Enterprise Risk Management Policy

July 2022

newcastle.nsw.gov.au

City of Newcastle

Table of Contents

Commitment and mandate **3**

Part A Preliminary 4

1. Purpose 4

2. Scope 4

3. Principles 4

Part B – Framework details 6

4. ERM Framework 6

5. Background 6

6. Context 6

7. Risk types 7

8. Integration with Strategic and Business Planning 8

Part C CN's Risk Management model 9

9. Integrated approach 9

10. Risk culture 9

11. Risk Appetite and Risk tolerance 10

12. Escalation of risks 10

Part D Roles, responsibilities and resourcing 11

13. Roles, responsibilities, accountability and authority 11

14. The Three Lines Model 13

15. Resourcing 14

Annexure A - Definitions 15

Annexure B - Policy Authorisations 16

Document Control 17

Commitment and mandate

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 throughout the organisation.

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

CN's ERM and Corporate Governance Frameworks are the totality of systems, structures, policies, processes and people within CN that identify, measure, monitor, report and control or mitigate all internal and external sources of strategic, operational and emerging risks and includes CN's Risk Appetite Statement and risk and governance culture.

Part A Preliminary

1 Purpose

1.1 The purpose of this Policy is to support a consistent, effective and structured approach to the management of risk at City of Newcastle (CN); and support CN to achieve its objectives and embed risk management in all strategic and operational processes.

This in turn provides a framework for:

1.1.1 Encouraging understanding by staff of the implications of risk as well as risk management opportunities;

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

1.1.3 All CN staff applying risk management to their day-to-day work activities;

1.1.4 Defining and documenting responsibilities, processes and reporting lines;

1.1.5 Risks being identified, prioritised and managed in a coordinated manner;

1.1.6 Improvements to strategic planning processes as a result of a structured consideration of risk;

1.1.7 Compliance with relevant legislation and the Australian Standards ISO 31000.2019; and

1.1.8 Resources being safeguarded (for example: people, finance, property and reputation).

2 Scope

2.1 This Policy applies to all CN staff. Risk management applies, and incorporates, risk responsibility into all areas of CN's operations.

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

3 Principles

3.1 The *Australian Standards for Risk Management* 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.

CN commits itself to the following **principles:**

3.1.1 **Integrated** - Risk management is an integral part of all CN activities and supports evidence-based decision making.

3.1.2 **Structured and comprehensive** - CN's ERM Framework has a structured and comprehensive approach to risk management.

3.1.3 **Customised** - The ERM Framework is customised considering CN's external and internal context relative to core objectives.

3.1.4 **Inclusive** - Appropriate and timely involvement of all CN staff enables knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

3.1.5 **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.

3.1.6 **Best available information** - The inputs for risk management are based on historical and current information as well as future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

3.1.7 **Human and cultural factors** - It is acknowledged that human behaviour and culture significantly influence all aspects of risk management at each level and stage.

3.1.8 **Continual improvement** - Risk management is continually improved through learning and experience.

Part B – Framework details

4 ERM Framework

4.1 CN's ERM Framework compromises:

4.1.1 **This Policy:** To formally outline policy principles and commitment.

4.1.2 **CN Risk Appetite Statement:** An appropriate risk appetite enhances decision-making and facilitates efficient distribution of an organisation's resources to achieve its goals and objectives. A considered and tailored Risk Appetite Statement is a key component of CN's ERM Framework.

4.1.3 **ERM Guideline and supporting tools:** The ERM Guideline and supporting tools are designed to guide, direct and assist CN staff to better understand the principles of risk management and to adopt consistent processes for managing risks. They are updated as required to reflect the current CN environment.

4.1.4 **Risk Register:** CN captures corporate risks electronically in CAMMS. The Risk Register enables areas to analyse risks, monitor controls, prioritise treatment actions and standardise reporting.

4.1.5 **Emerging Risk Framework:** This framework is currently under development.

4.1.6 **Governance and Risk (Executive) Committee (GREC):** The purpose of GREC is to provide oversight and guidance to the CEO and Executive Leadership Team (ELT) to fulfil their responsibilities for CN's ERM and Corporate Governance Framework.

4.1.7 **Audit, Risk and Improvement Committee (ARIC):** The objective of the ARIC is to provide independent assurance and assistance to CN on risk management, control, governance, and legal and regulatory obligations. The Audit and Risk Committee provides a reporting forum for internal and external auditors. The Committee cannot make decisions on behalf of CN and may not direct any CN officer in his or her duties.

5 Background

5.1 CN recognises that robust risk management is integral to good governance and management practice with CN needing to provide assurance to the community that we are operating effectively and efficiently.

5.2 CN's operations span a wide spectrum of disciplines, fields and environments that create a diverse and complex range of risks as well as opportunities for CN. To ensure that we are achieving our objectives, CN monitors risks and their controls in a consistent and systematic manner according to CN's ERM Framework. The ERM Framework, integrates the processes for managing risks into CN's overall governance, strategy and planning.

6 Context

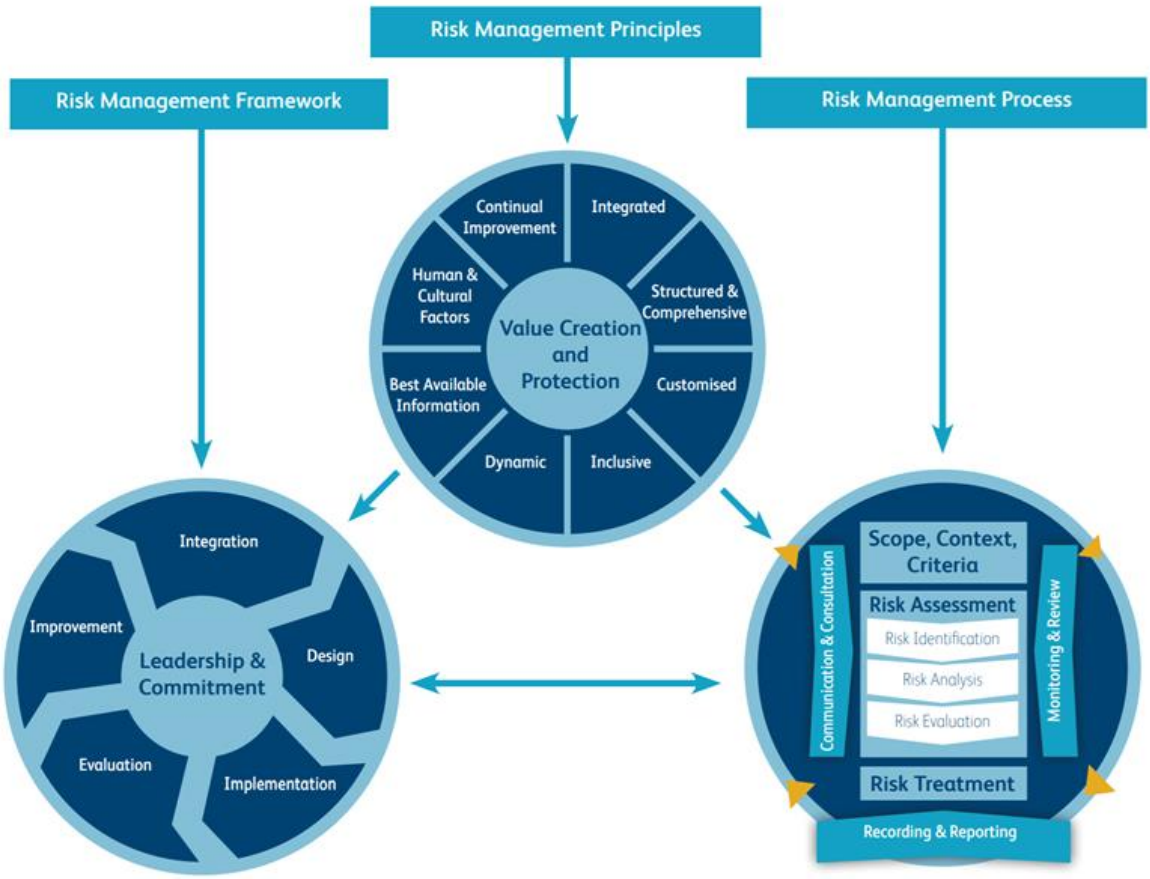
6.1 CN's approach to risk management is aligned to the *Australian Standards for Risk Management*. The three key components within the standard for managing risk are:

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

6.1.2 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

6.1.3 An effective **Process** that can be applied across CN to its many areas and management levels, as well to specific functions, projects and activities.

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



7 Risk types

7.1 CN recognises that there is the potential for risks (and potential opportunities or benefits) in various aspects of operations.

7.2 The ERM Framework accommodates Emerging, Strategic, Operational, Fraud, Project and Cyber Security. These risks are described below.

7.2.1 **Emerging risks** are newly developing risks that cannot yet be fully assessed but that could, in the future, affect the viability of CN's strategy with effective risk management requiring identification of emerging risks.

7.2.2 **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 and owned by the CEO.

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

7.2.4 **Fraud 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.

7.2.5 **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.

7.2.6 **Cyber security** (crown jewels) risks relate to the probability of exposure, loss of critical assets and sensitive information, or reputational harm as a result of a cyberattack or breach within CN’s network.

8 Integration with Strategic and Business Planning

8.1 Risk is fundamentally linked to the objectives and processes in CN's strategic and operational planning. Through identification, assessment, evaluation and, where appropriate, additional treatments to controls, opportunities can be maximised whilst also minimising the severity of adverse consequences.

8.2 Failure to incorporate risk management in the integrated planning and reporting process (IP&R) significantly reduces its effectiveness.

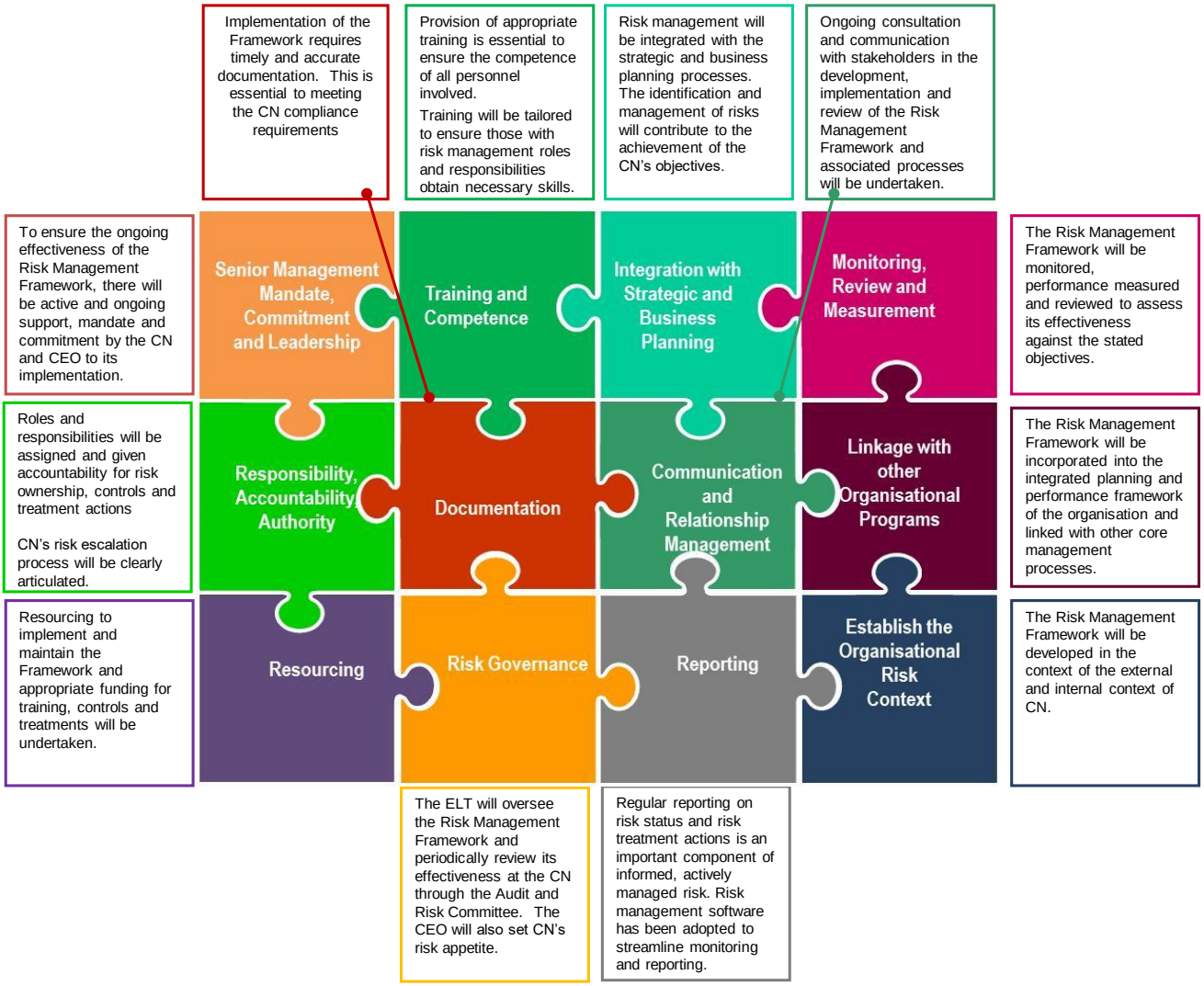
8.3 CN has a tiered structure of externally and internally focused plans and strategies that align with the IP&R framework.

8.4 CN has a structured annual review of Strategic Risks. This is completed in consultation with each of the Responsible Owners which are members of the ELT with all Strategic Risks owned by the CEO.

Part C CN's Risk Management model

9 Integrated approach

CN's approach to risk management is integrated into CN's strategic planning, operational planning, project management and IP&R processes.



10 Risk culture

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

10.1.1 ELT and LT championing risk management behaviours and actions.

10.1.2 All staff owning risk.

10.1.3 Ensuring policies and procedures incorporate risk management.

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

10.2 CN recognises that a proactive risk management culture is necessary to effectively respond to unexpected events. Therefore, successful risk management requires involvement by all staff.

11 Risk Appetite and Risk Tolerance

11.1 Risk appetite enhances decision-making and facilitates efficient distribution of an organisation's resources to achieve its goals and objectives. A considered and tailored risk appetite is a key component of CN's ERM Framework.

11.2 CN's risk appetite is based on a four-level risk scale comprising: Avoid; Resistant; Accept; and Receptive. This scale, together with a structured method of articulating each level of risk appetite, has been applied to CN's Risk Categories.

11.3 While risk appetite provides a general qualitative view of the risks CN is willing to take to achieve its strategic objectives, risk tolerance provides a more specific and measurable indicator.

11.4 Risk tolerance operationalises the statements by using quantitative measures where possible to better enable monitoring and review. It informs expectations for avoiding, mitigating and accepting risk and the actions to be taken or consequence for acting beyond approved tolerances. It represents the limits beyond which CN will not go without specific authorisation from the Chief Executive Officer.

11.5 CN Risk Categories and the level of risk CN is prepared to accept in each Risk Category is detailed in Appendix E of the ERM Guideline.

12 Escalation of risks

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

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

Part D Roles, responsibilities and resourcing

13 Roles, responsibilities, accountability and authority

13.1 Risk management is considered an integral part of all management and decision-making functions.

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

13.2.1 **Elected Council**

Consider risk as an integral part of decision making consistent with its functions under the Local Government Act 1993.

13.2.2 **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.

13.2.3 **Internal Audit**

13.2.3.1 Plan, perform and oversee the delivery of CN's Internal Audit Program.

13.2.3.2 Monitor and track the status of Agreed Audit Actions and report on these to the Audit and Risk Committee, Governance and Executive Leadership Team.

13.2.3.3 Continually promote a positive "no blame" risk aware culture across CN.

13.2.3.4 Facilitate sharing of risk management "best practices" across CN.

13.2.4 **CEO (Level 1)**

13.2.4.1 Lead the development of a "no blame" risk aware culture across CN.

13.2.4.2 Set CN's risk appetite and tolerance levels.

13.2.4.3 Approve this Policy and the ERM Framework.

13.2.4.4 Monitor and received reports on CN's risk and their management.

13.2.5 **Directors (Level 2)**

13.2.5.1 Lead the development of a "no blame" risk aware culture across CN.

13.2.5.2 Champion, participate in, communicate and demonstrate support for risk management.

13.2.5.3 Communicate CN’s risk appetite and tolerances and escalate extreme risks to the CEO as appropriate in accordance with the established risk appetite.

13.2.5.4 Assess and manage strategic risks, including the assessment of emerging to ensure that appropriate action is being taken.

13.2.5.5 Provide direction regarding responses to strategic, operational and project risks, as required.

13.2.5.6 Resolve urgent, sensitive, complex or CN-wide risk management issues that cannot be resolved by staff.

13.2.5.7 Ensure the ERM Framework is being effectively implemented and operated within their areas of responsibility.

13.2.5.8 Collaborate with Emergency Management during significant events.

13.2.6 **Governance and Risk (Executive) Committee (GREC)**

13.2.6.1 The purpose of the Committee is to provide oversight and guidance to the CEO and Let to fulfil their responsibilities for CN's ERM and Corporate Governance Framework.

13.2.6.2 Facilitate the implementation and priority setting of the ERM Framework and the development of a 'no blame' risk aware culture.

13.2.6.3 Oversight of the effective implementation and operation of CN's ERM Framework.

13.2.6.4 Sponsor initiatives to support the ERM Framework across CN.

13.2.7 **Legal Services Unit**

13.2.7.1 Lead the development of a 'no-blame' risk aware culture across CN.

13.2.7.2 Provide specialist risk management support to ensure a consistent risk management approach across CN.

13.2.7.3 Facilitate the progressive implementation of the ERM Framework including opportunities for improvement.

13.2.7.4 Maintain CN's Risk Register in a consistent and accessible form, providing quality information as a basis for effective risk management.

13.2.7.5 In consultation with Internal Audit, 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. Collaborate with Emergency Management during a crisis or emergency.

13.2.7.6 Provide Risk Status Reports to the Audit, Risk and Improvement Committee.

13.2.7.7 Develop strategies for the management of emergency and disaster risks and document these.

13.2.8 **Service Unit Managers (Level 3)**

13.2.8.1 Lead a culture of a "no-blame" risk aware culture across CN.

13.2.8.2 Ensure that the ERM Framework is being effectively implemented and operated within their areas of responsibility.

13.2.8.3 Participate in operational and project risk assessments.

13.2.8.4 Including collaboration with Emergency Management during significant events.

13.2.8.5 Manage risks (including controls and control effectiveness) within the Service Unit and accordance with established risk appetite.

13.2.8.6 Develop strategies for the management of applicable operational.

13.2.8.7 Report as required on operational risks to their Director.

13.2.8.8 Escalate medium/high risks to the Director as appropriate in accordance with the established risk appetite.

13.2.9 **Managers and Coordinators (Level 4 and 5)**

13.2.9.1 Lead a culture of a "no-blame" risk aware culture across CN.

13.2.9.2 Manage risks (including controls and control effectiveness) within the Service Element and accordance with established risk appetite.

13.2.9.3 Escalate risks to the Service Unit Manager as appropriate in accordance with the established risk appetite.

13.2.10 **Project Manager**

13.2.10.1 Develop strategies for the management of project risks and document these strategies in the project plan.

13.2.10.2 Ensure the effective management of risks within the project team to support the achievement of project objectives.

13.2.10.3 Escalate risks to the Project Sponsor or a Director (where required).

13.2.11 **People and Culture**

13.2.11.1 Facilitate a risk management training program where required.

13.2.11.2 Manage WHS and wellbeing risks within CN.

13.2.12 **Staff**

Proactive identification, escalation and management of risk in accordance with this Policy and the ERM Framework.

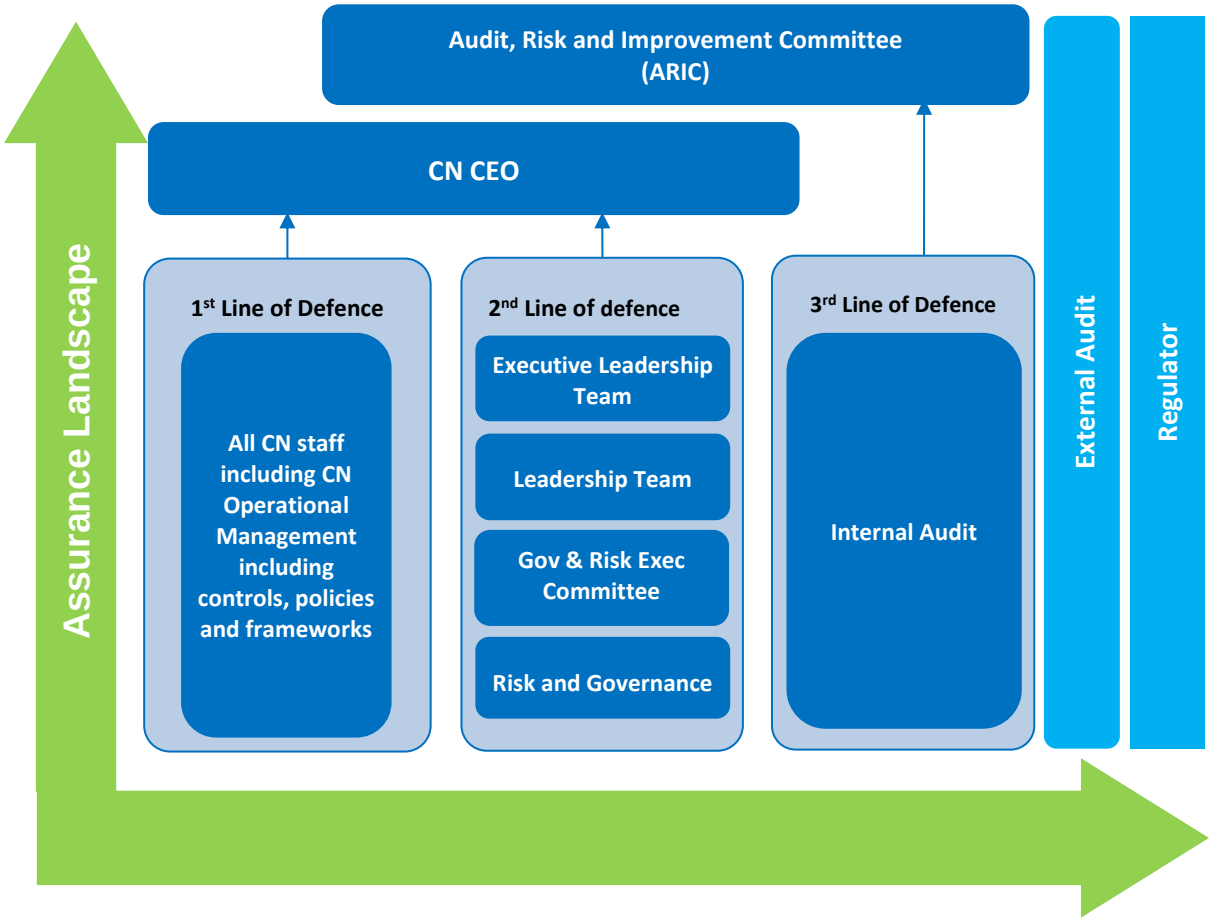
14 The Three Lines Model

14.1 CN has adopted the three lines model as part of its ERM Framework and Corporate Governance Frameworks. The three lines model is implemented as follows:

14.1.1 Risk owners and managers are CN's first line, as they own and manage the risk and are responsible for internal controls.

14.1.2 The Governance and Risk (Executive) Committee and CN's risk management and governance functions are CN's second line, providing a governance and risk compliance and oversight function on behalf of the CEO and ELT.

14.1.3 Internal audit is CN's third line, providing an independent risk assurance function that the risk and governance management and internal control framework is working as designed.



15 Resourcing

Risk management is adequately resourced as follows:

15.1 **Risk Treatment Action**

3.1.9 Internal resources

3.1.10 Operational and capital budgets

3.2 **Risk Management Training**

3.2.1 External and internal training resources

3.2.2 Operational budget

3.3 **Risk Management Framework Audit**

3.3.1 External provider

3.3.2 Operational budget

3.4 **Risk Management System**

3.4.1 Internal and external providers

3.4.2 Operational budget

Annexure A - Definitions

Australian Standards for Risk Management means the *AS/NZS ISO 31000.2018 Risk management - Guidelines*.

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 CNs Enterprise Risk Management Framework.

Risk means the effect of uncertainty on objectives, where 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.

Risk Management means coordinated activities to direct and control an organisation with regard to risk.

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.

Annexure B - Policy Authorisations

Function	Position Number / Title
Nil	

Document Control

Policy title	Enterprise Risk Management Policy
Policy owner	Director Governance / Manager Legal
Policy expert/writer	Manager Risk and Audit
Associated Procedure Title (if applicable)	NIL
Procedure owner (if applicable)	NIL
Prepared by	Governance
Approved by	CEO
Date approved	25/07/2022
Policy approval form reference	ECM# 7480738
Commencement Date	25/07/2022
Next revision date (date policy will be revised)	25/07/2025
Termination date	25/07/2026 (1year post revision date)
Version	2
Category	Governance
Keywords	Enterprise, risk, management, framework, ERM Framework
Details of previous versions	Version 1 ECM#5909005
Legislative amendments	NIL
Relevant strategic direction	Open and Collaborative Leadership
Relevant strategy	Open and Transparent Governance Strategy
Relevant legislation/codes (reference specific sections)	- *Australian Standards for Risk Management* - *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	- ERM Guideline - CN Risk Appetite Statement - Business Continuity Management Policy - Fraud and Corruption Control Strategy - Audit and Risk Committee Charter - Governance and Risk (Executive) Charter
Related forms	NIL
Required on website	Yes
Authorisations	Refer Part C