/03/2019
Next revision date (date policy will be revised)	14/03/2021
Termination date	14/03/2022 (one year post revision date)
Version	1
Category	Governance
Keywords	Enterprise, risk, management, framework, ERM Framework
Details of previous versions	NIL
Legislative amendments	NIL
Relevant strategic direction	Open and Collaborative Leadership
Relevant strategy	Open and Transparent Governance Strategy
Relevant legislation/codes (reference specific sections)	*AS/NZS ISO 31000:2018 Risk Management – Guidelines* - *HB 158:2010 Delivering assurance* based on *ISO 31000:2009 Risk management—principles and guidelines.* - ISO Guide 73:2009 - *Internal Audit Guidelines* (2010), Division of Local Government, NSW Department of Premier and Cabinet
Other related policies/ documents/ strategies	Project Management Policy
Related forms	NIL
Required on website	Yes
Authorisations	Refer Part C