

# Risk Management Policy

## Contents

1. Introduction
2. Purpose of the Policy
3. Accountabilities, responsibilities and framework
4. Risk Registers
5. Risk Management Life Cycle
6. Risk Identification
7. Risk Definition and Description
8. Risk Ownership
9. Risk Assessment
10. Target Risk Assessment
11. Risk Appetite
12. Risk Mitigation and Management
13. Opportunity Risk
14. Reviewing and Reporting
15. Staff Training and Development
16. Links with Other Processes
17. Appendices

Issue Date	1 April 2020	Version 2
Review Date	<a href="#">1 April 2022</a>	<a href="#">1 April 2023</a>
Author: Internal Audit	F Haywood	Corinne Lawrie, Assistant Director, Assistant Director ICT/Digital and Transformation

Management Sign Off	BDC Council – 20 November 2020 SNC Full Council - 2021 September 2020	
Review frequency	Every two years – next review April 2025	

## 1. Introduction

- 1.1 Everything we do as a Council involves a degree of risk whether it is innovative projects, purchasing a new system or equipment, determining priorities, or making decisions about the future. It is therefore an essential part of good governance that we manage these risks effectively.
- 1.2 Risk is considered as part of the business planning processes to ensure that proposed objectives are ambitious and achievable and continuously monitored thereafter to ensure they are being effectively managed.
- 1.3 This risk management policy explains how the Council will ensure that it is managing risk effectively to increase the likelihood that business objectives will be achieved.
- 1.4 Effective risk management helps us to:
  - Successfully achieve corporate priorities and objectives by capitalising on opportunities and minimising threats;
  - Strengthen corporate governance and the internal control framework;
  - Improve partnership arrangements;
  - Embeds risk management into corporate processes including financial and strategic planning.
- 1.5 Risk is defined as **‘the effect of uncertainty on objectives’**.
- 1.6 Risk is an event, which if it crystallises, could adversely impact on the work of the Council. It may be a one-off event, repeated events or progressive continuum.
- 1.7 Risk Management is defined therefore as **‘the culture, policies and processes directed towards realising opportunities whilst managing threats’**. Its purpose is not to eliminate risk, but to understand it so as to take advantage of the upside and minimise the downside.
- 1.8 The internal control framework must therefore include arrangements for identifying, assessing and managing internal and external risks. Risk management is also closely linked to business planning and performance processes.
- 1.9 **Scope** - This policy applies to all employees, including those on temporary contracts and fixed term appointments and agency workers, members and anyone that works with the Council to achieve its objectives.

## 2. Purpose of the Policy

- 2.1 The aim of this document is to:
  - Introduce and promote an Enterprise Risk Management style Framework;
  - Develop a ‘whole risk’ approach to threats facing the Council; and

- Introduce appropriate processes to assist managers in the identification and management of risk in their areas of responsibility.

22 The key objective of this guide is to:

- Develop a robust approach to identification and understanding of risk facing the Council;
- Minimise threats facing the delivery of Council objectives;
- Establish practices and procedures to manage risk and maximise opportunities;
- Identify resources required to manage, control and evaluate risks.

### 3. **Accountabilities, responsibilities and framework**

31 Cabinet has ultimate responsibility for:

- Setting the culture for risk management at the Council
- Endorsing and approving this Policy
- For developing and approving Risk Appetite

32 Detailed oversight of the risk management process is delegated to the Audit Committee. Cabinet will seek assurance from the Audit Committee on the adequacy and effectiveness of the risk management process.

33 The Audit Committee is responsible for scrutinising the scope and effectiveness of the risk management systems in place. Overseeing the implementation of the risk management policy on behalf of Cabinet. Audit Committee uses a range of assurances to satisfy itself that a proper system of risk management and internal control is maintained.

34 The Managing Director is responsible for ensuring proper systems of financial control, risk management, legal and regulatory compliance are established and maintained, and that regular reports on these are provided to Cabinet.

35 The Corporate Leadership Team (CLT) are responsible for:

- Identifying and evaluating the significant risk faced by the Council in achieving objectives;
- Reviewing risk responses from management and ensuring that they receive reports on risks above agreed limits;
- Providing adequate information in a timely manner to Cabinet on the status of risks and controls.

36 Specifically, Assistant Directors are responsible for ensuring risk conversations form a

standard agenda item in Portfolio Holder meetings. These ongoing conversations will include the escalation of risks where applicable, associated mitigating actions and anticipated impacts are highlighted in a timely manner.

3.63.7 The ~~Transformation~~, Strategy and ~~Intelligence Programmes~~ Team are responsible for the development of the risk management policy, the implementation of the strategic risk management process and strategic risk management reporting.

3.73.8 The Head of Internal Audit is responsible for the development of the risk-based Internal Audit Programme and ensuring that Audit Committee has the required assurance on the management of risk and the effectiveness of internal control.

3.83.9 Managers are responsible for identifying and evaluating risks that threaten the achievement of objectives, for building a risk aware culture within their department, ensuring staff complete training where appropriate and understand how to identify and manage risk. Managers are responsible for reporting and escalating risks in line with this Policy and are responsible for the implementation of mitigating actions in respect of each risk.

3.93.10 **Appendix A** sets out the Council structure for risk management.

#### **4. Risk Registers**

4.1 The achievement of the Strategic Plan and subsequent in year Delivery Plans will carry several risks. The risks that could prevent the Council from achieving its objectives are described as strategic risks and are recorded in the Strategic Risk Register.

4.2 Strategic risks are those risks which could have organisational-wide impacts and are cross cutting or strategic in nature. Risks that could impact the work of the Council but would not have a strategic impact are described as operational risks and are recorded within directorate or project risk registers.

4.3 To facilitate the management of risk throughout the organisation the Council maintains a system of risk registers.

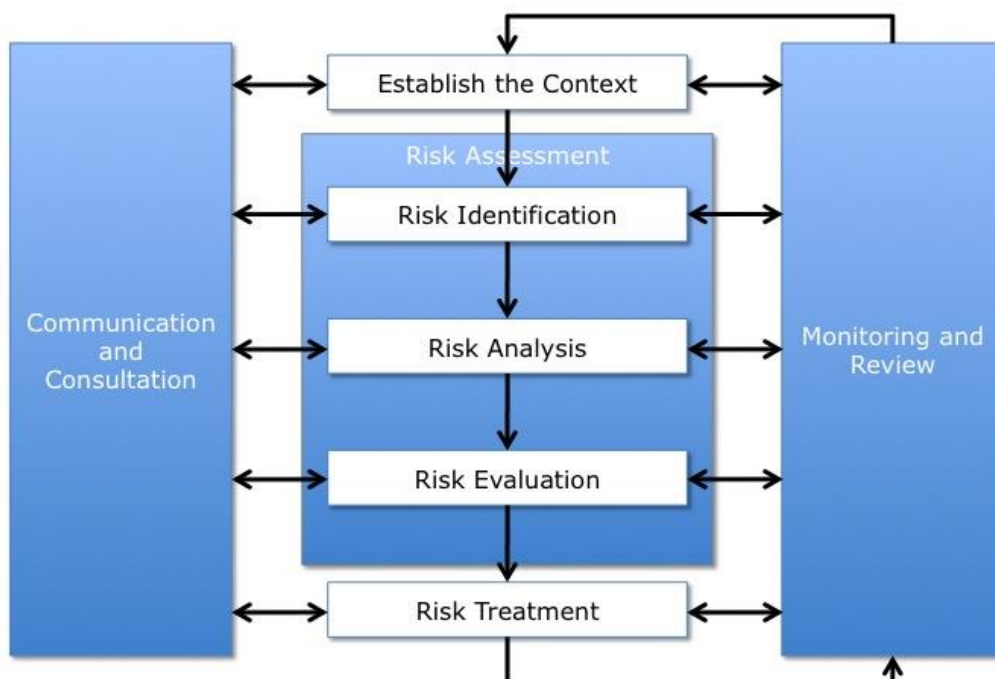
- **The Strategic Risk Register (SRR)** records the strategic risks facing the Council. These are risks that could prevent the Council from achieving its Strategic Plan and objectives. The risks on the SRR are identified through CMLT's assessment of the risks to the Council's Strategic Plan. These risks are reviewed by Cabinet and Audit Committee. Operational risks that are considered to have a strategic impact outside of appetite should be escalated on the SRR. The SRR is maintained by the Strategy and Intelligence Team on behalf of the CMLT and is presented in its entirety to Cabinet and to Audit Committee at least three times a year.
- **Directorate Risk Registers (DRR)** provides a record of the significant

operational risks facing each directorate. Each Director and Assistant Director takes responsibility for risks in their own area of work. Any risks deemed significant should be recorded in the risk register, linked to service level objectives and monitored as a regular agenda item at directorate level meetings to ascertain if the impact/likelihood is increasing or decreasing. Managers at all levels are encouraged to add significant risks to the Directorate Register using the Risk Identification Guidance and following the prescribed template on the risk management intranet pages to determine the most appropriate course of action. Action could either include; closely monitoring the risk or escalating the risk to the SRR if the likelihood/impact is scored outside of the appetite as agreed by the relevant Assistant Director.

- **Project Risk Registers** provide a record of the risks that have been identified from individual projects. Project risks are escalated to either Directorate risk registers via the relevant Assistant Director or to the SRR if outside of the agreed risk appetite. Project leads are responsible for maintaining the project risk registers.
- 4.4 **Appendix C** provides an overview of how risks are escalated to the strategic risk register.

## 5. Risk Management Lifecycle

- 5.1 The lifecycle of managing risk at the Council ensures that risk registers at all levels remain live and comprises the following key elements:



## 6. Risk Identification

- 6.1 In order to manage risk, the Council needs to understand what risks it faces and be able to evaluate them. Identifying risks is the first step in building the risk profile. Care should be taken to avoid identifying risks that do not impact on the Council's aims and objectives. Incidents that have already materialised should be distinguished from risk.
- 6.2 Risks can originate from inside or outside of the Council. Tools and techniques such as; PESTLE, SWOT, brainstorming and workshops can be used to ensure that a full range of internal and external risks are considered and assessed accordingly. These could include risks such as changes in government policy, extreme climate events, pandemics and business continuity threats.

## 7. Risk Definition and Description

- 7.1 Risks should be described in terms of the cause and consequence so that stakeholders can understand why they are of importance to the Council.

## 8. Risk Ownership

- 8.1 All risks on the SRR should be assigned to one member of CMLT as the owner.
- 8.2 Risks identified at Operational or Project level should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed.

## 9. Risk Assessment

- 9.1 Risk assessment is concerned with the measurement of identified risk. Risk is measured on two distinct scales:
- The likelihood of the risk event occurring (on a 1 to 5 scale), and
  - The impact of that risk event occurring (on a 1 to 5 scale).
- 9.2 The scores for each are then multiplied together to give a risk rating (on a 1-25 scale), which will form the basis for allocating resources for implementing risk control and mitigation activities.
- 9.3 Risk assessment and risk scores should be graded by using the risk scoring matrix provided at **section 11 of this policy in line with guidance given around Risk Appetite.**
- 9.4 The risk assessment should take into consideration the effectiveness of existing controls that are already in place that will have an impact on the likelihood and impact of the risk occurring.

95 Once risks have been assessed, the risk priorities for the Council will emerge. The greater potential exposure to the risk, the higher the priority required for addressing it. The highest priority risks (those that have the potential to have a strategic impact), should be given attention at the highest level i.e. CMLT and Cabinet.

## 10. Target Risk Assessment

10.1 If the identified risk requires mitigation due to it being outside of the appetite of the Council, actions will be identified that reduce the likelihood or impact of the risk. A second risk assessment should then take place to evaluate the risk exposure as if all the actions have been completed, reflecting how the planned actions would have reduced the overall risk rating.

10.2 The template for the register and assessment is provided on the Risk Management intranet pages.

## 11. Risk Appetite

11.1 Risk appetite is defined as: ‘the amount of risk an organisation is prepared to accept in pursuit of its objectives’. The principle recognises that risk cannot be reduced to zero and that mitigation will have both resource and cost implications.

11.2 –When considering threats, the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. It is about comparing the cost (financial or otherwise) of containing the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance.

11.3 When considering opportunities, the concept embraces consideration of how much the organisation is prepared to actively put at risk in order to obtain the benefits of the opportunity.

11.4 The risk appetite of the Council is outlined by a risk appetite statement which is as follows:

***We are a dynamic, innovative and commercially-minded Council that empowers its staff to make well-rounded decisions and take proportionate risks within our boundaries based on intelligence, reason and insight, seizing opportunities to enhance the wellbeing of our community, economy and staff, reimagining the role of local government.***

11.5 The statement outlines the Council’s approach to risk appetite and is accompanied by a risk scoring matrix which indicates whether the combined risk likelihood and impact score is above the appetite of the Council.

11.6 The appropriate approach for managing the risk is then highlighted depending on the combined score.



Risk Scoring Matrix		1	2	3	4	5
		Insignificant	Minor	Moderate	Significant	Severe
5	Expected	Medium 5	Medium 10	High 15	Very High 20	Very High 25
4	Highly Likely	Low 4	Medium 8	High 12	High 16	Very High 20
3	Likely	Low 3	Medium 6	Medium 9	High 12	High 15
2	Not Likely	Very Low 2	Low 4	Medium 6	Medium 8	Medium High 10
1	Rare	Very Low 1	Very Low 2	Low 3	Low 4	Medium 5
<b>Very High 20-25</b>		Risks scored here represent a severe threat to the delivery of the Council's objectives and service delivery and are outside of the risk appetite of the Council. Risks scored at this level should be treated as a priority and should either be reduced to a score within tolerance or removed. Reporting on progress will be required at Cabinet/Audit Committee and at CLT until risk level is reduced to tolerance.				
<b>High/Medium High 10-16</b>		Risks scored here represent a significant threat to the delivery of the Council's objectives and service delivery and are outside the risk appetite. Action is required to reduce the rating to a score within tolerance. Reporting on progress is required at Cabinet/Audit Committee and CLT until risk level is reduced to tolerance.				
<b>Medium 5-10</b>		Risks scored here represent a moderate threat to the delivery of the Council's objectives and service delivery and are within the risk appetite of the Council with some proportionate mitigation and regular monitoring required. These risks can be managed at operational/service level but regular management review of assurance on control effectiveness should occur. Routine reviews should also be carried out to ensure there is no change.				
<b>Low 3-4</b>		Risks here represent a minor threat to the delivery of the Council's objectives and service delivery and are within the risk appetite. Review required to ensure risk score does not change/increase, however these risks can be managed at operational/service level.				
<b>Very Low 1-2</b>		Risks scored here represent an insignificant threat to the delivery of the Council's objectives/service delivery and are within the risk appetite. No further action is required.				

11.7 As demonstrated by the table shown above, any risk with a combined score of 10-25

is outside the risk appetite and action must be taken to reduce the score down to an acceptable level to protect the achievement of the Councils' strategic aims and objectives.

- 11.8 In order to assist staff in the risk assessment and scoring of each risk, scoring criteria has been identified for a series of key categories. This may not be applicable in all instances but can be used as a guide. Please see likelihood and impact scoring criteria at **Appendix B**.

## 12. Risk Mitigation and Management

- 12.1 Identifying gaps in existing controls and identification of the actions that are needed to improve the mitigation of risks in line with ~~the~~ **both** Councils's risk appetite will involve employing either one or a mix of the following:

- Acceptance – Where the level of the risk falls below the Councils risk appetite and a conscious decision is made to accept that risk and to take no further action other than ongoing monitoring and periodic review. Sometimes referred to as tolerate.
- Avoidance – Where the actions causing the risk are avoided; for example, withdrawing from a particular activity, project or service.
- Reduction – Take action to reduce the level of risk by reducing either the impact or the likelihood of the risk event occurring.
- Transferring – Transferring most or some of the risk to a third party. The main types are insurance and outsourcing.
- Sharing – Risk sharing is the distribution of risk to multiple organisations for example during a project with a number of stakeholders involved.

- 12.2 In choosing between these responses, factors to consider include cost, feasibility, probability and the potential impact. Every control has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling.

## 13. Opportunity Risk

- 13.1 Opportunity risk is defined as a 'failure to identify or exploit an opportunity which is unable to be perused later without an additional cost'. Managing opportunity risk involves creating a climate for innovation in which an awareness of the constraints doesn't prevent people coming up with ideas and putting them forward.

- 13.2 Risk and opportunity go hand in hand. The opportunity for advancement cannot be achieved without taking risk and risk is essential to progress and innovation. Excessive caution can be as damaging as unnecessary risk taking.

## 14. Reviewing and Reporting

- 14.1 Regular monitoring and review are essential to gain assurance over the risk management framework and to ascertain whether:
- Risks are still relevant
  - Emergent risks have been identified
  - Likelihood and impact of risks has changed
  - Controls are still effective.
- 14.2 Cabinet will review the Strategic Risk Register three times a year, with a year end review of the previous years' output. The papers provided to Cabinet will include a summary on the effectiveness of the risk management framework and any specific comments on the strategic risks identified.
- 14.3 Audit Committee will support Cabinet by reviewing and advising on the operation and effectiveness of arrangements in place across the Council that support the achievement of objectives. Audit Committee will review both the Strategic risk register and risk management arrangements three times a year. They will also periodically receive results of independent assurance on the adequacy of the risk management framework and control framework.
- 14.4 In particular, Audit Committee will scrutinise the adequacy of:
- All risk and control related assurance statements, together with any accompanying internal audit statement, external audit opinion or other appropriate independent assurances.
  - The underlying assurance processes that indicate the degree of the achievement of the Council's objectives, the effectiveness of the management of strategic risks and the appropriateness of the above disclosure statements.
- 14.5 The Corporate Leadership ~~Management~~ Team will receive reports on the progress of the risk management framework prior to Cabinet and the make-up and movement in the strategic risk register three times a year.
- 14.6 Risks and risk registers at a directorate/service level and project level are reviewed as part of the routine cycle of team meetings or as required.
- 14.7 All staff are required to consider and monitor risks as part of their job role. If a risk is identified that is above risk appetite of the Council and requires escalating to the strategic risk register, the procedure at **Appendix C** should be followed. These risks should be monitored and reported until they are reduced to an acceptable level or the risk no longer poses a threat to the achievement of Council objectives.

## 15. Staff Training and Development

15.1 To support colleagues in the move towards a mature enterprise wide risk management process, the following training will be available:

- An e-learning self-facilitated learning module developed to provide guidance on the fundamental principles of risk, covering the policy and procedures specific to the Council.
- A rolling programme of small team specific workshops on the fundamental principles of risk management [available upon request](#).
- One to one training and support offered to officers by the Strategy and ~~Programmes~~ [Intelligence](#) Team and or Internal Audit.
- **Risk Identification Guidance** is also available on the intranet under risk management pages.

## 16. Links with other processes

16.1 The risk management process is carried out during the setting of strategic delivery plans and is considered during Internal Audit's approach to risk based planning. The Strategic Risk Register is considered during the completion of assurance statements informing the Council Annual Governance Statement.

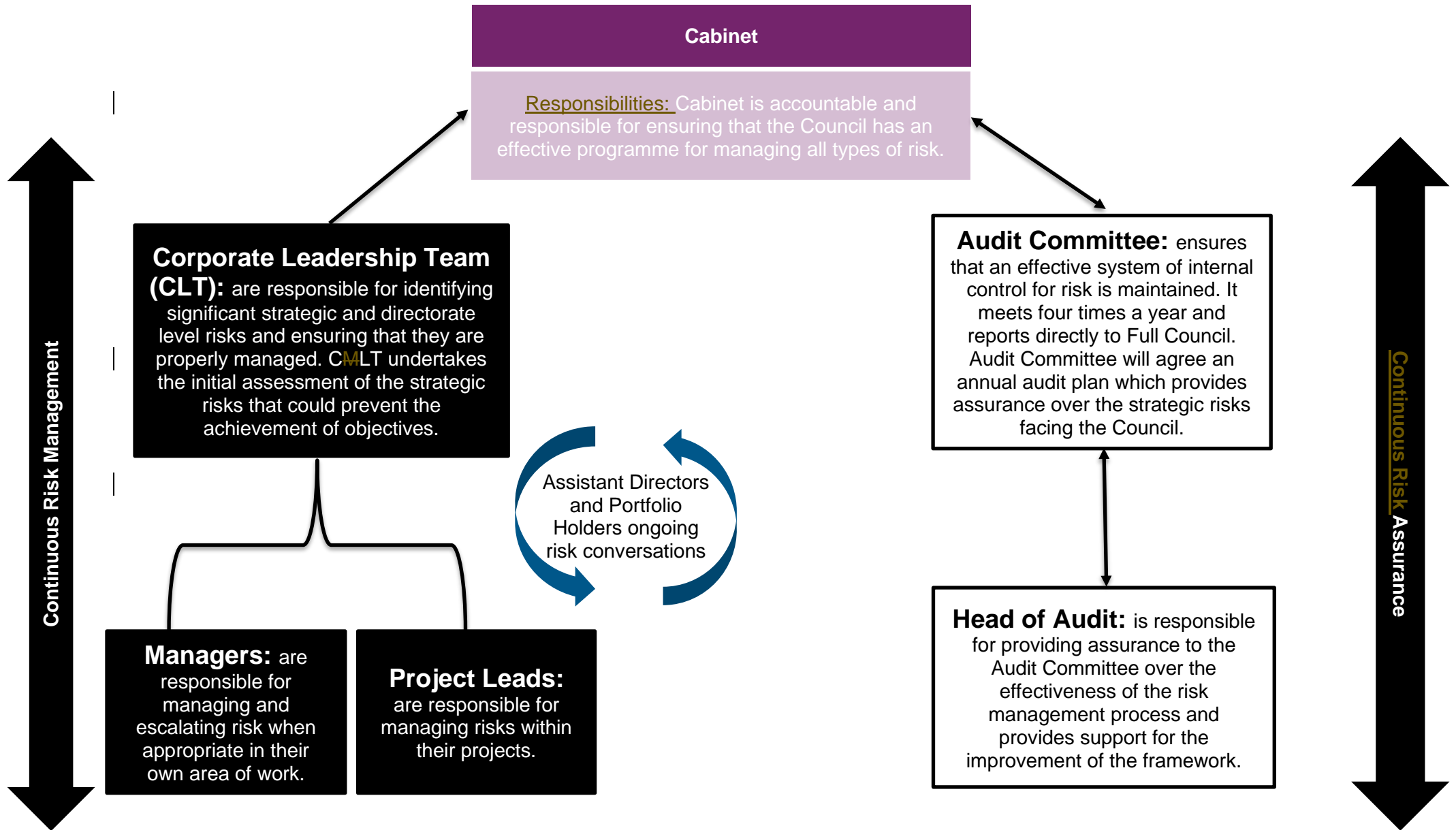
## 17. Appendices

**Appendix A** – Structure for Risk Management

**Appendix B** – Risk Scoring Criteria – Likelihood and Impact

**Appendix C** - Escalation to the Strategic Risk Register

## Appendix A – Structure for Risk Management



## Appendix B – Risk Scoring Criteria Likelihood and Impact

### Likelihood

<b>Likelihood</b>		<b>Description</b>	<b>Timing</b>
<b>5</b>	<i>Expected</i>	<i>Risk event or circumstance is relatively certain to occur</i>	<i>More than once per year</i>
<b>4</b>	<i>Highly Likely</i>	<i>Risk event or circumstance is highly likely to occur</i>	<i>Once per year</i>
<b>3</b>	<i>Likely</i>	<i>The risk event or circumstance is more likely to occur than not</i>	<i>At least once between 1-5 years</i>
<b>2</b>	<i>Not likely</i>	<i>The risk event or circumstance is possible</i>	<i>At least once between 5-10 years</i>
<b>1</b>	<i>Rare</i>	<i>This will probably never happen</i>	<i>Probably within 10-15 years</i>

## Impact on delivery of services

<b>Impact Type</b>	<b>Insignificant</b>	<b>Minor</b>	<b>Moderate</b>	<b>Significant</b>	<b>Severe</b>
Financial loss	£0k - <£10k	£10k - <£25k	£25k - <100k	£100k - £500k	Over £500k
Service provision	Inconsequential disruption to a service.	Minimal disruption to Council activities/service.	Significant disruption to service delivery.	Significant disruption to large parts of the Council or suspension of service.	Service suspended long term.
Projects	Minor delay	Minor milestones missed	Significant milestones missed or delayed	Major milestones missed	Project will not achieve objectives and misses majority of milestones
Objectives	No effect	Some team objectives not met	Team objectives not met	Portfolio objectives not met	Strategic objectives not met
Health and Safety	Isolated incident/ injury/illness. No lost time to injury days.	Minor injury or illness requiring medical treatment.	Threat of violence, serious injury or illness requiring medical attention.	Significant/extensive/multiple injury or illness, permanent or partial disability.	Fatality. Multiple major injuries/illness. Permanent total disability.
Staff Engagement	Isolated events of dissatisfaction	Some hostile relationships/minor non-co-operation	Hostile relationships. Major non-cooperation across the organisation	Industrial Action	Mass staff walkout/leaving
Reputational	Minor unfavourable social media coverage/attention	No media coverage. Minor letters of complaint	Adverse local media/social media coverage relating to conduct of leader or members or Council	Adverse national media exposure	Prolonged adverse national exposure
Statutory/Legal	Isolated non-compliance. Informal recommendation not followed up.	Non-compliance Warning received	Breach. Improvement Notice	Enforcement Action	Prosecution Fine Successful Judicial Review

## Appendix C – Escalation to the Strategic Risk Register

