Ashfield DISTRICT COUNCIL

Corporate Risk Management Strategy & Process

Version	Date	Status (draft, approved, signed off	Author	Change Description
V1.0	02/12/21	draft	C Clarke	Annual review of strategy
V2.0	24/01/22	Revised draft	C Clarke	Audit comments taken into consideration and applied
V3.0	29/03/2022	Final	C Clarke	Audit Committee approval given on 28/03/22

Approved for submission to Sponsor, given by	C Clarke	Date	24/1/22
Sponsor sign off to proceed with project identification, given by	Joanne Froggatt	Date	29/03/22

Distribution List

Name	Organisation	Job title / Dept.

Contents

1. Ashfield District Council Risk Management Strategy - Introduction

1.1 Philosophy and aims

Our philosophy:
Ashfield District Council will seek to embed risk management into its culture, processes and structure to ensure that opportunities are maximised. Ashfield District Council will ensure that the resources and support is available to assist managers to identify, understand and manage risks, and learn how to accept the right risks. Adoption and application of this strategy will deliver success in delivering services to the customers of Ashfield District Council.

1.2 Purpose

The purpose of this risk strategy document is to set out in clear simple terms how risk management will be managed within Ashfield District Council and become embedded in the culture.

It therefore aims to:

- Develop risk management and raise its profile across the Council, and ensure that risk management becomes a living tool.
- Make risk management part of normal business and therefore incorporated within all decision making processes.
- Integrate risk management into the culture of the Council.
- Ensure that all risks are managed in accordance with best practice.
- Create effective processes that will allow risk management assurance statements to be made annually.

1.3 What is risk management?

Risk definition: Risk is uncertainty of outcome. The delivery of an organisation's objectives is surrounded by uncertainty which both poses threats to success and offers opportunity for increasing success. Risk is defined as this uncertainty of outcome, whether positive opportunity or negative threat, of actions and events

Risk Management can be defined as:

> **“**Risk management is the process of identifying risks, evaluating their probability and potential consequences and determining the most cost effective methods of controlling and /or responding to them. It is not an end in itself. Rather, risk management is a means of maximising opportunities and minimising the costs and disruption to an organisation caused by undesired events” ‘Risk Management – A Key to Success,’ published by ALARM

Risk management therefore is essentially about identifying all the obstacles and weaknesses that exist within the Council. A holistic approach is vital to ensuring that all elements of the organisation are challenged including our decision making processes, work with partners, consultation processes, existing policies and procedures as well as the effective use of all assets – including our staff. Once the obstacles have been identified the next stage is to prioritise them to identify the key obstacles facing the Council and to help the organisation to effectively deliver services to our customers. Once risks have been identified and prioritised it is essential that steps are taken to then effectively manage those key obstacles / risks. This will ensure that major obstacles or blockages that exist within the organisation can be mitigated to provide the Council with a greater chance of being able to maximise the delivery of its objectives and provision of services to our customers.

Risk management will be used as a strategic tool and an essential part of effective and efficient management and planning within the organisation.

1.4 Risk Management policy statement

Risk is the chance of something happening that may an impact on what we set out to achieve.

Risk management is the process for dealing with this effectively – identifying, evaluating, prioritising and mitigating the risks. It is not an end in itself. Effectively managing our risks means that we can maximise opportunities and minimise the costs and disruption to the Council caused by undesired events.

Risk appetite is the “amount and type of risk that an organisation is prepared to pursue, retain or take". This is reviewed annually alongside this framework. The current risk appetite framework outlines the Council’s approach to risk appetite as well as how to determine and evaluate risk appetite.

As a Council we have identified our strategic risks and have a process in place to control and monitor them. We regularly review them (at least quarterly) to ensure that the corporate risk register remains up-to-date. We also have a system in place to identify project and operational risks at an early stage and again to control and monitor them effectively.

The aim is to manage risk rather than to eliminate it. Too little attention to the control of risk will lead to unnecessary losses and poor performance. An overzealous approach to risk control can stifle creativity and service delivery and may mean that opportunities for improvement are missed. Successful risk management means getting the balance right, thereby making the best use of available resources. We identify actions to reduce negative risks to an agreed acceptable level and this is monitored via the risk register.

The management of risk should not be viewed in isolation; it forms an integral part of the Council’s business. The risk management process forms part of the service planning framework. In addition risk management techniques can be used when considering new service delivery methods or policy options. Much risk management already takes place intuitively.

There is clear ownership of risks at all levels within the authority and we expect partner organisations and contractors to have suitable risk management arrangements.

1.5 Why do we need a risk management strategy?

Risk management will, by aligning to the business planning and performance management processes, strengthen the ability of the Council to achieve our objectives and enhance the value of the services we provide.

Also, Risk Management will, by aligning to the Business Continuity processes, strengthen the ability of the Council to react to all situations and protect its own interests and those of the district, ensuring essential service delivery.

However it is also something we are required to do, for example:

- The CIPFA/SOLACE framework on Corporate Governance requires the Council to make a public assurance statement annually, on amongst other areas, the Council's risk management strategy, process and framework. The framework requires us to establish and maintain a systematic strategy, framework and processes for managing risk.
- Risk management was a key discipline identified in the Organisational Assessment, particularly looking at whether an authority has assessed the risks inherent in its corporate and service plans. This requirement has now been removed, however, is recognised as good practice.
- Risk management is now considered standard practice in both the public and private sectors.
- To meet our statutory obligations such as Civil Contingencies Act, providing emergency response and planning and providing for emergency assistance.

1.6 Benefits of risk management

Successful implementation of risk management will produce many benefits for the Council if it becomes a living tool. These include:

- Increased chance of achieving strategic objectives as key risks are identified and minimised.
- Achieves buy-in to risk (and action) for officers and members.
- An organisation can become less risk averse (because you understand risks).
- Improved performance, accountability and prioritisation - feeds into and aligns with the performance management framework.
- Better governance can be demonstrated to stakeholders.
- Control and mitigation of business continuity risk

1.7 Link to Corporate Objectives

Adequate risk management arrangements link to the authority's Innovate and Improve priority. However, the minimisation of risks also enables all of the Council's priorities to be achieved. The identification of risk relating to the achievement of performance and improvement is a key aspect of the performance management framework

1.8 Risk appetite

The ISO 31000 risk management standard refers to risk appetite as the:

"Amount and type of risk that an organisation is prepared to pursue, retain or take".

The Corporate Risk register is reviewed quarterly-taking into consideration the risk appetite as stated in our risk appetite framework.

The appropriate level will depend on circumstances and must be appropriate given our corporate objectives. Risk rating analysis is the identification and evaluation of all risks to achieving objectives. The task of risk management is to limit the organisation's exposure to an acceptable level of risk in relation to the expected gain by taking action to reduce the probability of the risk occurring and its likely impact. Service Directors are responsible for ensuring that all risks are contained within the limits of the risk appetite framework and those that fall above the acceptable limit are referred to the corporate risk register. For example, where public safety is involved our appetite will tend to be low, while for an innovative project that is a key part of our transformation programme, it may be higher, recognising that there will be uncertainty and the potential for things to go wrong but the potential rewards will be higher too.

1.8.1 Risk appetite categories

A detailed framework has been written in relation to risk appetite and this should be read in conjunction with this strategy in order to understand what risk levels are acceptable to the Council.

Averse: Avoidance of risk and uncertainty; minimal exposure to risk preferred; consequently likely to be low potential for reward / achieving a stretching objective; corresponding risk score = **low**

Cautious: Preference for safe options with a low to medium degree of risk only; again this is likely to consequently reduce the potential for reward / achieving a stretching objective; tight controls in place; corresponding risk score = **low to medium**

Open: Willing to consider all potential options and choose the one most likely to achieve the objective, while also providing an acceptable level of reward and value for money; balanced approach recognising that things may go wrong but we will learn from them; corresponding risk score = **medium**

Hungry: Eager to be innovative and to choose options offering potentially higher rewards, despite greater inherent risk; willing to tolerate uncertainty and accept possibility of significant loss; corresponding risk score = **high**

2. Implementing a risk management process

This section covers the implementation of the risk management process within the Council. In order to implement risk management within the Council managers and staff need to become familiar with, and have guidance on, the:

- risk management process,
- roles and responsibilities of officers and members,
- reporting and monitoring.

2.1 The Risk Management Process

Implementing the strategy involves adopting a systematic and robust process. The following risk management cycle describes the processes that should be followed.

Step 1 Identifying risks facing the Council.

Risk management is all about understanding, assessing and managing the Council's threats and opportunities. The Council accepts the need to take proportionate risk to achieve its strategic obligations, but expects these to be appropriately identified, assessed and managed.

Risk Identification includes identification of events which might create, prevent, accelerate or delay achievement of the organisation's strategic *objectives.
The Risks can then be categorised under strategic and operational. Strategic risks are those risks identified as potentially damaging to the achievement of the Council's objectives. These can be sub-classified into:

• Political	• Social
• Legislative	• Competitive
• Economic	• Technological
• Environmental	• Customer/citizen

Operational risks are those risks that should be managed by departmental officers who will be responsible for operating and maintaining the services. These can be sub-classified into:

• Professional	• Legal
• Contractual	• Environmental
• Financial	• Physical
• Information	

Step 2 Analysing the risks

The risks are analysed and reported in a corporate standard format. (See Appendix 3). All risks assessed in a 6x4 risk matrix should be dealt with according the table below.

Probability Score	Impact Score			
	1 Negligible	**2 Minor**	**3 Major**	**4 Critical**
6 (Very High)	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly to CLT	Monitor Quarterly to CLT*
5 (High)	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly to CLT	Monitor Quarterly to CLT
4 (Significant)	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly to CLT
3 (Low)	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly	Monitor Quarterly
2 (Very Low)	Monitor 6 Monthly	Monitor 6 Monthly	Monitor Quarterly	Monitor Quarterly
1 (Almost Impossible)	No action required	Monitor 6 Monthly	Monitor 6 Monthly	Business Continuity Plan

*it may be that these need to be monitored more regularly than every 3 months depending on the seriousness of the risk. CLT will decide if that is the case.

Aligned with the Risk Appetite Framework which describes the type of action required in accordance with our risk appetite

Risk rating Score	Risk rating action required
18-24	Risks at this level sit above the tolerance of the Council and are of such magnitude that they form the Council's biggest risks. The Council is not willing to take risks at this level and action should be taken immediately to manage the risk (this may include ending the activity and then managing the risk down to an acceptable level). Corporate Risks, monitored by CLT
15-16	These risks are within the upper limit of risk appetite. While these risks can be tolerated, controls should be identified to bring the risk down to a more manageable level where possible. Corporate Risks, monitored by CLT
5-12	These risks sit on the borders of the Council's risk appetite and so while they don't pose an immediate threat, they are still risks that should remain under review. If the impact or likelihood increases then risk owners should seek to manage the increase. Corporate Risk only if deemed threat to delivery of Corporate Objectives

3-4	These are low level risks that could impede or hinder achievement of objectives. Due to the relative low level it is unlikely that additional controls will be identified to respond to the risk.
1-2	Minor level risks with little consequence but not to be overlooked completely. They are enough of a risk to have been assessed through the process, but unlikely to prevent the achievement of objectives.
Impact 4, Likelihood 1	Rare events that have a catastrophic impact form part of the Council's Business Continuity Planning response.

Service Directors should regularly review high level risks within their directorate and aim to reduce the level of risk (impact and likelihood) and where the action taken cannot reduce the risk level they should then consider whether it has a major impact on the Council being able to achieve its strategic obligations and elevate to the Corporate Risk register.

Step 3 Prioritising the risks

The process then prioritises the risks resulting in a focus on the key risks and priorities i.e. those risks most likely to happen and with the greatest impact. The table immediately above sets the priorities.

Step 4 Managing of the risks through action plans

The risks are then managed through the development of appropriate risk management action plans. The Corporate standard template incorporates risk identification and action planning. This is managed through the performance management software ''Pentana''.

Step 5 Monitoring of the action plans and the risks

Risks are managed through the performance management framework at least once every three months, whilst monitoring the delivery of the service and corporate action plans. The information is held in the performance management software ''Pentana''.

The cycle is continuous and should be followed on a regular basis.

The risk management process is described in detail in Appendix 1.

2.2 Roles and Responsibilities

The successful management of risk is a collective responsibility for all Members and employees. The Council has a duty to the community to manage its resources economically, efficiently and effectively.

The Chief Executive has overall responsibility for ensuring that strategic risks are effectively managed within the Council and to provide an annual statement of assurance on strategic risks.

It is the responsibility of **all Elected Members** to be aware of the risk management implications of their actions, decisions and public statements. All decision making reports include a section identifying any key risks. Elected Members can ask for these and any other risks which they have identified to be fed into the Council's risk process e.g. an operational risk may be passed to the service manager to lead on, a strategic risk may be passed to Audit Committee and/or Cabinet to debate.

It is the responsibility of **Cabinet Members**:

- To agree an effective strategy and framework to manage risks within the Council
- To set the Council's risk appetite in conjunction with senior managers and the Audit Committee
- To receive exception reports on risk management (focused at the strategic level) as part of the established quarterly monitoring and to recommend action where necessary
- To agree the Council's response to its highest risks i.e. doing what is practicable to reduce the risk, whilst not using a disproportionate amount of resource
- To formally consider risk management implications when making decisions
- To hold the Audit Committee and CLT accountable for the effective management of risk
- Monitoring the Council's risk management and internal control arrangements via quarterly reports to Cabinet.
- Approving the public disclosure of the annual outcome of this assessment (the assurance statement), and publishing it in the annual Statement of Accounts.

The **Portfolio Holder for Customer Services and IT** is the Cabinet lead on risk management issues. It is their responsibility to promote awareness of potential risk implications at Cabinet level. For example, to pay particular attention to the risk elements in decision making reports; to be available to colleagues to discuss risks; to be satisfied that the risk arrangements are in place and working well; to present the quarterly risk information to Scrutiny & Cabinet.

It is the responsibility of the **Audit Committee**:

- To have an overview of risk management in the Council through reporting and advice provided by the Assistant Director - Corporate Services and Transformation
- To carry out an quarterly review of the risk management framework, including the risk appetite, and to recommend it to Cabinet for approval
- To carry out an quarterly review of the strategic risk register and to recommend it to Cabinet for approval

Corporate Leadership Team (CLT)

The Corporate Leadership Team is pivotal in leading the promotion and embedding of risk management within the Council. In addition they have an important role in identifying and managing risks.

Corporate Leadership Team's key tasks are:

- Recommending to Cabinet the Corporate Risk Management Strategy and its subsequent revision.
- actively being involved in the assessment and management of risks on a quarterly basis, at Corporate strategic level
- being actively involved in the identification, assessment and management of risks within their directorates as part of the service planning process.
- supporting and promoting risk management throughout the Council,
- support the Risk Management Sponsor

Risk Management Sponsor – Strategic Planning Risk
The Risk Management Sponsor (Strategic Planning Risk) will lead the championing and embedding of strategic risk management and drive its implementation within the Council. This role is part of the duties of the Assistant Director – Corporate Services and Transformation.

Responsibilities include:

- compiling, and reporting quarterly (from Pentana), to CLT all corporate risks, including the risks escalated up from the Directorate level, and lead their identification, assessment and management of strategic risks on a biannual basis. The report will be shared with Leadership after CLT has reviewed the register on a quarterly basis.
- Production of an quarterly report to Cabinet on the progress of strategic risk management, the risks, and action in managing them,
- Production of a quarterly report to Audit Committee
- supporting and advising CLT on strategic risk management issues
- communicating the benefits of effective strategic risk management to all members of Ashfield District Council
- ensuring the alignment of risk within strategic planning and performance and improvement processes
- ensuring all levels of risk are discussed and reviewed at Performance Boards, including the identification of new risks.

It is the responsibility of **Service Managers:**

- To have responsibility of risk within their service areas
- To have an overview of risk management in the Council at officer level
- To contribute to the annual review of the risk management framework, including risk appetite
- To ensure that the Council's risk management framework is applied in their service areas by identifying, assessing, reporting and monitoring risks and setting risk appetites
- To contribute to the management of strategic risks in support of CLT

It is the responsibility of **Project leads**:

- To ensure that the Council's risk management framework is applied to their project by identifying, assessing, reporting and monitoring risks and setting the risk appetite
- To exception report via reporting at intervals agreed with the Project Sponsor.

Other key staff include

- Service Manager - Risk & Emergency Planning (covers H&S and Business Continuity)
- ICT Technical & Security Manager (Covers ICT and data security)
- Principal Accountant, Financial Management (Covers all insurance related risk)

It is the responsibility of **All Employees:**

- To be aware of the Council's risk management framework
- To have an understanding of the risks that arise within their area of work
- To participate in risk management training as appropriate
- To challenge practices, identify new ways of doings things and be innovative
- To learn lessons from risk management rather than apportion blame and to concentrate at least as much on how risks have been managed in any given situation rather than just the outcome if something goes wrong

2.3 Reporting and monitoring

The responsibility for monitoring and reviewing the corporate risk is the responsibility of the Corporate Leadership Team who are required to do this quarterly.

The responsibility for monitoring and reviewing the service risk is the responsibility of Service Managers who are required to do this as a minimum quarterly. This should be done by updating the risks that have been recorded in Pentana.

Service Directors are responsible for escalating risks, those above the risk tolerance line as set out in the risk appetite framework to the Corporate Leadership Team who will determine if they should be included on the Corporate Risk Register. Where action taken cannot reduce the risk level then they should then consider whether it has a major impact on the Council being able to achieve its strategic obligations and elevate to the Corporate Risk register This should be done through the Risk Management Sponsor – Assistant Director – Corporate Services and Transformation.

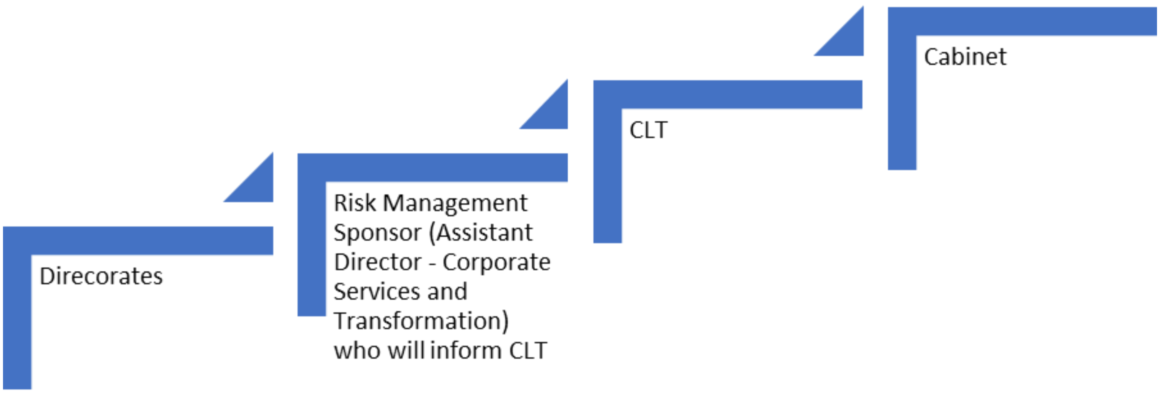
The definition of a corporate risk is - any key risk facing the Council or a particular service in the delivery of its plans, that is, a threat that an event or action will adversely affect the Council's ability to achieve its corporate objectives, perform its duties or meet expectations of its stakeholders.

The Risk Management Sponsor – Assistant Director – Corporate Services and Transformation will report progress on the risk management performance, process, and key risks, annually to Cabinet. They will also be responsible for reviewing the Corporate Risk Management Strategy and most effective risk management processes on an annual basis.

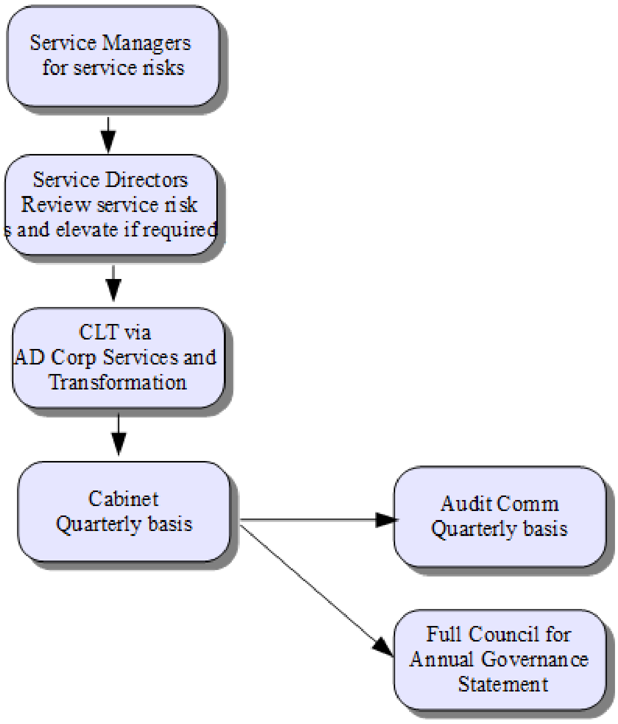
The action plans developed to manage the Strategic risks will be aligned to the Performance Management Framework and will be monitored by the Risk Management Sponsor – Assistant Director – Corporate Services and Transformation through the Performance Management System Pentana. This will ensure the integration of risk management with other processes and ultimately ensure its profile and success is maintained.

Project risks should be documented and approved by the relevant project sponsors and reviewed at intervals set out in the project initiation document.

The framework for reporting risk is summarised below:
Risk assessments will be included in all policies and reports, as well as in our partnership working arrangements, so that risk is considered in everything the Council does.



The below illustration shows the governance structure in relation to risk responsibilities.



Risk types

The Orange Book published by HM Treasury provides guidance on risk types and the below are examples of types of risks and further detailed information is contained in Appendix 1.

- Strategy risks
- Governance risks
- Operations risks
- Legal risks
- Property risks
- Financial risks
- Commercial risks
- People risks
- Technology risks
- Information risks
- Security risks
- Project/Programme risks
- Reputational risks

Corporate Risk Register

Where a risk has been elevated to be included on the Corporate Risk Register it remains the decision of the Corporate Leadership Team who will decide when and if it can be removed. It should only be removed if it no longer threatens the objectives of the Council and is no longer a threat. The decision to remove a risk should be documented in the minutes of the CLT meeting. This should also be documented in the notes field for that risk within the register that is recorded in pentana.

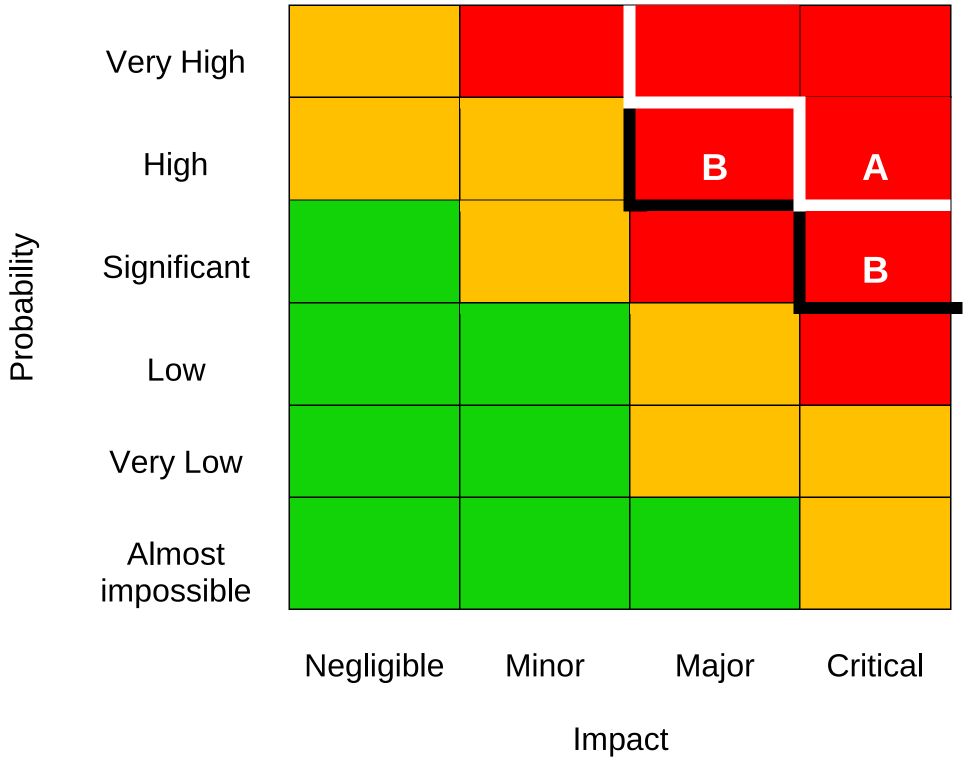
Conclusion

The adoption of a sound risk management strategy will achieve many benefits for Ashfield District Council. It will help with business planning, the achievement of objectives, the demonstration of continuous improvement, the delivery of projects and demonstrate effective corporate governance.

The challenge however is to implement this comprehensive risk management process without significantly increasing workloads. This should be achieved by the integration of risk management into existing processes and reviews rather than as a separate process.

Appendix 1 – The risk management process

Source : ALARM Risk Management toolkit



At a summary level, we have established the broad levels of residual risk which may be accepted or tolerated for overall general application, monitoring and control. Those in ‘’A’’ and ‘’B’’ are unacceptable and must be referred to the Corporate Risk Register.

Stage 1 - risk Identification

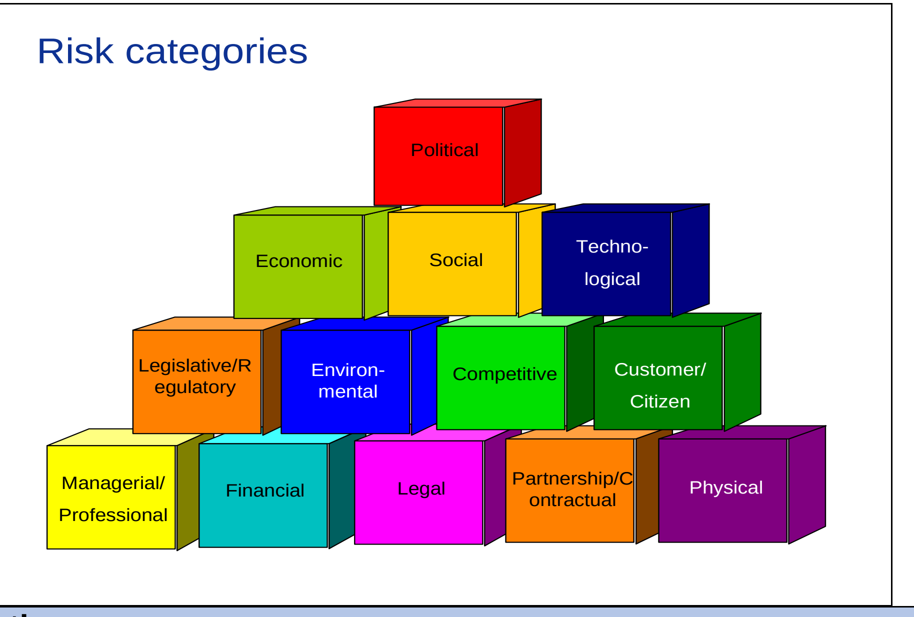
Corporate Risk will be managed and monitored by CLT quarterly in partnership with the Assistant Director – Corporate Services and Transformation. However it will be for each Directorate to decide upon the appropriate approach to identifying its key risks as this process is cascaded down throughout Ashfield District Council.

The categories of risk to prompt identification and to help to identify the cause / source of risks are:

Strategy risks
Governance risks
Operations risks
Legal risks
Property risks
Financial risks
Commercial risks
People risks
Technology risks
Information risks
Security risks
Project/Programme risks
Reputational risks

The risk identification stage should also include a review of published information such as corporate/service plans, strategies, financial accounts, media mentions, inspectorate and audit reports etc.

Service Level Strategic Planning and Performance Management –
Each Service will review any relevant risks in the achievement of performance and improvement activity, and therefore achievement of Corporate Priorities. This will be undertaken quarterly as well as refreshed annually as part of the service planning process. The Corporate Timeline Managers Checklist includes prompts for service managers to review risk on a regular basis (Appendix 2)



Risk Type	Description
Strategy risks	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).
Governance risks	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations risks	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
Legal risks	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take

	appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
Property risks	Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
Financial risks	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting
Commercial risks	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.
People risks	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, Page 16 industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance
Technology risks	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information risks	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security risks	Risks arising from a failure to prevent unauthorised and/or inappropriate access to key government systems and assets, including people, platforms, information and resources. This encompasses the subset of cyber security
Project/Programme risks	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputational risks	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Stage 2 – Risk analysis

The information gathered from the risk identification processes above should be analysed and risk scenarios developed for the key concerns using the Risk Register and Action Plan (see Appendix 3). The Risk Register and Action Plan (Corporate and Service) should include a clear description of the risk, priority rating of the risk and proposed action. Generally, where interviewees have perceived a risk, which has been corroborated by others, the risk should appear in the scenarios – particularly if it is backed up by available evidence.

Evaluate likelihood and impact

Likelihood/Probability					
1 Almost Impossible/ Never	2 Very Low/ Hardly Ever	3 Low/ Possible	4 Significant/ Probable	5 High/ Almost certain	6 Very High/ Almost definite
Never happened	No more than once in last 10 years	Happened a few times in last 10 years	Happened in last 3 years	Happened last year	More than once in last year
Will almost never to happen	Extremely unlikely again in year	Could happen in year	Possibility it might happen in year	Likely to happen in year	Expected to happen in year

Impact/Consequences				
	Service delivery	Finance	Reputation	People
4 Critical	Interruption to core service Failure of key project	Severe costs incurred; Financial loss of >10% of the tolerance set Impact on whole Council; Statutory	Significant media interest seriously affecting public opinion	Loss of life; Major causalities

		intervention		
	Service delivery	**Finance**	**Reputation**	**People**
3 Major	**Key targets missed Some services compromised**	**Significant costs incurred Financial loss of >5% of the tolerance set Resetting of budgets required Service budgets exceeded**	**Local media interest and significant social media commentary; Comment from Inspectors; Impact on public opinion**	**Serious injuries; Traumatic experience; Exposure to dangerous conditions**
2 Minor	**Management action required to address short term difficulties**	**Some costs incurred Financial loss of <5% of the tolerance set Minor impact on budgets; (managed by Service Manager)**	**Limited local publicity; Mainly within local government community; Causes staff concern**	**Minor injuries or discomfort; Feelings of unease**
1 Negligible	**Managed within normal daily routines**	**Little loss anticipated Financial loss within the tolerance set**	**Little or no publicity; Little staff comment**	

Stage3 – Prioritisation

Following identification and analysis the risk scenarios need to be evaluated

This should look at the risk scenarios and decide on their ranking according to the probability of the risk occurring and its impact if it did occur. The matrix (shown over) should be used to plot the risks and once completed this risk profile clearly illustrates the priority of each scenario.

It is essential at this stage that there is agreement around the timescales being used. The profiling group will agree if the risks are to be profiled over a 12-18 month timescale or a 3-4 year timescale. It will often depend on what the information will be used for – annual planning or 3-year planning. Impact should be assessed against the achievement of the Corporate, or service objectives as applicable. The ALARM model suggests that '' Risk assessment scales should be developed based on the parameters of the project/programme, for example, the likelihood scale should be aligned to the duration of the project/programme''. Therefore the likelihood scale should reflect the timeframe of the activity/project or programme.

Although the risk profile will produce a priority for addressing each risk determining the group's appetite for risk can enhance this. All risks above the appetite cannot be tolerated and must be managed down, transferred or avoided. The appetite for risk is determined during the facilitated workshop and is achieved by starting in box P1:I1 and asking the group to decide if they are prepared to live with a risk in that box or if they want to actively manage it. Continuing this process up and across the matrix sets a theoretical tolerance line.

When prioritising risks the P6:I4 box is the first priority or the most important risk to be managed. The priority is led by the impact axis – i.e. P5:I4 followed by P6:I3, P4:I4 followed by P5:I3 followed by P5:I2 and so on.

The risk matrix is given below:

PROBABILITY	**Very High P6**				
	High P5				
	Significant P4				
	Low P3				
	Very Low P2				
	Almost Impossible P1				
		I1 Negligible	**I2 Minor**	**I3 Major**	**I4 Critical**
		IMPACT			

Stage 4 - Risk Management

Once the risks have been prioritised the next step is to identify actions to help control the risk. Most risks are capable of being managed – either by managing down the likelihood or impact or both. Relatively few risks have to be avoided or transferred however the response should always be the one that is best suited. Action plans will also identify the resources required to deliver the improvements, key dates and deadlines and critical success factors as well as detailing the risk and control owners.

These plans should not be seen as a separate initiative and are incorporated into the existing business planning process. Therefore the results of the risk management work will be fed into the corporate planning, service planning and budgeting process. Ownership of each action plan needs to be allocated to appropriate members of staff with appropriate seniority and ability to drive the progress of the action plans. It will therefore be their responsibility to develop the actions required to mitigate the risks and complete the plans. The corporate Risk Register and Action plan template is shown in Appendix 3.

Stage 5 - Monitoring and reporting

Monitoring the progress of action plans will be done as part of the Council's Performance Management process. This ensures the integration of risk management with other processes and ultimately ensure its profile and success is maintained. This is achieved through the recording and monitoring of risks within the corporate performance system called Pentana. The system sends email reminders to risk owners on a regular basis to review and re-assess the risk, adding comments regarding mitigating actions.

The strategic risk register is reviewed, updated and reported quarterly in the report to CLT, and to Cabinet and Audit Committee.

The operational risk register holds service specific, project and partnership risks and is also updated quarterly or quarterly with exception reporting in the quarterly report at the discretion of Heads of Service e.g. if the risk has increased sufficiently to cause concern corporately or if additional mitigating action is required.

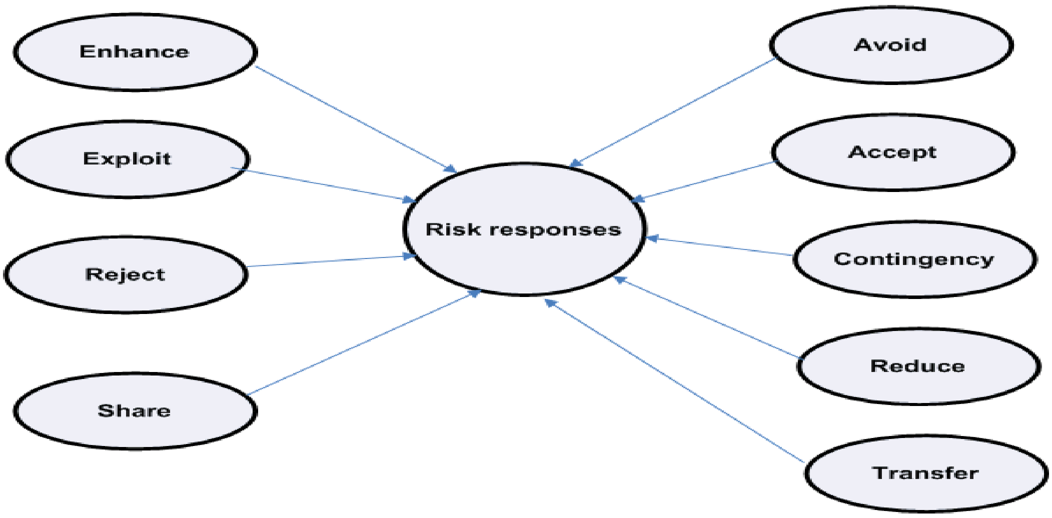
Stage 6 – Response

The response(s) to a given risk should reflect the risk type, the risk assessment (likelihood, impact, and criticality) and the organisation's attitude to risk. There are a number of possible responses to risks and as risks can be threats or opportunities these include responses that are suitable for potential opportunities

Risk Review dates

Risk type	**Minimum review due**	**Action taken**
Corporate	No less than 3 months	Controls to be evaluated and treatment to lower risk.
Service	No less than 3 months	Controls to be evaluated and treatment to lower risk. Service Director to decide if risk to be elevated to corporate risk register.
Project	As per PID (Project Initiation document)	Controls to be evaluated and treatment to lower risk. Service

		Director on the advice from the Project Sponsor to decide if risk to be elevated to corporate risk register.
Health and Safety	No less than 2 years	Service health and safety risk *assessments* should be reviewed and updated at least every two years although significant changes to work process or accidents/incidents would mean they are reviewed at the time of change or incident occurrence / investigation
Business Continuity	No less than annually	Business Continuity Policy stipulates annual review (as a minimum) for service level business continuity plans and critical function plans
Insurance	No less than 3 months	Controls to be evaluated and treatment to lower risk. Service Director to decide if risk to be elevated to corporate risk register.
Legal	No less than 3 months	Controls to be evaluated and treatment to lower risk. Service Director Legal & Governance to decide if risk to be elevated to corporate risk register.
ICT Security	No less than 3 months	Assessed and monitored at service level and elevated to Service Director when exceeding risk tolerance levels, the Service Director may elevate to the Corporate Leadership team.



Risk response	Description
Threats	
Avoid	The risk is avoided e.g. change in strategy
Transfer	Some or all of the risk is transferred to a 3rd party
Reduce	Action is taken to reduce either the likelihood of the risk occurring or the impact that it will have
Accept	The risk may be accepted perhaps because there is a low impact or likelihood
Contingency	A plan is put in place to respond if the risk is realised
Opportunities	
Share	An opportunity is shared with a partner or supplier to maximise the benefits e.g. through use of shared resource/technology
Exploit	A project could be adjusted e.g. to take advantage of a change in technology or a new market
Enhance	Action is taken to increase the likelihood of the opportunity occurring or the positive impact it could have. e.g. Strategic/commercial opportunities such as new partnerships, new capital investment
Reject	No action is taken and the chance to gain from the opportunity is rejected. Contingency plans may be put in place should the opportunity occur.- Political or environmental e.g. new transport links, change of government bringing positive changes in policy/opportunities

Links to other risk-related areas of work

- Fraud awareness and training – Finance team
- Emergency planning and business continuity – Corporate Risk Manager
- Insurance – Finance team
- Health & Safety – Health & Safety officer
- Information management and security – ICT Technical & Security Manager

Appendix 2 – Corporate Timeline Service Managers Checklist

Task	By When	Progress	Completion Date
Financial			
Review of budgets	End November		
Review of fees and charges	End November		
Review of contracts			
Review of year end employee unused benefits	6 April		
Review of year end spend/ income and accruals/ prepayments	6 April		
Monitor service spend	ongoing		
Capital bids	twice year to be agreed by CLT		

Service planning/ performance/ risk			
Review of front line service plans	End February		
Review of support service plans	End March		
Finalise service plan based on year end performance	End April		
Monitor performance and productivity	ongoing		
Quarterly risk register review	Mid-June		
	Mid October		
	Mid-January		
	Mid-April		
People			
PDRs – front line services	End March		
PDRs –support services	End April		
Workforce planning/ service needs analysis/ skills audits	Mid- February		
Business Continuity			
Review risk assessments	End September		
Review business continuity service plans	End December		
Review of critical function plans	End December		
Other health and safety			
Equalities			
Review equalities report	Yearly (by end of January)		

Appendix 3 – The Risk Register & Action Plan –

Ashfield

DISTRICT COUNCIL

2019/2020 Risk Register & Action Plan

Last updated by	C Clarke	09/11/2020
Approved by		
Document Owner		

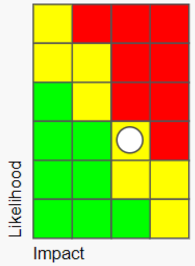
INDEX

Risk Matrix

PROBABILITY or LIKLIHOOD					
	Very High P6				
	High P5				
	Significant P4				
	Low P3				
	Very Low P2				
	Almost impossible P1				
		I1 Negligible	I2 Minor	I3 Major	I4 Critical
		IMPACT			

(ADC) CR032b-c Level of central government funding 2020 onwards

Current | Compare | Description



Impact **3** Critical
Likelihood **3** Low
Score 9

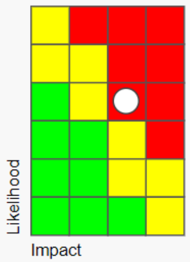
Assessment **3x3** Critical - Low
Date Assessed 27 Oct 2020

Next Assessment due 01 Jan 2021

Update

(ADC) CR072 Risk of Government's Waste strategy setting unattainable targets around recycling and service provision. Including the requirement to provide free garden waste service and separate food waste collections

Current | Compare | Description



Impact **3** Critical
Likelihood **4** Significant
Score 12

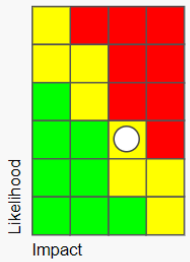
Assessment **3x4** Critical - Significant
Date Assessed 21 Sep 2020

Next Assessment due 01 Jan 2021

Update

(ADC) CR083 Failure to Support and Safeguard Vulnerable people

Current | Compare | Description



Impact	3 Critical
Likelihood	3 Low
Score	9 —

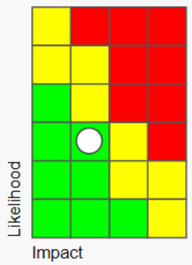
Assessment	3x3 Critical - Low
Date Assessed	21 Sep 2020

Next Assessment due 01 Jan 2021

Update

(ADC) CR032b-a Business Rates appeals are higher than forecast

Current | Compare | Description



Impact	2 Marginal
Likelihood	3 Low
Score	6 —

Assessment	2x3 Marginal - Low
Date Assessed	27 Aug 2020

Next Assessment due 01 Jan 2021

Update

Risk Review Timetable

	Jan 22	Feb 22	March 22	April 22	May 22	June 22	July 22	August 22	Sep 22	Oct 22	Nov 22	Dec 22
Cabinet		X				X			X			X
Audit Cttee	X		X			X			X			X
CLT	X				X			X			X	
DMT		X		X		X		X		X		X
Service areas	X		X		X		X		X		X	

Previous Cabinet reports are held locally on the s drive as well as published on Modern.gov as part of the agenda for the meeting.

Risk Management reporting: This is held in Pentana and is updated in real time and available on request from the Corporate Performance Lead.