# Derby
# Risk Management Handbook
# 2020 edition



**Version History**

| Version | Alterations | Approved by | Date |
|---|---|---|---|
| 1.1 | Amended document written with external consultancy support (Zurich) | Audit and Accounts Committee | March 2018 |
| 1.1 | Document reviewed | Corporate Risk Management Group | December 2019 – March 2020 |
| 2.1 | Amended document written following document review | Audit and Accounts Committee | November 2020 |
| | | | |
| | | | |

Derby City Council

# Contents

Derby City Council

## 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. Good risk management will allow us to:

- create focus towards our objectives, with an awareness of challenges;
- inform and manage change; managing threats and taking positive action to opportunities;
- give flexibility in responding to issues and risks, within our agreed 'risk appetite';
- support innovation;
- improve transparency and justify decisions;
- inform the budget & Medium-Term Financial Planning processes;
- identify the appropriate level of controls;
- share knowledge on controls and actions; and
- strengthen and protect reputations.

A positive risk culture is one where every person in a business believes that thinking about and managing risk is part of their job

It creates the tone and sets expectations

It modifies behaviour to what is expected

It underpins risk based decision making

Leadership    Information    Accountability    Responsibility    Competence    Communication

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 the successful management of those risks and that the controls are complied with.

The contents of this handbook formally affirm 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; and the 2020 edition of this Handbook sees more guidance on managing risks as opportunities.

This Risk Management Handbook 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 councillors, colleagues, 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.

We will review both this document and the Risk Management Strategy at least every two years, and any variations will be agreed by the Audit and Accounts Committee, who will also be engaged in review activity.
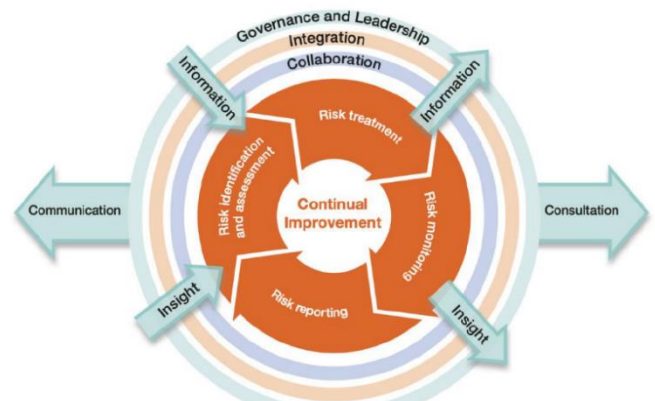
## Risk Management Process

Whilst risk management is a statutory requirement, it is not simply a compliance exercise. It is 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.



*Source - HM Government: The Orange Book Management of Risk Principles and Concepts 2019*

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 the 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 on iDerby.  Further advice and assistance on risk management is available from the Assurance Team (Policy, Communications and Insight – performance@derby.gov.uk).

In line with ISO 31000 definition of risk management, Derby City Council defines a risk as:

*"The chance of something happening that may have an impact on our 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."*

## 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 the 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. In all types of risk identification, it is important that you scan the horizon, considering both internal and external factors that can impact. There are a number of tools available to do this, with SWOT (an analysis of; strengths, weaknesses, opportunities and threats) and PESTLE (political, environmental, social, technological, legal and economic) analysis used most frequently to aid our horizon scanning.

> **Risk or Issue?**
> An 'issue' is something that is here today, as appose to a 'risk' that is something that has the potential of happening at some point in the future. The simplest way of distinguishing issues from risks is to ask whether the likelihood of the situation occurring is 100% (i.e. certain). If it is certain or if it has already happened, then it is an issue; if not, it is a risk.
> Issues should be documented on an issue log not a risk register.

Risks can be identified in a number of forums, including:
• business planning workshops
• 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 risk identification. Some examples are listed below:
• council, directorate, service or team plans
• existing or historical risk registers

- committee reports
- inspection reports or peer review findings
- performance information
- customer insight including complaints
- benchmarking information
- 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
- contracts, procurement activity, analysis of the market and sufficiency for commissioned services
- partnership, programme or project documentation (e.g. business case or project risk register)
- experience of those running or participating in the risk identification process.

> **Emerging risks**
>
> A 'hazard' can be defined as 'unassessed loss of potential'. A risk assesses this potential.
>
> A key part of our risk management framework, emerging risks are risks that are in the early stages of risk identification, which we are yet to fully define and capture on a risk register. To ensure that we do not lose this valuable intelligence we have an emerging risk log that can be added to at any time.

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 that 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. Reflecting on historical examples of risk management going wrong can assist in avoiding the same mistakes.

There are a number of tools available that can assist in the early stages of risk identification (i.e. flow charts, root cause analysis and risk bow ties). Each tool available breaks down the 'event' to allow a systematic assessment of the possible risks (both threat and opportunities). More details on these tools are available in Appendix 1.

**At Corporate or Strategic 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 (i.e. the Council Plan);
- recorded in the Strategic Risk Register; and
- used to inform directorate and department risk identification.

**Strategic**
- Major risks to organisation
- Reported to CRMG, SLT & Cabinet quarterly

**Directorate**
- Significant risks which cut across departments / services
- Reported to DLTs & CRMG and exception reporting to SLT quarterly

**Department**
- Risks affecting delivery of objectives in business plans
- Monitored by DLTs quarterly

**Project**
- Risks to project delivery - monitored by project boards regularly
- Should be escalated to directorate risk registers if required

**Service**
- Technical / team operational risks
- Day to day decision making

**At Service Level**, the approach focuses on identifying the risks to service objectives (i.e. Business Plans). 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, which may result in risk escalation.

**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:
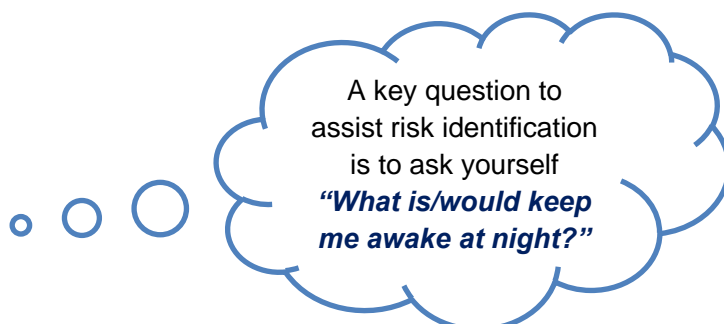- those that could significantly impact on the achievement of the project and its objectives;
- recorded in the Project Risk Register; and
- potentially used to inform both strategic and service risk identification.

**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).

In 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;
- those recorded in the partnership risk register (which may or may not be maintained by the Council); and
- council risk assessments.

A key question to assist risk identification is to ask yourself *"What is/would keep me awake at night?"*
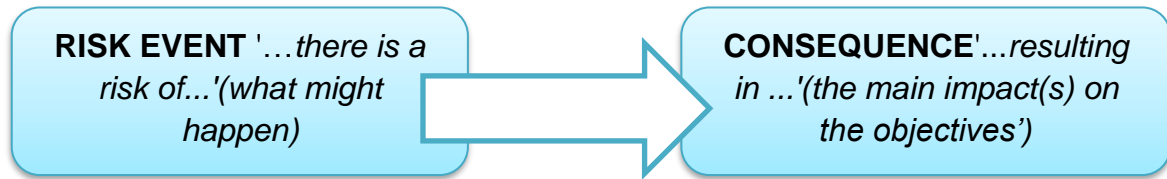
### Describing the risk

As part of the risk identification process it is important to consider the scenario or event 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 in 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 the worst likely scenario)

When identifying risk, using the below format can help when defining and describing the risk.

**RISK EVENT** '…*there is a risk of...'(what might happen)* → **CONSEQUENCE**'...*resulting in ...'(the main impact(s) on the objectives')*

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.<br><br>• Think about what resources you need to deliver the objectives and whether there is any uncertainty around having these in place.<br><br>• Think about the background and what is driving the risk so that you can understand what the real risk is.<br><br>• Think only about the risk that will affect the delivery of objectives. | • Describe the impact of the risk as the risk itself<br><br>• Describe everyday issues when the outcome is already known.<br><br>• 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 3, we have included some example areas of potential risks.

## Stage 2 – Risk Analysis

Prioritising risks against potential impact and likelihood enables management to easily identify risks which require additional resources to bring them 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 risk identified will need to be considered as if **no** controls exist.

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

**Risk target score / tolerance** – what the risk will be when further action has been taken.

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 below.

| | | Remote | Possible | Probable | Highly probable |
|---|---|---|---|---|---|
| **Impact** | *Very High* | 4 | 8 | 12 | 16 |
| | High | 3 | 6 | 9 | 12 |
| | Medium | 2 | 4 | 6 | 8 |
| | Low | 1 | 2 | 3 | 4 |
| | | Likelihood | | | |

The process of evaluating risks as opportunities is the same as evaluating a risk as a 'threat', and they can also be plotted onto our Risk Matrix:

| | | | | | |
|---|---|---|---|---|---|
| 16 | 12 | 8 | 4 | Significant - 4 | **Impact** |
| 12 | 9 | 6 | 3 | Moderate - 3 | |
| 8 | 6 | 4 | 2 | Minor - 2 | |
| 4 | 3 | 2 | 1 | Insignificant – 1 | |
| 4 Highly probable | 3 Probable | 2 Unlikely | 1 Rare | | |

Likelihood

Guidelines of each category of likelihood and impact for both risks as threats and opportunities are outlined in Appendix 2.



***Which diving board would you dive from?***

*The identification and assessment of risks and opportunities will depend upon experience, knowledge and skills. Assessments of risk must take into account national and local context, alongside factors that affect both impact and likelihood. Group identification and assessment will aid a balanced view. Different services may have a different interpretation of risk, but this should fit within our organisational risk appetite and where we are willing to take risks.*

## 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:<br><br>I. the likelihood<br><br>II. the impact<br><br>III. or both | This is the most likely form of management for most 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 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 an 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.
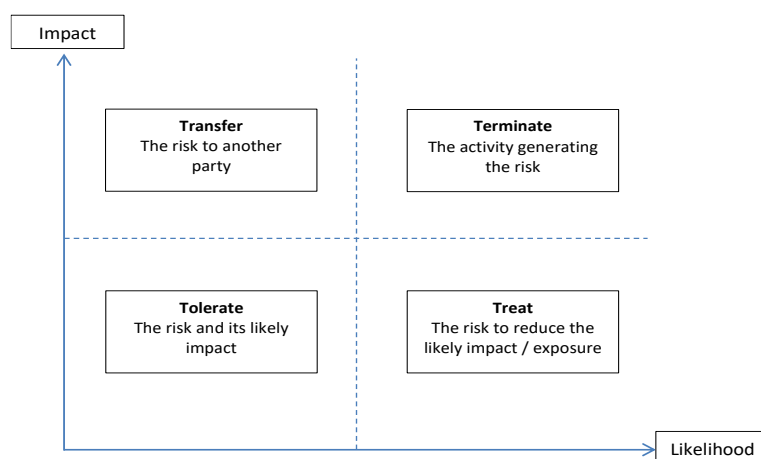
The most common way to manage a risk is to produce and implement an action plan that identifies the resources required to deliver the improvements, key dates and deadlines and critical success factors/Key Performance Indicators.

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.

### Risk opportunities

The approach for assessing and agreeing what action to take with respect to 'risk opportunities' can also be broken down into four categories…

| Response | Which means? | Example |
|---|---|---|
| *Take* | Taking new action(s) | Seeking to make the opportunity happen and putting in place measures to ensure that the benefits of the opportunity are maximised and realised.<br><br>The decision to 'take' an opportunity is likely to be set out within our strategic vision and aims, requiring capacity to be identified to support it; ensuring that the maximum benefit is realised. |
| *Enhance* | | Put in place actions to increase the impact or likelihood of the opportunity.<br><br>The decision to 'enhance' an opportunity is most likely to be taken at a department and/or service level, where actions can be undertaken through 'business as usual activity' or through the identification of an objective within our business planning cycle. |
| *Share* | Acting alongside others | Managing the opportunity through partners or key stakeholders to maximise the chance it will happen and increase the benefits.<br><br>This may be the course of action decided upon in areas of opportunity that impact bigger proportions of the city / our communities and therefore require wider input. |
| *Ignore* | Taking no deliberate action(s) to increase the likelihood of the opportunity being realised. | A minor opportunity may not require explicit actions.<br><br>The opportunity, once fully analysed, may not be considered worth the 'costs', so no action is to be taken. |

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. Risks within the Council's framework are assessed under the 'best case' and 'worst case' scenarios to allow a balanced and informed judgment on how the risk should be managed going forward.

It should also be noted, that when risks are prioritised it is shown that some risks are over-controlled or over-regulated, and a reduction in controls can result in savings that can be used elsewhere.

In most cases it is appropriate to identify mitigations to put in place to prevent a risk from occurring, or to identify actions to increase the impact and likelihood of an opportunity; however when deciding how to manage the risk there should be consideration given to our risk appetite.

There is no 'single' risk appetite for the Council. Different risks and activities will have different risk levels and 'appetite' associated with them; in the same way we may define risk as either threats or opportunities differently, depending on what area of service they relate to. Despite this, any level of risk appetite must be linked to our vision and priorities/outcomes.

There must also be consideration given to the effectiveness of controls, as a more 'relaxed' approach to risk controls in instances where we are tolerating risk can result in weaker outcomes.

> ***Risk Appetite is defined as being the organisation's willingness to accept risk in pursuit of its business objectives. It also forms part of the overall framework around which decisions are made and is dynamic.***

> ***Why is risk appetite important, and what are the benefits?***
> - *It sets clear boundaries for risk taking (i.e. not being too risky, or too cautious)*
> - *It will focus resources into addressing the most significant risks / opportunities*
> - *It will bring focus to higher priority risks and concerns*
> - *Ensures that responses to risk(s) are appropriate and proportionate*
>
> ***Ultimately it is about making better, more informed decisions…within an environment that you understand and have fully assessed.***

## 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 and includes the following areas:

| | |
|---|---|
| ***Risk reference*** | A 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 – worst case*** | What will happen in the event of the risk materialising – financial, reputational, sickness, injury. |
| ***Consequences – best case*** | When analysing the risk are there any opportunities? Consider the same factors as you would when assessing the risk as the threat (i.e. financial, reputational, service delivery, compliance (what is the minimum expectation?), wellbeing etc.). |
| ***Inherent score*** | Score of risk based on likelihood of occurring and impact prior to any |

mitigating actions being implemented

**Controls**  Identification of controls or mitigations prioritised based on the impact the actions will have on the scoring and timescales identified. Controls are defined in Derby as 'actions that are already in place and require maintaining'. If there is something new that needs to happen to reduce the risk or optimise the opportunity, then it should be reflected as an action. Each quarter, risk owners will be asked to confirm controls remain in place.

**Action**  Further, additional action to be taken to reduce the risk score. These are 'new activities'. Each quarter, risk owners will be asked to assess whether their actions are 'on track', or if there is either 'some slippage' or 'major slippage', both of which could impact on our overall assurances of our risk mitigations.

**Current score**  Risk score based on current position, taking into account mitigations already applied.

**Risk treatment**  Risk owners are asked to select which of the 4T's are being used to manage the risk as a 'threat' and/or, which of the 4-risk opportunity criterion are being employed for the current period. Risk owners will be asked to review their risk treatment every quarter to make sure that it remains up to date, reflecting the dynamic nature of many service areas. One or more treatment measure can apply to risks.

**Target risk score or risk tolerance**  The level of risk which we aspire to get to if all controls are in place and all actions that can be taken are fully implemented. When assigning a target/tolerance score risk owners should consider the period of time required for actions to positively impact on the risk level. Are there ways that the impact of the controls and actions can be assessed? (*Please refer to Stage 5).* The target risk score should be set within our risk appetite, reflecting the level at which, we as a Council, are willing to 'tolerate' the risk.

**Risk owner**  Named individual with responsibility for the risk. This should be managed at the lowest level possible for the nature of the risk.

**Risk updater**  Named individual with responsibility for the updating this risk, if this is someone different to the Risk Owner. This risk updater may be the individual responsible for the implementation of the controls and/or actions, with more detailed knowledge on current levels of assurance. Any updates provided will always require the sign off of the Risk Owner.

**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.

A guidance for updating our risk registers is available on iDerby. Templates for risks can also be found online or can be requested from performance@derby.gov.uk.

## Stage 5 – Monitoring, Reporting and Reviewing the Risks

Monitoring of risks, opportunities 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
- being delegated to one responsible body (risk owner).

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

| | |
|---|---|
| **High-level risks** | • With a score of 9 or above<br>• Need to be monitored monthly by the Risk Owners, with updates provided to the Assurance Team as requested/agreed. |
| **Strategic risks** | • Monitored quarterly by the Assurance Team and Corporate Risk Management Group (January, April, July & October) linking into the performance reporting process.<br>• The strategic risks will be reported to the Strategic and Corporate Leadership Teams, and Cabinet, on a quarterly basis. |
| **Directorate risks** | • Monitored quarterly by the Assurance Team and Corporate Risk Management Group (January, April, July & October) linking into the performance reporting process.<br>• Directorate risks will be reported to Directorate Leadership Teams (DLTs) on a quarterly basis.<br>• All Directorates have a nominated Risk Champion (Assurance Advocate), who are individuals identified within each directorate with responsibility to support risk management processes within their directorate. |
| **Department level risks** | • Operational risk registers will be reviewed quarterly through Senior Management Teams (SMTs).<br>• Annual review of risk themes by the Corporate Risk Management Group.<br>• Any key operational risk which needs to be escalated to a strategic risk register will be considered by DLTs and CLT within the quarterly risk management report. |
| **Project level** | • Monitoring of project risks is undertaken by individual Project Boards, supported by the relevant Project Manager.<br>• Escalation of project risks will be considered by DLTs and CLT within the quarterly risk management report.<br>• Monitoring of priority projects quarterly through the Programme Management Office. |
| **Partnership** | • Monitoring is undertaken by individual Partnership Boards, with ownership of the Partnership Register being hosted by the Council. |

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.

When risks are either 'closed' or 'de-escalated' from the strategic or directorate risk registers they will still be reported at the quarter end when this decision was taken, to ensure appropriate scrutiny on the impact of mitigations.

**Risk assurance**

A key part of the Council's Risk Management Framework is risk assurance. This is the process of reviewing, re-assessing and challenging all aspects of a risk…

- Is the risk or opportunity still relevant?
- Have there been any changes or movement to the risk or opportunity and/or its mitigations or actions?
- Has anything occurred, which might change the impact and/or likelihood and the risk score?
- Are the mitigations and actions effective, and what has the progress been?
- If the risk or opportunity is increasing, are any further mitigations or actions needed to prevent or enhance its occurrence?
- If the risk or opportunity is decreasing, can any of the mitigations or actions be relaxed?
- Are there any new or emerging risks or opportunities?

Many aspects of risk assurance are undertaken on an on-going basis, as risks are mitigated, with targeted analysis every quarter in line with our reporting cycles. In addition to this, we have identified 'tiers' of further scrutiny and challenge, using the governance for the monitoring of risks set out within our Risk Management Strategy, as part of our cycle of continuous improvement.

When deciding whether to undertake more targeted analysis of a risk, Risk Owners should have re-visited Stages 1 and 2 of our risk management cycle to ensure that the risk is accurate, before a full review of mitigations.

| Type of assurance | What? | When? | Who? |
|---|---|---|---|
| 1. **Business as usual** | On-going analysis of risk and opportunities by risk owners/project managers; including updates as part of quarterly risk monitoring reports. | On-going, with quarterly reporting in line with established reporting frameworks. | • Risk updaters and owners<br>• SMTs and DLTs<br>• Risk Champions/ Assurance Advocates |
| 2. **Deep-dive risk reviews** | Targeted analysis of specific risks and opportunities from the strategic or directorate risk registers, where one or more of the following criteria are met:<br><br>o Previously established risk controls have been identified as no longer being in place.<br>o The current risk/opportunity score is above 9, and there has been no change/progress in controls/actions for 6 months or more.<br>o The risk score exceeds 9, and there has been major slippage in mitigating actions for two or more consecutive quarters.<br>o The inherent risk score is the same as the current risk score, despite identified mitigations. | To be identified through quarterly reporting.<br><br>Deep dive risk reviews can also be requested by Risk Owners.<br><br>Internal Audit will align their audit programme to risk registers to provide further assurance, completing deep | • Assurance Team<br>• Corporate Risk Management Group<br>• SLT and/or CLT<br>• Internal Audit<br><br>*NB - The outcomes of deep-dive reviews completed on Strategic Risks should be reported to Cabinet and Audit and Accounts as part of our assurance framework.* |

| Type of assurance | What? | When? | Who? |
|---|---|---|---|
| | o Risk tolerance/target scores have been set and not achieved within 'specific timescales'.<br>o There has been a change in the risk score but no change in mitigations. | dive assessment through formal audits. | |
| 3. **Risk surgeries** | Targeted analysis of specific risks from the strategic risk register, where mitigations have not been sufficient to reduce the risk score, and this has subsequently resulted in the risk becoming an issue for the Council; to inform learning for future risk assurance activity. | To be identified through assurance monitoring reports. | • Audit and Accounts Committee with support from the Assurance Team<br>• Cabinet |

To ensure effective and targeted use of capacity, and a focus on our 'highest risks', it is recommended that there are no more than two deep-dive risk assessments and/or risk surgeries supported by the Assurance Team in any quarter/3-month period.

## 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 Strategic Leadership Team (SLT) 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 SLT will consider, alongside the Corporate Leadership Team (CLT) and agree the key strategic risks on a quarterly basis;

- SLT and CLT are supported by an established Corporate Risk Management Group, chaired by the Director of Legal, Procurement and Democratic Services and Monitoring Officer that meets at least on a quarterly basis;

- Council Cabinet will receive updates on strategic risks on a quarterly basis, as part of performance monitoring reports;

- The Audit and Accounts Committee will receive an assurance report on a six-monthly basis;

- The full Council will receive an update on the Council's key risks on an annual basis, as part of the Annual Report;

- Directors and Heads of Service will revisit their service risks frequently to ensure that registers are kept dynamic and up to date. Reviews should be held on a quarterly basis, as a minimum. Should any service risks need to be escalated this would be considered by the Corporate Risk Management Group and agreed by the Senior Leadership Team; and

- All service and department risks will be subject to an annual review (as a minimum) through the review and refresh of business plans.

A summary of the reporting framework is presented on page 18.

All roles and responsibilities pertaining to the Council's Risk Management Framework are set out in the Risk Management Strategy, which is available on iDerby.
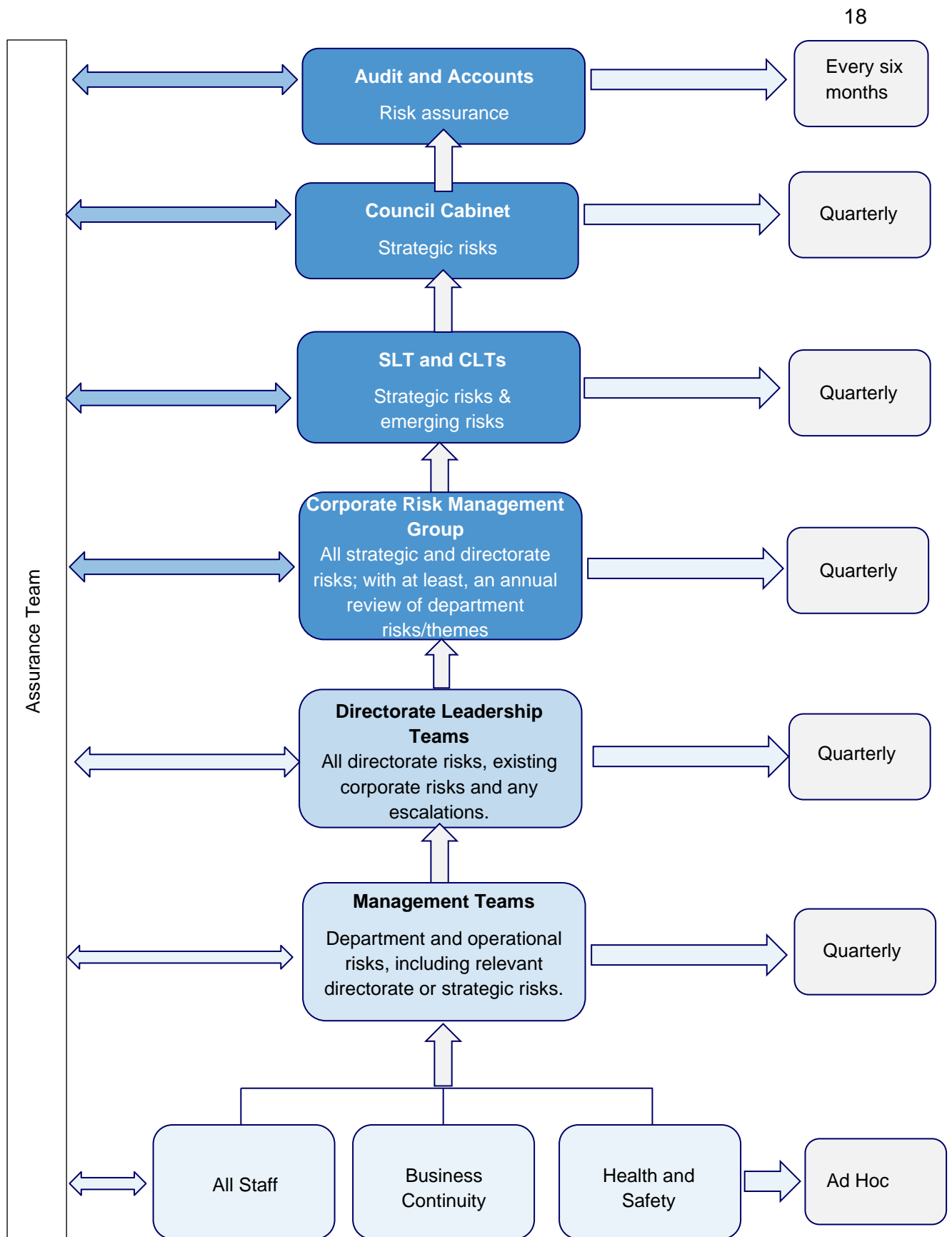
*Project risks should be reported through the established project governance, with reporting to the Programme Management Office Board at least once every quarter. More frequent monitoring may take place on priority projects through SLT and CLT.*

*Partnership risks are monitored through the Partnership Board, with the partnership register being reviewed at least annually.*

## Risk Management Culture and Training

Successful organisations manage risk effectively. This does not mean that they avoid risk at all costs. They make allowances for the risks they face to achieve what they want; seeking opportunities alongside the management of risks as threats.

The purpose of risk management is to anticipate and manage the significant risks you face that could stop you from achieving what you want to achieve.

In order to support effective risk management in the Council, we have identified risk roles and responsibilities that are set out within our Risk Management Strategy. Key to embedding our risk management culture are the Assurance Team that leads on risk management, our Corporate Risk Management Group and directorate Risk Champions (Assurance Advocates).

| Corporate Risk Management Group | <ul><li>Chaired by the Director of Legal, Procurement and Democratic Services and Monitoring Officer.</li><li>Attended by Risk Champions (Assurance Advocates) for each Directorate, subject matter experts in priority areas and members of the Assurance Team.</li><li>Consider escalated operational risks and recommend actions to mitigate.</li><li>Promote a risk aware culture and embed risk management throughout the Council.</li><li>Review and challenge directorate, department and operational risks.</li><li>Preparing, monitoring and reviewing the strategic risk register.</li><li>Inform the review and refresh of Derby City Council's Risk Management Strategy and Handbook.</li><li>Undertake deep dive reviews of risk to seek assurance on controls/actions.</li><li>Horizon scan on matters related to; local and national policy, finance, insurance, safeguarding, emergency planning, project management, health and safety, performance and audit, to inform a strategic assessment of current threats and opportunities.</li><li>The Corporate Risk Management Group has overall responsibility for identifying, analysing and scoring strategic and service risks; to ensure consistency in the application of the risk management matrix.</li></ul> |
|---|---|
| Assurance Team | The Assurance Team are pivotal in the promotion and embedding of risk management by managing a culture change within the Council. They are responsible for managing strategic risks, as well as supporting services in their individual areas of responsibility. Assurance Team key tasks are to:<ul><li>review the Council's approach to risk management and supporting processes and recommend for approval any subsequent changes;</li><li>recommend any appropriate changes to the Risk Management Strategy to councillors;</li><li>support and promote risk management throughout the Council – ensuring that it works effectively;</li><li>actively identify, analyse and profile strategic risks on a quarterly basis;</li><li>determine and prioritise actions on strategic risks, allocating individual ownership of the key risks to appropriate members of the Strategic Leadership Team and/or Corporate Leadership Team;</li><li>receive escalated directorate and service risks and consider their inclusion onto the strategic risk register;</li><li>propose the "risk appetite" of the Council i.e. the definition of high (red) risk, medium (amber) risk and low (green) risk;</li><li>monitor progress of risk arrangement activities as part of existing</li></ul> |

| | performance management approaches; <br> • coordinate deep-dive risk assessments and risk surgeries; <br> • report quarterly to Cabinet on strategic risks and their management; <br> • issue a six-monthly report to Audit and Accounts on risk assurance; and <br> • ensure that the Council has robust processes and procedures in place that are consistently applied, for the management of operational risks, including project risks. |
|---|---|
| **Risk Champions (Assurance Advocates)** | • Individuals identified within each directorate with responsibility to support risk management process within their directorate. <br> • Act as point of contact for officers within the directorate to assist in the application of Risk Management. <br> • Attend the Corporate Risk Management Group, providing updates on strategic and operational risks from within their Directorate. <br> • Responsibility for supporting Derby City's aim of embedding risk management across the organisation. <br> • Identifying areas of non-compliance with Risk Management Strategy, and escalating issues as appropriate. |

To develop a mature risk culture all of our colleagues and councillors have a key role to play in risk management, to:

- manage risk effectively in their jobs, reporting opportunities and risks to their service managers;
- adhere to Council policies and procedures;
- attend training and development sessions as appropriate; and
- participate in risk assessment and action planning, where appropriate.

Risk management training will be coordinated by the Assurance Team. An annual programme will be agreed through the Corporate Risk Management Group, with targeted sessions available, as required.

Further tools and information on risk management are available on iDerby, including the details of nominated Risk Champions (Assurance Advocates) that can assist in the application of this Handbook.

If, after reading this document, you would like any further information or you would like to request a bespoke training session please contact performance@derby.gov.uk

**Tools for risk identification**

**SWOT analysis**

SWOT stands for Strengths, Weaknesses, Opportunities, and Threats, and so a SWOT Analysis is a technique for assessing these four aspects of your service, which will allow you to think in a balanced way about risks, as threats and opportunities, in the context of your service strengths and areas for improvement.

Find out what's working well, and what's not so good. Ask yourself where you want to go, how you might get there – and what might get in your way.

| Strengths | Weaknesses |
|---|---|
| • What do you do well? <br> • What do others see as your strengths? <br> • What evidence do you have to confirm these? <br> • Are your areas of strength sustainable? | • What could you improve? <br> • Where does capacity/resources impact on the service? <br> • What are others likely to see as your weaknesses? <br> • How do you compare to other similar services? |
|  |  |
| Opportunities | Threats |
| • What opportunities are you open to? <br> • What national and/or local trends could you take advantage of? <br> • How can you turn strengths, weakness or threats to opportunities? | • What threats could harm services and/or customers? <br> • Are threats within our risk appetite? <br> • What are others doing in response to threats? <br> • What threats do your weaknesses expose you to? |
|  |  |

**PESTLE analysis**

PESTLE (Political, Economic, Social, Technological, Legal, Environmental) is a form of strategic analysis that allows us to reflect and plan, by highlighting the factors that may affect our services. A PESTLE is broken down into six categories referencing different types of acts that can or will affect the topic chosen for analysis. It is best completed in small groups and can inform the identification or both risks and opportunities at many different levels.

**Political factors**: Politics, politicians, government — both local and national. Examples:
- National policies
- Local policies / decision making
- Health & Safety

**Economic factors**: services, monetary value, currency, and the economy are affected by economic factors. Examples:
- National policies (i.e. Comprehensive Spending Review)
- National and local funding

- Income and charges
- Demand for costly services

**Social factors**: our communities, residents and their behaviours and needs. Examples:
- Demographics
- Cultural differences
- Ethnicities
- Employment
- Location

**Technological factors**: digital technology. Examples:
- Appliances
- Programs and software
- Websites
- Social media

**Legal factors**: the way in which particular laws influence how we deliver services and what services we deliver. Examples:
- Statutory duties
- Planning regulations
- General Data Protection Regulations
- Freedom of Information and Subject Access requests

**Environmental factors**; physical changes in our 'space' – local, national or worldwide. Examples:
- Green spaces and parks
- Climate change
- Air quality
- Flooding

### Flow chart exercise

Once a service area has been identified for further exploration to identify and analyse risks and opportunities, a risk flow chart exercise can be helpful. All individual steps in a process need to be broken down and assessed individually for risks and opportunities, these can then be assessed 'as one' to determine which risks are within our 'risk appetite' and what areas we feel need mitigation.

A key question in a flow chart exercise is; ***What might happen to disrupt the successful completion of each component of the flow?***

Traditionally, flow chart analysis is used for identifying operational risks, as it enables the flow to be broken down into manageable component parts. A key benefit of this approach is that it encourages a systematic and detailed focus on each component part of a process, highlighting the critical links between each 'task' and subsequently what the key service risks might be. It is a good exercise to do to engage colleagues in the identification of risk and opportunities, as it encourages participation. It can also be used alongside a LEAN review to improve the efficiency of a process within a service area.

## Risk bow ties

A risk bow tie is a form of risk assessment or tool that can be used to identify both proactive and re-active risks; allowing both to be mitigated.

It is a very visual form of risk identification, as shown below, and allows the relationships between different aspects of risk definition (causes and impacts) and controls to be clearly mapped out, allowing more targeted assurance activity at a later date.

| Controls or actions to treat causes | Causes | Risk | Impacts | Controls or actions to treat impacts |
|---|---|---|---|---|

## Risk management matrix and categories

Derby City Council's Risk Management matrix aims to provide a comprehensive framework, systems and processes to identify, evaluate and manage risks as both threats and opportunities. It has been refreshed, as part of the 2020 review, to integrate risk opportunity into our organisational culture and to encourage an environment of both challenge and innovation.

| Risk – Threats | | | | | | Risk – Opportunities | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Impact** | Very high – 4 | 4 | 8 | 12 | 16 | 16 | 12 | 8 | 4 | Significant - 4 | **Impact** |
| | High - 3 | 3 | 6 | 9 | 12 | 12 | 9 | 6 | 3 | Moderate - 3 | |
| | Medium - 2 | 2 | 4 | 6 | 8 | 8 | 6 | 4 | 2 | Minor - 2 | |
| | Low – 1 | 1 | 2 | 3 | 4 | 4 | 3 | 2 | 1 | Insignificant – 1 | |
| | | 1 Remote | 2 Possible | 3 Probable | 4 Highly probable | 4 Highly probable | 3 Probable | 2 Unlikely | 1 Rare | | |
| | | **Likelihood** | | | | **Likelihood** | | | | | |

## Derby City Council Risk Matrix – Analysis Criteria

| Threats criteria | | Opportunities criteria | |
|---|---|---|---|
| **Impact** | **Thresholds and Description** | **Impact** | **Thresholds and Description** |
| 1 – Low | Limited impact on service objectives if any, section objectives unlikely to be met, financial loss less than £500k, no media attention | 1 – Insignificant | • Little or no improvement to service<br>• Little or no improvement to welfare of staff / public<br>• Little or no financial income / efficiency savings (less than £500k)<br>• Little or no improvement to environment or assets<br>• Little or no feedback from service users |
| 2 – Medium | Slight delay in achievement of service objectives, minor injuries, financial loss over £500k, adverse local media attention, breaches of local procedures | 2- Minor | • Minor improvement to service<br>• Minor improvement to welfare of staff / public<br>• Improvement that produces £500k+ of income / efficiency savings<br>• Minor improvement to environment or assets<br>• Positive user feedback |
| 3 – 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. | 3 – Moderate | • Moderate improvement to service<br>• Moderate improvement to welfare of staff / public<br>• Improvement that produces £1million of income / efficiency savings<br>• Moderate improvement to environment or assets<br>• Positive local media contact |
| 4 – Very high | Objectives cannot be delivered. Statutory duties not achieved, death, financial loss over £5million, adverse national media attention, litigation almost certain, prosecutions, breaches of law, inspection highlights inadequate service, council unable to work with partner organisation | 4 – Significant | • Significant improvement to service<br>• Significant improvement to welfare of staff / public<br>• Improvement that produces £5million or more income / efficiency savings<br>• Significant improvement to environment or assets<br>• Positive local media coverage |

| Threats criteria | | Opportunities criteria | |
|---|---|---|---|
| **Likelihood** | **Description** | **Likelihood** | **Description** |
| 1 – Unlikely | May occur only in exceptional circumstances (e.g. once in 10 years) | 1 – Rare | Opportunity has not been fully investigated but considered extremely unlikely to materialise |

| Threats criteria | | Opportunities criteria | |
|---|---|---|---|
| **Likelihood** | **Description** | **Likelihood** | **Description** |
| 2 – Possible | Unlikely to occur but could at some time *(e.g. once in 3 years)* | 2 – Unlikely | Opportunity has not been fully investigated; achievability is unproven / in doubt |
| 3 – Probable *(in 2 years)* | Fairly likely to occur at some time or under certain circumstances *(e.g. once in 2 years)* | 3 – Probable *(in 2 years)* | Opportunity may be achievable, but requires significant management, planning and resources. |
| 4 – Highly probable *(in 12 months)* | Will probably occur at some time or in most circumstances *(e.g. once in 12 months)* | 4 – Highly probable *(in 12 months)* | Opportunity is achievable with careful management. |

## Examples of 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. Supply chain reliance. |
| **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. |

We can give you this information in any other way, style or language that will help you access it. Please contact us on: 01332 640767 Minicom: 01332 640666

## Polish

Aby ułatwić Państwu dostęp do tych informacji, możemy je Państwu przekazać w innym formacie, stylu lub języku.
Prosimy o kontakt: 01332 640767      Tel. tekstowy: 01332  640666

## Punjabi

ਇਹ ਜਾਣਕਾਰੀ ਅਸੀਂ ਤੁਹਾਨੂੰ ਕਿਸੇ ਵੀ ਹੋਰ ਤਰੀਕੇ ਨਾਲ, ਕਿਸੇ ਵੀ ਹੋਰ ਰੂਪ ਜਾਂ ਬੋਲੀ ਵਿੱਚ ਦੇ ਸਕਦੇ ਹਾਂ, ਜਿਹੜੀ ਇਸ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਸਹਾਇਤਾ ਕਰ ਸਕਦੀ ਹੋਵੇ। ਕਿਰਪਾ ਕਰਕੇ ਸਾਡੇ ਨਾਲ ਟੈਲੀਫ਼ੋਨ 01332 640767    ਮਿਨੀਕਮ 01332 640666    ਤੇ ਸੰਪਰਕ ਕਰੋ।

## Slovakian

Túto informáciu vám môžeme poskytnúť iným spôsobom, štýlom alebo v inom jazyku, ktorý vám pomôže k jej sprístupneniu. Skontaktujte nás prosím na tel.č: 01332 640767   Minicom 01332 640666.

## Urdu

یہ معلومات ہم آپ کو کسی دیگر ایسے طریقے، انداز اور زبان میں مہیا کر سکتے ہیں جو اس تک رسائی میں آپ کی مدد کرے۔ براہِ کرم   01332 640767
منی کام   01332 640666   پر ہم سے رابطہ کریں۔

Derby City Council

Derby City Council  The Council House  Corporation Street  Derby DE1 2FS
www.derby.gov.uk