Derby City Council
Risk Management Handbook
2018

Derby City Council

Contents

FOREWORD

In my role as Chair of the Audit and Accounts Committee, I am pleased to provide the foreword to Derby City Council's Risk Management Handbook.

As the management of risk is key to the successful delivery of public services, we must clearly demonstrate that all risks are fully considered in the delivery of all our services.

The Audit and Accounts Committee has an important role to play as it is responsible for considering, approving and monitoring the effective development and operation of risk management in the Council.

The Council is committed to an effective, systematic and proportionate approach that will minimise risk and enable the Council to optimise its contribution to the achievement of our vision for Derby.

The unprecedented pressure on the council's budget will mean that the need to identify and manage risk has never been more crucial. The council's insurance and risk advisors have commented that '*understanding and mitigating risk is critical when budgets are squeezed*'. As the impact of the budget cuts is felt, the Council will inevitably be forced to have more of an appetite for risk in that it 'cannot do everything' and will face 'hard choices'.

Effective management of risk is essential in ensuring that the Council is ready for the further challenges that lay ahead and in supporting a 'culture of innovation' and moving from a 'risk averse' to a 'managed risk' approach.

This handbook explains how the risk management process will be embedded into the Council's culture and form a central part of the management process. It aims to improve the effectiveness of risk management across the Council. Effective risk management allows us to:

- Have increased confidence in achieving our priorities and outcomes
- Reduce threats to acceptable levels
- Take informed decisions about developing opportunities
- Improve partnership working arrangements and corporate governance.

Effective risk management helps the Council to maximise its opportunities and minimise the impact of the risks it faces, thereby improving its ability to deliver priorities and improve outcomes.

This Handbook explains Derby City Council's approach to risk management, and the framework that will operate to manage those risks effectively.

Councillor Paul Hezelgrave
Chair of Audit and Accounts Committee

INTRODUCTION

The Council recognises that Risk Management is an integral element of Corporate Governance and a key contributor to ensuring a robust internal control environment. The management of risk is considered good practice within the public sector.

Risk Management can be defined as the culture, process and structure that are directed towards effective management of potential opportunities and threats to the organisation achieving its objectives.

The Council will establish and maintain a systematic framework and process for managing corporate, operational, project and partnership risks which will be outcome focussed. This will include assessing risks for likelihood and impact, identifying and allocating responsibility for implementing mitigating controls and receiving assurances to ensure successful management of those risks and that the controls are complied with.

The Risk Policy within this handbook formally affirms the Council's strategic commitment to building a risk management culture in which risks and opportunities are identified and managed effectively. The Council recognises that, in pursuing its strategic objectives, measured risk-taking is both acceptable and appropriate.

This Risk Management Handbook provides details on the principles and processes identified in the Council's Risk Policy. It includes resources which have been designed to assist with the risk management process and to encourage a consistent and comprehensive language and approach to managing risk across the whole Council.

The main purpose of this handbook is to:-

- Ensure a common level of understanding of risk identification assessment and management across the Council
- Ensure the process of risk management is developed and managed in a consistent manner
- Encourage the embedding of risk management throughout the Council
- Promote a culture of risk awareness.

All members, employees, service providers, partners, and stakeholders are expected to play a positive role in ensuring that effective risk management is embedded into the culture and activities of the Council.

What good Risk Management will allow us to do is:

- Create focus towards objectives
- Help inform and manage change
- Give flexibility in responding to issues
- Support innovation
- Improve transparency and justify decisions
- Inform the budget & MTFP process
- Identify the appropriate level of controls
- Share knowledge in controls
- Protect reputations

The Council will review the Policy and Strategy annually and any variations from this Policy will be agreed by the Audit and Accounts Committee.

Don McLure
Interim Strategic Director of Corporate Resources

1. Risk Management Process

Whilst risk management is a statutory requirement it is not simply a compliance exercise but an indispensable element of good management and corporate governance, which is essentially the way an organisation manages its business, determines strategy and objectives, and goes about achieving its goals.

Risk management will help identify and deal with the key risks facing the Council in the pursuit of its goals and its implementation is crucial to the Council and essential to its ability to discharge its various functions: as a partner within the Local Strategic Partnership, a deliverer and commissioner of public services, a custodian of public funds and a significant employer.

The Risk Management Process outlined within this Practical Guide should be used as a guide to best practice in managing risks which could impact strategic priorities, operational activities (e.g. delivery of actions identified in team plans) and delivery of projects or programmes.

Derby City Council has well-established risk management approaches in place for Health Safety and Welfare and Business Continuity Management and Emergency Planning. Various mechanisms also exist to manage projects and programmes. This risk management Practical Guide does not supersede the specific guidance issued in relation to those risk areas but supports it.

Derby City Council's risk management process consists of five steps:

A step-by-step guide follows to enable you to understand the risk management process.

This document should be read in conjunction with the Council's Risk Management Strategy available from the intranet. Further advice and assistance on risk management is available from Director of Governance, lead officer for Risk Management across Derby City Council.

Derby City Council defines risk as:

The chance of something happening that may have an impact on objectives

And Risk Management as:

"A planned and systematic approach to the identification, evaluation and control of those risks which can threaten the objectives, assets, or financial wellbeing of the Council."

2. Stage 1 – Risk identification

Risk identification attempts to identify the Council's exposure to uncertainty. To ensure that key risks are identified the process requires imagination, creativity, ingenuity and wide involvement as well as a methodical framework.

This is the most important step of the process, as it enables us to articulate risks associated to the achievement of our objectives enabling management of these risks in the subsequent stages.

There are a wide range of methods available that can be used to identify and understand risks. The method that you select will depend upon the type of risk(s) that you are dealing with.

Risks can be identified in a number of forums, including:

- A 'brainstorming' session or workshop with the whole management team
- Interviews
- Meetings with smaller groups of people
- Questionnaires to participants

Additionally, existing sources of information could help inform this stage. Some examples are listed below:

- Council, directorate or service plans
- Existing risk registers
- Committee reports
- Partners' documented or perceived views of risk, for example their own risk registers
- Internal or external research papers or statistical trends
- Risks or issues raised by internal audit or any other external scrutiny body
- Risks identified through budget setting process
- Health & safety risk assessments
- Business continuity risk assessments
- Partnership, programme or project documentation (e.g. business case or project risk register)
- Experience of those running or participating in the risk identification process

It is the responsibility of those identifying risks to decide which sources of information they should consult. This may be one or more of the sources listed above or it could be something else you think is appropriate. What is vital is that this is a group exercise that considers the views of a range of relevant staff, or members, for the risk assessment. No one person holds all the risks so involving others will ensure the process is as comprehensive as possible.

It is crucial for risks to be defined properly at this stage. Failure to do so can result in confusion about the exact nature of the risk, ineffective risk controls being implemented, or the risk analysis being over or underestimated.

At Corporate Level, the approach focuses on identifying strategic risks. The risks identified are:

- Those that could significantly impact on the achievement of the Council's aim and strategic priorities;
- Recorded in the Strategic Risk Register; and
- Used to inform directorate risk identification

At Service Level, the approach focuses on identifying the risks to service objectives. The risks identified are:

- Those that could significantly impact on the achievement of the service objectives;
- Recorded in each Service's Operational Risk Register; and
- Used to inform the strategic risk identification.

For major projects, the approach focuses on identifying the risks that could impact on the successful delivery of the project. Risk management will be incorporated at the conceptual stage of the project and embedded within the project management arrangements for the duration of the project. The risks identified are:

- Those that could significantly impact on the achievement of the project and its objectives;
- Recorded in the Project Risk Register; and
- Potentially used to inform both Strategic and Service risk identification.

For significant partnerships, the risks to the Council as well as the risks to the partnership itself need to be considered. Risks to the Council from partnerships are:

- Those risks to the achievement of the Council's vision and key objectives (or departmental or service objectives) from being involved in the partnership or the partnership going wrong; and
- Recorded in the appropriate risk register (Strategic or service).

Within the partnership the Council and all of the partners should consider:

- Those risks that could significantly impact on the achievement of the partnership and its objectives;
- Recorded in the partnership risk register (which may or may not be maintained by the Council); and
- Used to inform Council risk assessments.

2.1 Describing the risk.

As part of the risk identification process it is important to consider the scenario that accompanies the risk. This step is concerned with describing risks in sufficient detail and then recording the risk in a consistent format to support effective decision making on the way that the risk is managed. The information that is gathered needs to be analysed into risk scenarios to provide clear, shared understanding and to ensure the root cause of the risk is clarified. Risk scenarios also illustrate the possible consequences of the risk if it occurs so that its full impact can be assessed.

The description of the risk should include three elements:

- Risk Title
- Description
    - Situation or event (real or perceived), that exposes us to a risk/statement of fact (the background). (What, Why, Where?)
    - The trigger event - Include the event that could or has occurred that results in an impact on the objectives being achieved (How, Why, When?)
- The likely consequences if the risk materialises (The impact, How big? How bad? How much? - Consider worst likely scenario)

To assist in describing risk here is a list of “do’s” and “don'ts”.

Do		**Don’t**
• Think about internal and external influences that might affect delivery of the objectives, e.g. customer needs, stakeholder needs and strategy and key performance indicators. • Think about what resources you need to deliver the objectives and whether there is any uncertainty around having these in place. • Think about the background and what is driving the risk so that you can understand what the real risk is • Think only about the risk that will affect the delivery of objectives		• Describe the impact of the risk as the risk itself • Describe everyday issues when the outcome is already known. • Define risks with statements which are simply the converse of the objectives.

It is also useful to map each risk scenario against one of the relevant corporate objectives. Although in practice this can be difficult as many of the risks will be quite broad and have a relationship to more than one objective, in this case the primary objective should be identified.

As a further guide in Appendix B, we have included some example areas of potential risks.

3. Stage 2 – Risk Analysis

Prioritising risks against potential impact and likelihood enables management to easily identify risks which require additional resources to bring within agreed tolerances for the council.

For each scenario a risk score will be calculated at two distinct levels and in the order shown below:

Inherent (Gross) risk – the likelihood and impact of the risks identified will need to be considered as if no controls exist.

Residual risk – the likelihood and impact are re-scored based on an evaluation of the effectiveness of the existing controls or the measures that are put in place.

A matrix is used to plot the risks (each risk should be given an identifying number which is then plotted into the appropriate square on the matrix) and once completed this risk profile clearly illustrates the priority of each risk.

When assessing the potential impact of a risk and its consequences these should be linked back to the appropriate objective(s). At the strategic level this would be the impact of the risks on the achievement of the Vision and key objectives, whilst in services this would be the achievement of service objectives and priorities. The challenge for each risk is how much impact it could have on the ability to achieve the objectives.

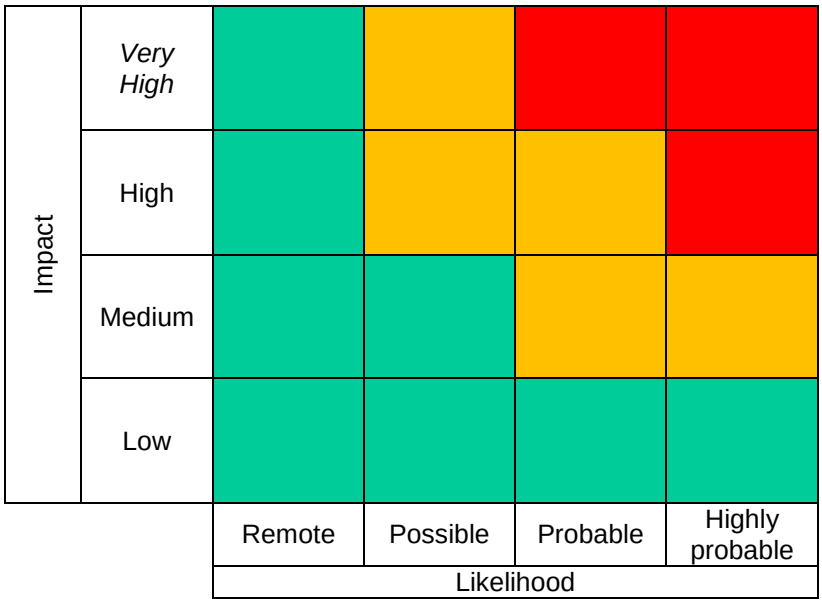
Likelihood is assessed by asking how likely it is that the trigger event should occur. The combination of both allows the Council to plot the risks on the matrix and set the risks in perspective against each other. Those risks towards the top right hand corner with higher likelihoods and impacts are usually the most pressing with the priority falling as we move down to the bottom left hand corner, however each risk will be judged individually and management actions considered in accordance with the Council's appetite to risk.

It is important when scoring the likelihood and impact of risks that a balanced view is taken with contributions from relevant team members and stakeholders. If there is real doubt over where to score a risk or agreement cannot be reached then it is best to place the risk in the higher category of likelihood and/or impact and escalated for consideration with senior officers.

At the beginning of this stage a timeframe needs to be agreed, and the likelihood and impact should be considered within the relevant timeframe. For example the likelihood of a risk occurring in the next 12 months could be very different to its likelihood of occurring in the next 3 years. It is suggested that strategic risks are assessed over the medium term – likelihood of the risks occurring in the next 3 years. Service risks would be assessed over the short term – likelihood of the risk occurring in the next 12 months.

Having assessed the likelihood and impact of each risk, the risk is plotted on the Risk Matrix, shown in figure 1. Guidelines of each category of likelihood and impact are outlined in **Appendix A.**

Figure 1.



4. Stage 3 – Risk Treatment

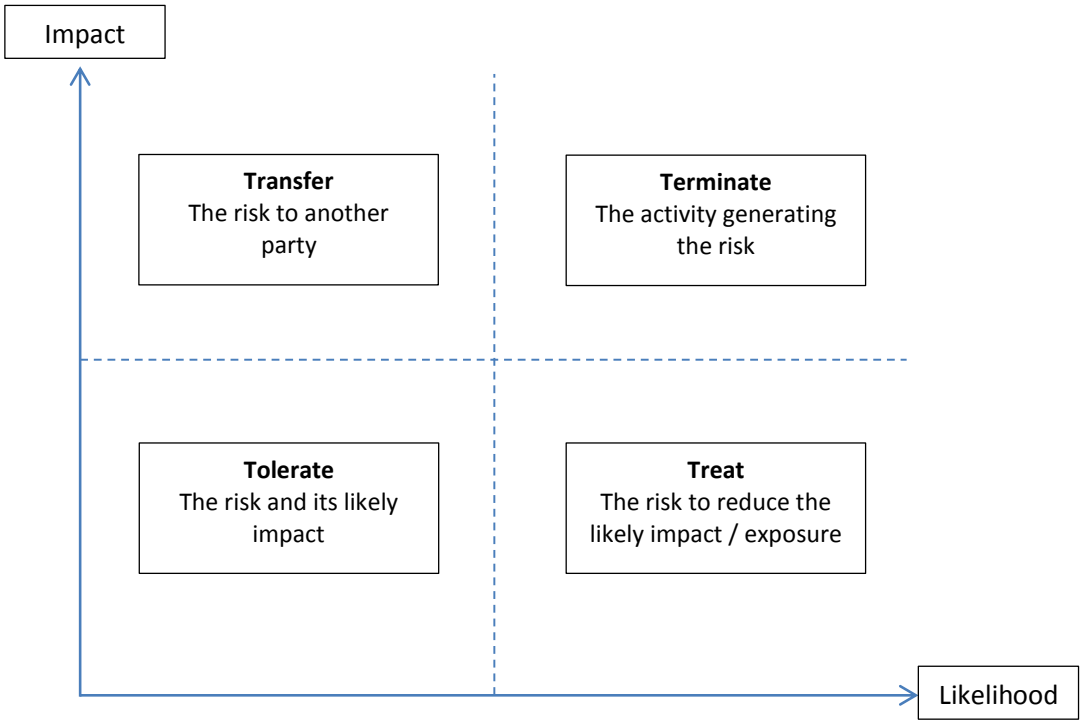
Once the risks have been prioritised the next step is to identify how to manage the identified risk. This is vitally important as it is during this stage that improvement actually occurs. Derby City Council have adopted the 4T's methodology for management of risks, these are:

Response	Which means?	Example
Tolerate	Do nothing 'extra' to manage the risk.	There will be some risks where your current control measures in place are sufficient to reduce the likelihood and impact of the risk to a tolerable level and there is no added value in doing more e.g. not cost effective or realistic to try and manage it any further. Alternatively there are some risks that are outside of your control and the organisation has no influence over them e.g. likelihood of the Government introducing legislation that has a negative impact on the Council. The Council therefore has to accept that these risks exist, will monitor them and take limited action if and when possible.
Treat	Mitigating the risk by managing either: I. the likelihood II. the impact III. or both	This is the most likely form of management for the majority of risks. Developing SMART actions to manage the likelihood of risks occurring, their impact if they were to occur, or both. Often preventative controls are used to mitigate likelihood – to ensure something does not happen e.g. training so that staff do not do something in the wrong way or fire walls to prevent computer virus attack. The impact is often mitigated with some kind of contingency e.g. alternative service providers or alternative service arrangements.

Transfer	Insurance/ outsourcing/ partnerships	Insurance, although essential for many types of risk, will not be applicable for most of the risks an organisation may face. Outsourcing or entering into partnerships may allow an organisation to transfer certain risks – however by entering into such arrangements an organisation will inevitably be faced with new and different risks which it will have to manage.
Terminate	Stop doing a activity	In some instances, a risk could be so serious that there is no other option but to terminate the activity that is generating the risk. In practice this can be difficult for a local authority given the number of statutory functions. However many authorities have stopped providing a non-statutory service due to the risks surrounding their operation.

The 4T's are shown in figure 2 in diagram form.

Figure 2.



The most common way to manage a risk is to produce and implement an action plan that identifies the resources required to deliver the improvements, key dates and deadlines and critical success factors/Key Performance Indicators.

Firm ownership of the risk and an accompanying action plan is vital so that the responsibility is clear and progress can be monitored.

These plans should not be seen as a separate initiative but should be incorporated into the existing business planning process. The action plan format is part of the information which will be entered onto the Risk Register.

Consideration should also be given here as to the 'Cost-Benefit' of each control weighed against the potential cost/impact of the risk occurring. Note: 'cost/impact' here includes all aspects including financial, resourcing, but also reputational.

4.1 Taking Opportunities

This option is not an alternative to those previous; rather it is an option which should be considered whenever tolerating, transferring or treating a risk.

There are several aspects to this for example: -

Whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages?

Whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be re-deployed.

When risks are prioritised and it is shown that some risks are over-controlled or over-regulated then it may be that the reduction in these controls can result in saving that can be used elsewhere

5. Stage 4 – Completing the Risk Register

The risk register is the tool which facilitates data collection and records the identified risks, their mitigations and associated scoring of impact and likelihood. A standard format for data collection has been designed in DORIS and includes the following areas:

Risk Reference	unique sequential number for each risk
Risk Title	Brief reference to the risk
Risk Description	Outline of the risk and the events which cause this to materialise
Risk Cause	What is the root cause of the identified risk, ask yourself why?
	Is it training, processes, finances, budget constraints…etc… which are causing the risk to materialise
Consequences	What will happen in the event of the risk materialising – financial, reputational, sickness, injury. Consider worst case scenario.
Inherent score	Score of risk based on likelihood of occurring and impact prior to any mitigating actions being implemented
Mitigations	Identification of mitigations, prioritised based on impact the actions will have on the scoring and timescales identified.
Current Score	Risk score based on current position, taking into account mitigations already applied
Risk Owner	Named individual with responsibility for the risk. This should be managed at the lowest level possible for the nature of the risk.
Commentary	Free text field to provide updates and story over the life of the risk
Escalation reason	Risks can be reported at 3 levels within the organisation (Departmental, Directorate, Strategic) escalations between the levels require this field completing Free text field to outline reason / justification for escalation and requested input needed.

6. Stage 5 – Monitoring, Reporting and Reviewing the Risks

Monitoring of risks and the associated mitigations is to be undertaken by:

- being part of existing performance monitoring;
- focusing on those risks above the tolerance line (score) that, because of their likelihood and impact, make them priorities; and
- Be delegated to one responsible body (risk owner).

To achieve this, the following monitoring/review process and frequency must be followed:

- **High level risks** (with a score of 9 or above) need to be monitored either monthly or every 2 months by the Management Team.
- Strategic risks will be monitored quarterly by the Risk Management Team (January, April, July & October) linking into the Performance reporting process. The strategic risk register (containing all risks) will be reported to the Chief Officer Group (COG) and Audit and Accounts Committee on a quarterly basis.
- At a department level, operational risk registers will be reviewed quarterly. Any key operational risk which needs to be escalated to a strategic risk register will be considered by COG within the quarterly risk management report.
- At project level, monitoring is undertaken by individual Project Boards supported by the relevant Project Manager
- At partnership level, monitoring is undertaken by individual Partnership Boards.

The frequency of review will be in line with the tolerance levels set on the risk matrix.

The risk register is to be updated with any relevant commentary information following these review / reporting milestones.

7. Risk Management Organisational Structure

The risk management process is a continuous one and risks can therefore be reported at any time. However risks will be formally reported as follows:

- The Chief Officer Group (COG) will formulate the Council's strategic risk view on a quarterly basis - this will ensure that there is always an up to date view of the key risks facing the Council and how they are being managed;
- The COG will consider and agree the key strategic risks on a quarterly basis;
- The COG will be supported by a newly formed Corporate Risk Management group, chaired by Strategic Director of Corporate Resources.
- The Audit and Accounts Committee will receive risk reports on a quarterly basis;
- The full Council will receive a report on the Council's key risks on an annual basis;

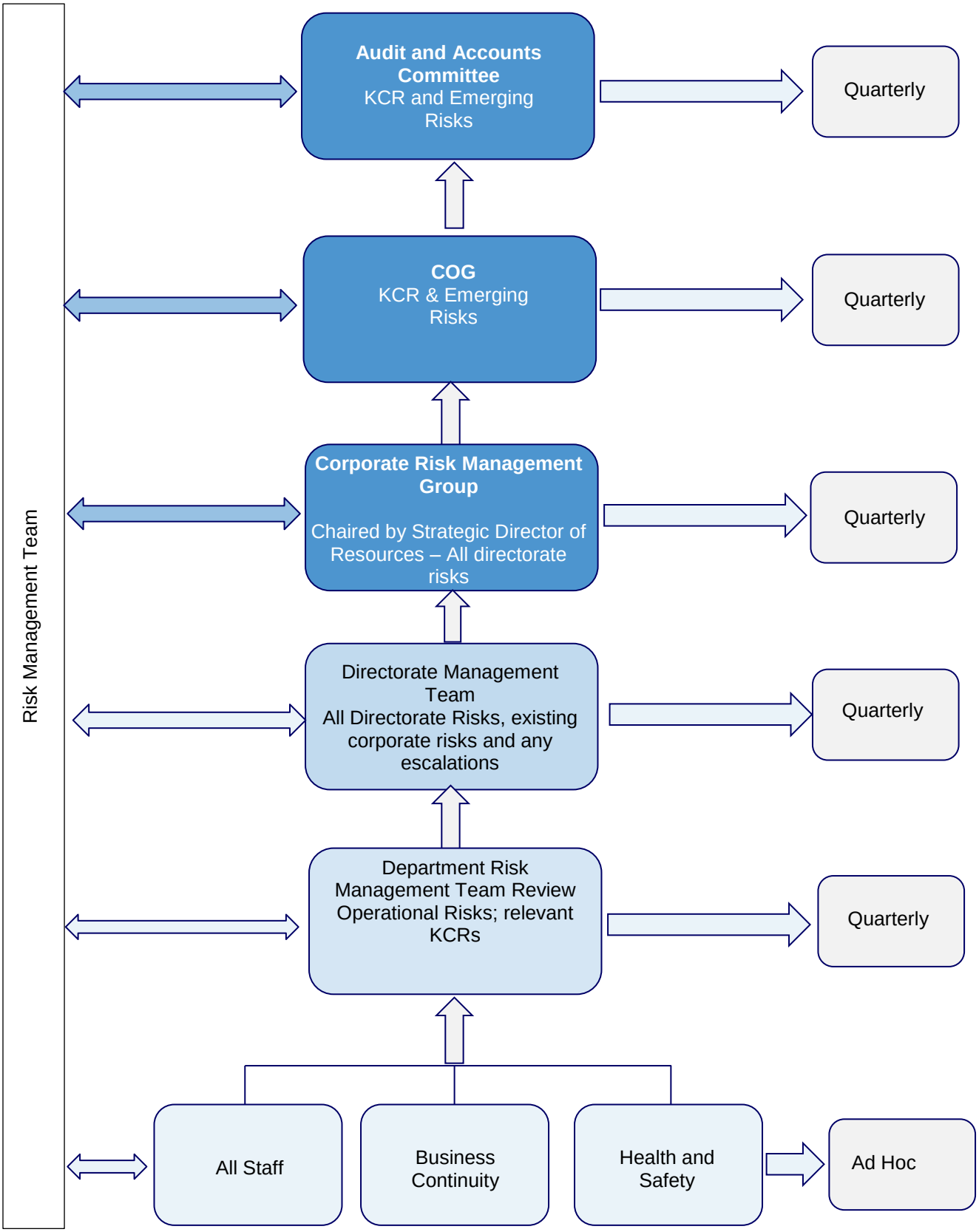
and

- Heads of Service will revisit their service risks on a quarterly basis. Should any service risks need to be escalated this would be considered by the Strategic Risk Management Group and agreed by the Senior Management Team.

The reporting structure is represented in figure 3

The frequency of review at Heads of Service, Strategic Risk Management Group and Management Team will be in line with the risk score e.g. monthly, quarterly, etc.

Figure 3



Derby City Council

Appendix A – Risk Matrix categories

The below categories are there assist in the prioritisation of risks. It is unlikely that any risk will fit neatly and adhere to all areas within each category. Officers should utilise knowledge and experience when determining risk scores.

Objectives cannot be delivered. Statutory duties not achieved, death, financial loss over £5million, adverse national media attention, litigation almost certain, breaches of law, inspection highlights inadequate service, council unable to work with partner organisation	Impact	Very High				
Significant threat to council objectives. Non-statutory duties not achieved, permanent injury, financial loss over £1million, negative national media attention, litigation expected, serious issues raised through inspection, breakdown of confidence of partners.		High				
Slight delay in achievement of service objectives, minor injuries, financial loss over £500k, adverse local media attention, breaches of local procedures		Medium				
Limited impact on service objectives if any, section objectives unlikely to be met, financial loss less than £500k, no media attention		Low				
			Remote	Possible	Probable	Highly probable
			Likelihood			
			Extremely unlikely	Fairly likely	More likely than not	Almost certain

Appendix B – Example areas of Risk

Sources of risk	Risk examples
STRATEGIC	
Infrastructure	Functioning of transport, communications and infrastructure. Impact of storms, floods, pollution.
Legislative and Regulatory	Effects of the change in Central Government policies, UK or EU legislation, local and National changes in manifestos. Exposure to regulators (auditors/inspectors).
Social Factors	Effects of changes in demographic profiles (age, race, social makeup etc) affecting delivery of objectives. Crime statistics and trends. Numbers of children/vulnerable adults 'at risk'.
Technological	Capacity to deal with (ICT) changes and innovation, product reliability, developments, systems integration etc. Current or proposed technology partners.
Competition and Markets	Cost and quality affecting delivery of service or ability to deliver value for money. Competition for service users (leisure, car parks etc). Success or failure in securing funding.
Stakeholder related factors	Satisfaction of LCC's taxpayers, Central Government, GOEM and other stakeholders.
Environmental	Environmental impact from Council, stakeholder activities (e.g. pollution, energy efficiency, recycling, emissions, contaminated land etc). Traffic problems and congestion.
OPERATIONAL (Internal influences)	
Finance	Associated with accounting and reporting, internal financial delegation and control, e.g. schools finance, managing revenue and capital resources, neighbourhood renewal funding taxation and pensions.
Human Resources	Recruiting and retaining appropriate staff and applying and developing skills in accordance with corporate objectives, employment policies, health and safety.
Contracts and Partnership	Failure of contractors to deliver services or products to the agreed cost and specification. Procurement, contract and life cycle management, legacy. Partnership arrangements, roles and responsibilities.
Tangible Assets	Safety and maintenance of buildings and physical assets i.e. plant and equipment, ICT equipment and control
Environmental	Pollution, noise, licensing, energy efficiency of day-to-day activities.
Processes	Compliance, assurance, project management, performance management, revenue and benefits systems, parking systems etc.
Professional Judgement and Activities	Risks inherent in professional work, designing buildings, teaching vulnerable children, assessing needs (children and adults).
CORPORATE GOVERNANCE	
Integrity	Fraud and corruption, accountability, transparency, legality of transactions and transactions and limit of authority.
Leadership	Reputation, authority, democratic changes, trust and branding.
Policy and Strategy	Clarity of policies, communication. Policy Planning and monitoring and managing performance.
Data and information for decision making	Data protection, data reliability and data processing. Control of data and information. E-government and service delivery.
Risk Management	Incident reporting and investigation, risk analysis or measurement, evaluation and monitoring. Taking advantage of opportunities.