Appendix 3

Derby City Council
Risk Management Handbook
2017

Derby City Council Risk Management

Contents

RISK DEFINITIONS

RISK MANAGEMENT METHODOLOGY

ADDITIONAL

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.

Richard Boneham
Head of Governance & Assurance

PURPOSE OF THE RISK MANAGEMENT HANDBOOK

This handbook, which has been developed in line with published good practice, is to provide a structured approach to the management of risk.

Risk management is an essential part of good governance within any organisation and is intended to provide a framework and process that enables an organisation to manage uncertainty in a systematic, effective, consistent and efficient way. It supports informed decision making thereby enabling opportunities to be exploited or action to be taken to mitigate or manage key risks to an acceptable level.

In addition to those goals it is also intended that this document will:

- Provide standard definitions and vocabulary to underpin the risk management process;
- Co-ordinate the approach to risk management across the Council, to ensure a consistency of process and outcome
- Clearly identify roles and responsibilities for managing risk,
- Ensure that risks are managed in accordance with best practice.

Risk management forms a key part of the corporate governance process to generate assurance that a sound system of internal control is in place. It is not about:

- Creating a totally risk free society
- Generating paper-work mountains
- Scaring people by exaggerating or publicising trivial risks
- Stopping important activities for individuals where the risks are managed

RISK DEFINITIONS

Risk

Derby City Council defines a risk as:

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

A risk is an event or occurrence that would prevent, obstruct or delay the organisation from achieving its objectives or failing to capture business opportunities when pursuing its objectives

Positive consequences or opportunities are the possibility that an event will occur and positively affect the achievement of objectives. Opportunities can be channelled back into the objective setting/business planning process, and plans formulated to seize those opportunities.

Risk management

What is risk management?

Risk management involves adopting 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. It is a means of minimising the costs and disruption to the Council caused by undesired events.

Risk Management covers the whole range of risks and not just those associated with finance, health and safety and insurance. It can also include risks as diverse as those associated with public image (reputation), the environment, technology, breach of confidentiality etc.

Risk Management is not about avoiding risks, being ‘risk averse’ – it is about being ‘risk aware’. Risk is ever present and some amount of risk taking is inevitable if the Council is to achieve its objectives.

Risk Management is about making the most of opportunities. By being ‘risk aware’ the Council is in a better position to avoid threats and take advantage of opportunities.

Risk owner

A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

Control

A control is an action to reduce either the likelihood of a risk occurring or the impact of the risk, should it occur.

Control owner

A control owner is the individual assigned with responsibility for the management of a control. They manage the implementation and maintenance of identified controls to the required level of effectiveness. Periodic confirmation that controls are in place and operating as intended will be sought.

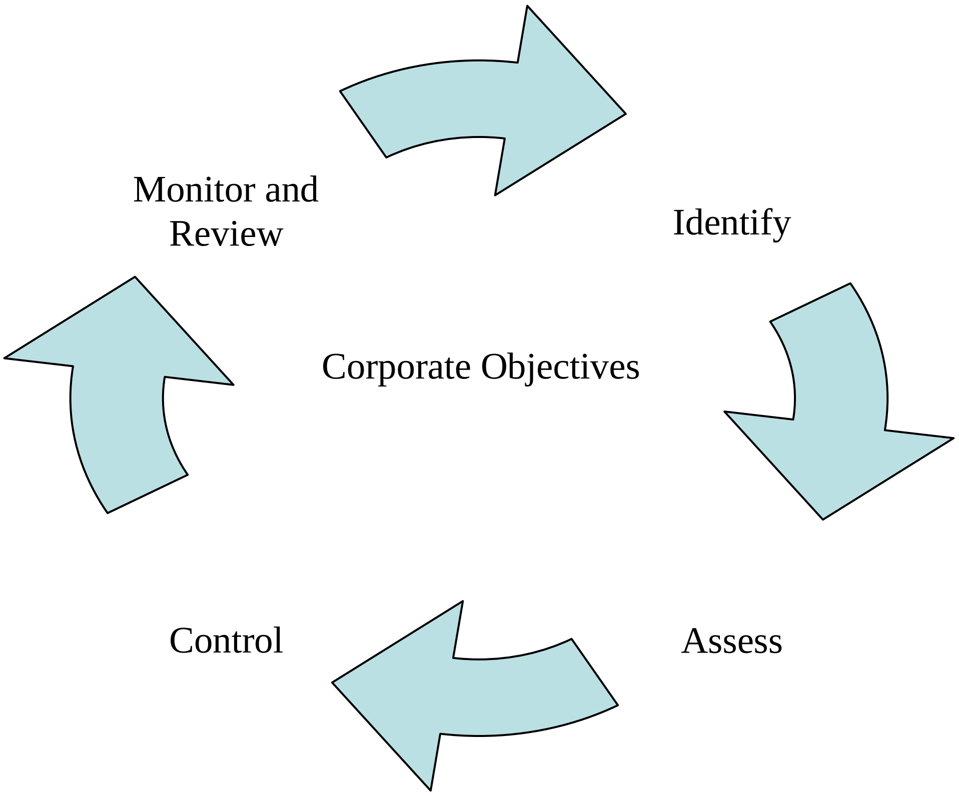
Risk appetite & Risk tolerance

Risk appetiteis the amount and type of risk the council is willing to accept in pursuit of its objectives.

Risk toleranceisthe specific **maximum** risk that an organisation is willing to take regarding each relevant risk. It’s the threshold that we will not cross even to meet the councils objectives. It’s typically determined at the higher levels of the organisation.

RISK MANAGEMENT METHODOLOGY

Risk management process



This process is applicable to all types of risk, from high level strategic issues to small scale individual projects.

Communication and Consultation

Good communication and consultation is essential for risk management and impacts at each and every stage and attempts to:

- improve people's understanding of risks and risk management processes
- ensure all relevant stakeholders are heard
- ensure that everyone is clear on their roles and responsibilities.

Managers when reviewing their risks should look to communicate and consult with all stakeholders including other relevant departments such as Health and Safety, Insurance, HR, Accountancy etc. to both seek advice and ensure all corporate policies are being followed.

Identification of Risks

In order to effectively manage risk, the Council needs to know what risks it faces, and to evaluate them. Identifying risks is the first step in building a risk profile. Firstly we have to consider what it is we are trying to achieve. Once that is known, thought can be given to what may impact on our ability to achieve our objectives.

What are our objectives?

Within the context of our established corporate priorities, Members and Senior Management establish strategic objectives, select strategy and set objectives cascading through the Council**.** Our Risk Management framework is therefore geared to achieving our objectives. Objectives must exist before we can identify potential events affecting their achievement (both positive and negative).
There is a direct relationship between objectives, which are what we are striving to achieve and risk management components, which represent what is needed to achieve them.

Risks can then be assessed and prioritised in relation to the objective.

The identification of risk can be separated into two distinct phases. They are:

- Initial risk identification (such as for a new project or activity)

- Continuous risk identification whereby new risks are identified which did not previously arise, or where there are changes in existing risks.

In each case risks should still be related to the objectives.

When a risk is identified it may be relevant to more than one of the organisation’s objectives, and the best way of addressing the risk may be different in relation to different objectives.

If there are any specific risks identified such as a health and safety risk, business continuity risk, environmental or fire risk then you would need to involve the relevant and specialist department to assist in undertaking the risk assessment.

In stating risks, care should be taken to avoid stating impacts which may arise as being the risks themselves, and to avoid stating risks which do not impact on objectives; equally care should be taken to avoid defining risks with statements which are simply the converse of the objectives.

A statement of a risk should encompass the cause of the impact, and its effects on the objective (cause and consequence) which might arise. For example:

Objective – to travel by train from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	**X** This is simply the converse of the objective
Being late and missing the meeting	**X** This is a statement of the impact of the risk, not the risk itself
There is no buffet on the train so I get hungry	**X** This does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	✓ This is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	✓ This is a risk which I cannot control, but against which I can make a contingency plan

Risks should be identified at a level where a specific impact can be identified and a specific action or actions to address the risk can be identified.

All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time.

A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed; the risk owner may not be the person who actually takes the action to address the risk.

Once I know my objectives how do I identify the risks?

The Council's chosen methodology for the identification of risk is through self-assessment by departments.

Think about what you are trying to achieve and ask yourself "what's going to impact on what I'm trying to achieve? What's going to stop me or slow me down?"

Each level and part of the Council has to review its activities and to contribute its diagnosis of the risks it faces. A particular strength of this approach is that better ownership of risk tends to be established when the owners themselves identify the risks.

For purposes of self-assessment you can use:

- Analysis of loss data (including insurance claims)
- Analysis of complaints
- Analysis of near miss and incidents data
- Judgement based on personal experience
- Brainstorming sessions with staff
- Individual interviews with managers and/or focus groups
- Undertake a SWOT analysis (identify strengths, weaknesses opportunities and threats)
- Risk surveys and questionnaires
- Benchmarking and networking
- Articles in professional or other journals which may flag up potential risk areas
- Client satisfaction surveys
- Employee satisfaction surveys
- Sickness and absence records
- Internal and external audit reports
- External inspection reports (OFSTED, HSE and other professional bodies)
- Horizon scanning (looking forward to tomorrow's threats)

Risk Management is the overall umbrella framework, which encompasses all risks. When looking at your objective you would look at all types and categories of risk that could impact on the achievement of that objective.

Successful delivery of our objectives often depends on our partners and contractors. We must, therefore, look beyond the boundary of our department or even the Council itself to identify risks to our objectives from these relationships and recognise that good risk management requires good stakeholder involvement.

Describing a Risk

It is important when describing the risk to be precise with language to avoid confusion and misinterpretation.

We should always try to phrase the risk description in such a way that ensures that it is best managed.

Good practice advises that the risk description should identify three aspects;

1. The circumstances that enable the risk to occur, often the trigger
2. The actual risk, or thing that might happen
3. The impact of the risk event occurring to the project or business

For example these are poorly framed risks;

- Failure to attend the important meeting

Anyone reading that will not know why you cannot attend the meeting or what resources or assistance is needed

- Resources are not available

Again anyone reading that will not know resources you are short of. Is it time or financial or staffing?

A more effective way of describing the risk;

- If I oversleep I could miss the train making me late for the important meeting and key information is missed resulting in failure to act in line with new protocols

- If additional financial resources are not available by [date] the project’s timetable will be affected resulting in at least a four month delay to completion

The second set of examples provide fuller descriptions that reduce the likelihood of misinterpretation and allow for a better assessment of the likelihood and impact of the risk.

That said, don’t spend so long drafting your wording that you miss the deadline to say anything at all!

Assessing the Risks

Once you have identified all the possible risks to your service area, it is necessary for you to analyse and evaluate the risks so that you may distinguish between minor acceptable risks and major risks.

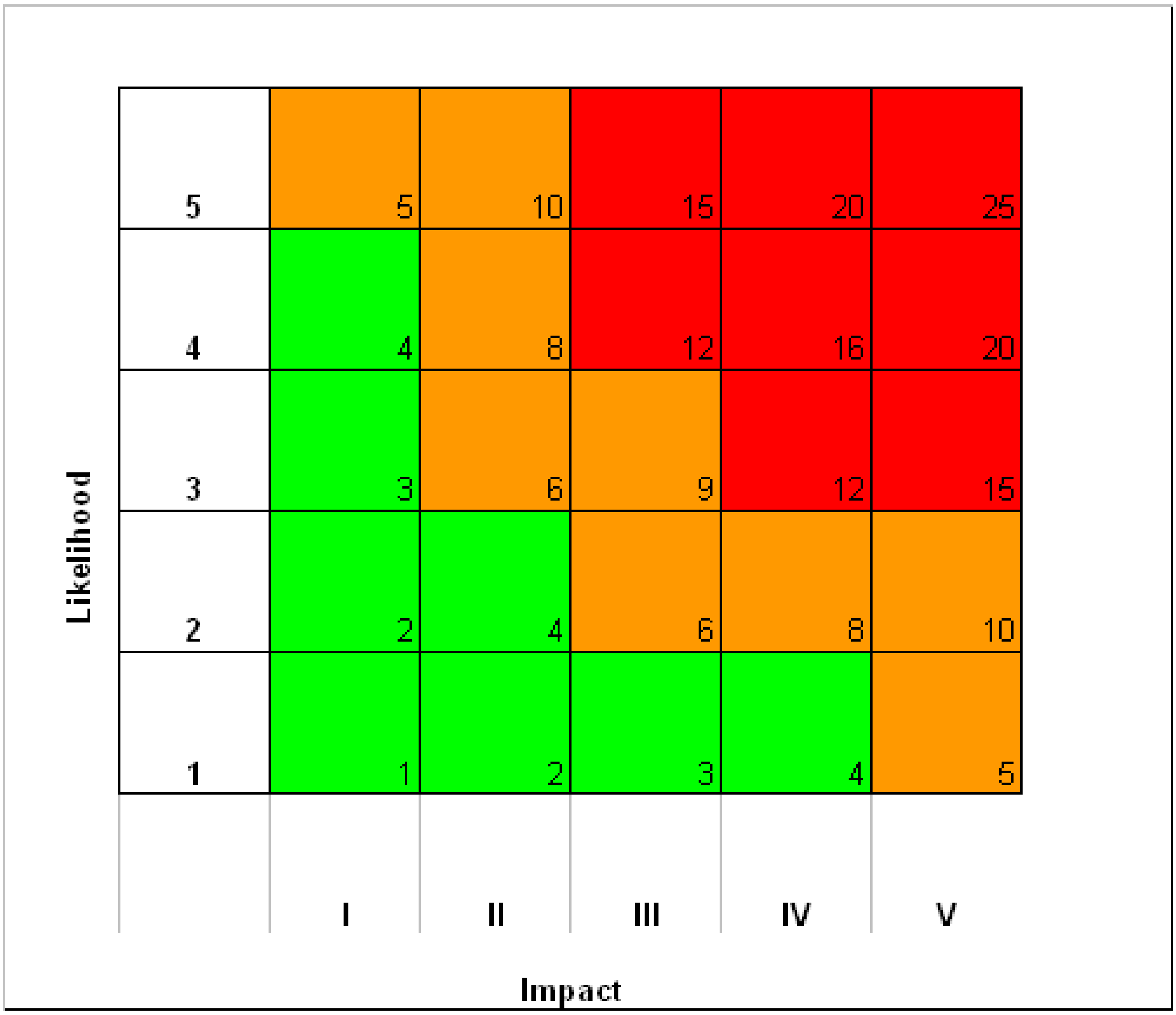
This process will also include determining the likelihood of the risk happening and the impact or consequence the risk will have on your service area should the risk occur.

The assessment should avoid confusing an impartial assessment of the risk with judgement about the acceptability of the risk. It is not the absolute value of an assessed risk which is important; rather it is whether or not the risk is regarded as tolerable, or how far the exposure is away from tolerability, which is important.

To assess the risks adequately you should give each risk a score or risk rating using the 5x5 Risk Matrix. Each impact is given a numerical score equivalent to a scale of insignificant / minor / moderate/ major/ catastrophic and likelihood on a scale of rare / unlikely / possible / likely / almost certain.

This process provides a structured way to identify, prioritise and manage the impact of the key risks/opportunities to the achievement of your objectives

The Risk Matrix



Likelihood					
5	🟧 5	🟧 10	🟥 15	🟥 20	🟥 25
4	🟩 4	🟧 8	🟥 12	🟥 16	🟥 20
3	🟩 3	🟧 6	🟧 9	🟥 12	🟥 15
2	🟩 2	🟩 4	🟧 6	🟧 8	🟧 10
1	🟩 1	🟩 2	🟩 3	🟩 4	🟧 5
	I	II	III	IV	V
	Impact				

	Likelihood of Risk			Impact of Risk	
5	–	Almost Certain	V	-	Catastrophic
4	–	Likely	IV	-	Major
3	–	Possible	III	-	Moderate
2	–	Unlikely	II	-	Minor
1	–	Rarely	I	-	Insignificant

Risk Scoring

We need to be able to compare our risks so that we can concentrate our efforts on addressing those that are most important. To do this we use the standard approach of giving each risk a score, calculated by multiplying the likelihood score by the potential impact score.

The first assessment should be undertaken on the ‘Inherent Risk’ i.e. the risk before any controls have been put into place. This is to ensure that all significant risks are highlighted and assurance provided that these risks are being managed. If you only assess the risk after controls have been put in place (Residual Risk) then you are assuming that the controls will always be there.
The second step is to assess your risks after your existing controls have been evaluated. This will give you a residual risk score and overall risk rating level.

The below is a guide to the appropriate score to allocate to the risk. **It is not definitive and is intended only as a guide**, as consideration should also be given to the nature of the objective as well as the risk that threatens it.

Guidance on likelihood ratings / scorings

Score	Definition
1 – Rare	The event may occur only in exceptional circumstances
2 – Unlikely	The event is not expected to occur
3 – Possible	The event might occur at some time
4 – Likely	The event will probably occur in most circumstances
5 - Almost Certain	The event is expected to occur in most circumstances

Guidance on impact ratings / scorings

1 Insignificant

- Loss of a service for up to one day
- Objectives of the individual are not met
- No injuries
- Financial loss of less than 1% of budget
- No media attention
- No breaches in Council working practices
- No complaints/litigation

2 Minor

- Loss of a service for one to four weeks
- Objectives of the Section are not met
- Injury to an employee or member of the public requiring onsite first aid
- Financial loss between 1% - 6% of budget
- Adverse local media attention – Local news paper report
- Breaches of local procedures/standards
- Unlikely to cause complaint/litigation

3 Moderate

- Loss of a service for one to six months
- Objectives of the Division are not met
- Injury to an employee or member of the public requiring medical treatment
- Financial loss between 6% - 25% of budget
- Adverse regional media attention – Televised or newspaper report
- High potential for a complaint litigation possible
- Breaches of regulations/standards

4 Major

- Loss of a service for six months or more
- Objectives of the Department/Directorate are not met
- Non-statutory duties are not achieved
- Permanent injury to an employee or member of the public
- Financial loss between 25% - 50% of budget
- Adverse national media attention – National newspaper report
- Litigation to be expected
- Breaches of law punishable by fine only

5 Catastrophic

- An incident so severe in it effects that a service or project will be unavailable permanently
- Strategic objectives set are not met
- Statutory duties are not achieved
- Death of an Employee or Member of the Public
- Financial loss over 50% of budget
- Adverse national media attention – National televised news report
- Litigation almost certain and difficult to defend
- Breaches of Law punishable by imprisonment

By multiplying the impact rating by the likelihood rating this produces a risk rating score. The risks can then be plotted onto a simple Risk Matrix as shown above and the level of risk determined.

Addressing / Controlling the Risks

Having identified and analysed the risks, it is necessary to decide what to do and who will do it.

The rating of risk is useful for both the prioritisation of risk and therefore controls. This ensures that risks are brought to the attention of the most appropriate staff, i.e. the most significant risks are notified at the most senior management level. The higher they are in this top corner, the higher their priority should be.

All risks identified should be managed (treated) in accordance with the Council's "risk appetite" identified above

Risk Control

Once the risk identified and evaluated the next step is to implement actions / controls in order to mitigate or manage them effectively.

In designing and implementing controls, it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of life) it is normally sufficient to design controls to give a reasonable assurance of confining likely loss within the Council's risk appetite.

Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to constrain risk rather than to eliminate it.

There are several ways to control risk. They are often referred to as the '4 Ts' and brief overview of them is as follows:

TOLERATE
The exposure may be tolerable without any further action being taken.

Even if it is not tolerable, ability to do anything about some risks may be limited; the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk.

This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

TRANSFER
For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way.

This option is particularly good for mitigating financial risks or risks to assets.

It is important to note that some risks are not fully transferable – in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk

TERMINATE

Some risks will only be treatable, or containable to acceptable levels, by terminating the activity.

It should be noted that the option of termination of activities may be severely limited in local government when compared to the private sector; a number of activities are conducted in the public sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved.

This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

TREAT
The purpose of treatment is that whilst continuing with the activity giving rise to the risk, actions are taken to constrain the risk to an acceptable level, by:

- **PREVENTIVE CONTROLS**
  These controls are designed to limit the possibility of an undesirable outcome being realised. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls.

  The majority of controls implemented tend to belong to this category.

  Examples of preventive controls include separation of duty, whereby no one person has authority to act without the consent of another (such as the person who authorises payment of an invoice being separate from the person who ordered goods prevents one person securing goods at public expense for their own benefit), or limitation of action to authorised persons (such as only those suitably trained and authorised being permitted to handle media enquiries prevents inappropriate comment being made to the press).

- **CORRECTIVE CONTROLS**
  These controls are designed to correct undesirable outcomes which have been realised. They provide a route of recourse to achieve some recovery against loss or damage.

  An example of this would be design of contract terms to allow recovery of overpayment. Insurance can also be regarded as a form of corrective control as it facilitates financial recovery against the realisation of a risk.

  Contingency planning is an important element of corrective control as it is the means by which the Council can plan for business continuity / recovery after events which it could not control.

- **DIRECTIVE CONTROLS**

These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided - typically associated with Health and Safety or with security.

Examples of this type of control would be to include a requirement that protective clothing is worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.

- **DETECTIVE CONTROLS**
  These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, ‘after the event’ so they are only appropriate when it is possible to accept the loss or damage incurred.

  Examples of detective controls include stock or asset checks (which detect whether stocks or assets have been removed without authorisation), reconciliation (which can detect unauthorised transactions), or any other monitoring activities which detect changes that should be responded to.

TAKING OPPORTUNITIES
This option is not an alternative to those above; 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

Risk Management Responsibilities

Risk management is a management responsibility. Consequently all managers are responsible, in consultation with his/her staff, for the development of a risk register in their area of responsibility.

The risk register when complete should be brought to the attention of all employees working in the service in a clear and understandable manner taking into account their level of training, knowledge and experience.

A critical part of the risk register is an action plan to address the additional controls identified as required to reduce the risk to an acceptable level. Additional controls (actions) identified as being required that cannot be managed at the service level at which they have been identified should be referred to the next level of management in order that decisions can be taken to manage them. Such decisions may involve the allocation of required resources, the provision of required authority or to escalate the action to a higher level of management.

At any stage in the process it may be decided to 'live with' or accept a certain level of risk as it is acknowledged that not every risk can be eliminated, for practical or other reasons.

A risk that cannot be completely eliminated must, nevertheless, be recorded in the relevant risk register along with a list of controls to be in place to reduce the risk to an acceptable level. These accepted risks will be monitored by the relevant service on a regular basis.

Risk Registers will capture risk information from the "bottom up" within each Service Area. The risk register will be a primary tool for risk tracking, and will contain the overall system of risks, and the status of any risk mitigation actions.

The action that needs to be taken is as follows:

- Strategic Directors need to embed risk management throughout their Directorate

- Directors to ensure that risk management has been explicitly considered in framing Business Plans

- Departmental Management Teams to review and up-date their risk registers on at least a Quarterly basis.

- Heads of Service to feed new key risks identified, such as from new projects arising or new partnership working to the Governance working group (in the absence of a Strategic Risk Group) to inform the corporate key risks summary at least quarterly.

- Strategic Directors to report to Chief Officer Group regarding progress on their management of corporate risks assigned to or identified by them or the people that report to them; in order to receive assurance and / feedback as appropriate

- Heads of Service to monitor the effectiveness of risk management actions in place and report on progress to their Service Director at least quarterly.

- Governance Group to review the corporate risk register and the effectiveness of actions put in place by COG to manage corporate risks on a half yearly basis.

- Directors to provide an annual assurance statement on risk management and internal control within their service area by 31st March each year by utilising information from their evaluation of the effectiveness of controls in place and the degree to which they have been consistently applied.

It will be necessary to obtain / retain evidence to demonstrate compliance with external inspection requirements

Monitoring & Reviewing Risks

The risk assessment process should be seen as a dynamic process with the adequacy of the control measures subject to continual review and monitoring and revised where necessary. In general terms, monitoring will be one of three types:

1. At service / department level

i. Identification of new risks

Within any service new risks are likely to emerge from time to time. These are likely whilst operating in an environment of limited resources, changing work environment e.g. regulatory, management, technological etc. The service must be aware of such issues which may impact on it and on a continuous basis be reflecting on sources of risk information

Any new risk identified should be included on the risk register following assessment and the identification of actions required in the same way as those that were identified through the initial risk register development process.

ii. Re-assessment of existing risks

It is good practice to review the risk assessment at least quarterly taking account of any new controls that have been put in place since the original assessment. This will allow for a re-prioritisation of the risk list thereby focusing the efforts of the service to address those risks that are most pertinent to the service.

When re-assessing existing risks, services should compare the risk rating from the re-assessment with the risk rating of the original assessment. If the reduction (or maintenance in certain circumstances) of risk levels is not as anticipated in the original assessment, then they need to check why i.e. have the additional controls been effectively implemented? If they have why are they not reducing the rating? Are they the right controls, and if not, is there a need to revisit and enhance the control measures?

2. At Directorate Level

In the same way as risks are monitored within services, risks should be monitored at a Directorate Level as outlined above:
a. Monitoring of actions arising from risks identified at Directorate Level
b. Monitoring risks:

i. Identification of new risks
ii. Re-assessment of existing risks

The risk register is a schedule used to collate all risk information. It is not a static document and will need to be reviewed and revised on a regular basis.

The frequency of these reviews is dependent on both the intended objective and the nature of the specific risks. Obviously the more significant the risk the more frequently it needs to be reviewed. The risk management section can assist in advising on the best approach for review in each instance.

Processes should be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed, and report significant changes which adjust risk priorities, and deliver assurance on the effectiveness of control.

The risk management section may also be used by management as an expert internal consultant to assist with the development of a strategic risk management process for the organisation. It will have a wide ranging view of the whole range of activities which the organisation undertakes.

3. At Strategic / Corporate level

There are some risks that are so significant that if they were to occur they would impact on the entire council and impede the council's ability to function. These risks will be identified by the Chief Officers Group and contained on the Strategic Risk register.

Because of the potential seriousness of these risks they are under a constant review, primarily by the Chief Officers Group but also the Governance Working Group and by both the Head of Assurance & Governance and the Insurance & Risk Manager.

Monitoring for Independent Assurance

From a governance perspective it is essential to demonstrate that services have conducted a proactive risk identification process, and also to demonstrate that the process was robust and has resulted in a positive effort to reduce risk.

The work of the Risk Management section provides an independent and objective assurance about the adequacy of risk management, control and governance.

The ongoing management of the risks identified by this process will be reviewed, making the risk registers a key tool for the monitoring of improvement actions identified as required for a service.

The Insurance & Risk Manager will review and report on the departmental and corporate risk management processes. Starting with the risk register published with the directorate business plans the review processes will:

- Comment on whether the risk management and governance processes in place are in line with policy.
- Require assurance that risk, and change in risk, is being monitored;
- Receive the various assurances which are available about risk management and consequently deliver an overall opinion about risk management;

That opinion will be expressed as a level of assurance detailed in the table below and will inform the subsequent actions required.

At Strategic / Corporate level

There are some risks that are so significant that if they were to occur they would impact on the entire council and impede the council’s ability to function. These risks will be identified by the Chief Officers Group and contained on the Strategic Risk register.

Because of the potential seriousness of these risks they are under a constant review, primarily by the Chief Officers Group but also the Governance Working Group and by both the Head of Assurance & Governance and the Insurance & Risk Manager.

Independent assurance will be given by the Chief Executive and the Head of Assurance & Governance

Levels of assurance

Level	Details	Assurance Sign Off	Action Required
Green	Taking account of the issues identified, COG can take reasonable assurance that the responses upon which the organisation relies to manage risks are suitably designed, consistently applied and effective.	Quarterly sign off of existing response effectiveness by management Independent assurance has been obtained for the next 12 months (or the duration of the current business planning cycle whichever is the shorter)	DMT to continue to ensure compliance with policy Insurance & Risk team may also suggest further action that could be taken to improve the effectiveness and efficiency of responses.
Amber	Taking account of the issues identified, whilst COG can take some assurance that the responses upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective, action needs to be taken to ensure compliance with council policy	Quarterly sign off of existing response effectiveness by management Independent assurance required within the next 6 months	Relevant DMT to work with Insurance & Risk team to address outstanding Actions / concerns
Red	Taking account of the issues identified, COG **cannot** take assurance that the responses upon which the organisation relies to manage risk are suitably designed, consistently applied or effective. Immediate action needs to be taken to ensure compliance with council policy	Management attention needs to be focused on implementing actions to improve existing responses or introduce new ones within the next 2 months	Insurance & Risk Manager will highlight concerns to GWC and COG respectively Relevant DMT to work with Insurance & Risk Team to address outstanding Actions / concerns

However, this is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff that has executive responsibility for the achievement of organisational objectives.

The Audit and Accounts Committee will be charged with approving risk management processes

This Committee will:

- Ensure that all aspects of the risk management process are reviewed at least once a year;
- Ensure that risks themselves are subjected to review with appropriate frequency (with appropriate provision for management's own review of risks and for independent review/audit);
- Make provision for alerting the appropriate level of management to new risks or to changes in already identified risks so that the change can be appropriately addressed.

However it should be noted that the Audit and Accounts Committee nor the Risk Management section should itself own or manage risks and is not a substitute for the proper role of management in managing their risks.

In addition, the overall risk management processwill be subjected to regular review by Internal Audit to deliver assurance that it remains appropriate and effective.

Review of risks and review of the risk management process are distinct from each other and neither is a substitute for the other.

Roles and Responsibilities

Risk management is a line management responsibility and consequently the line manager is responsible, in consultation with his/her staff, for the development of a risk register in their area of responsibility.

The risk register when complete should be brought to the attention of all employees working in the service in a clear and understandable manner taking into account their level of training, knowledge and experience.

In addition the roles and responsibilities of individuals and groups to implement the strategy are as follows:

- Audit and Accounts Committee - To review and approve the Council's risk management policy and strategy. To review the content of the strategic risk register, the adequacy of associated risk management arrangements.

- Members – involved via Regulatory Committees and the Scrutiny process. Also involved in other roles such as their membership of project boards/accountable bodies.

- Governance Group – To promote understanding of the management of risk in accordance with best practice, throughout the City Council.

  - Ensuring that the identification, analysis and prioritisation of corporate and cross cutting risks take place.

  - Monitoring / reviewing the corporate risk process, including the maintenance of risk registers and reporting to COG, Audit and Accounts Committee and Cabinet as appropriate. Ensuring that there are robust processes in place to implement risk management actions across the City Council. To assist with the ongoing development and review of the corporate risk management strategy and methodology. The Group will also work closely with the officers identified by COG to promote a risk aware culture and embed risk management throughout the Council.

- Chief Executive – leads on the wider corporate governance agenda of which risk management is a part. Receives assurance statements on internal control from Strategic Directors and signs off the Annual Governance Statement (AGS) along with the Leader of the Council, The Monitoring Officer and the Head of Audit & Accounts.

- Director of Governance – Overall responsibility for the risk management function.

- Head of Governance & Assurance– Lead officer for the Council on risk management. Maintains an effective corporate risk strategy and policy. Prepares reports to Audit & Accounts Committee seeking approval of the strategy and policy. Also reports on key risk management issues to the Audit and Accounts Committee and provide an opinion based upon the audit work carried out throughout the year.

- Insurance & Risk Manager – the Council's “Risk Champion” who advises on the corporate process. Develops, in conjunction with colleagues, practical approaches for implementing risk management. Will review and report on the departmental and corporate risk management processes. Will feed into the annual assurance statements. Will also issue guidance and information.

- Strategic Directors / Directors / Heads of Service – integral to the risk management process, providing leadership for the process to achieve the culture change. Need to be involved in corporate, major projects, cross cutting and external environment risk assessments as part of corporate planning. Assessing the wider implications of departmental risk assessments and feeding information to the Insurance & Risk Manager for consideration as corporate key risks. There is a particular duty for Strategic Directors to reduce the impact of high risks that are likely to occur. Make arrangements for embedding risk management throughout their Department, which will assist them in providing assurance to the Chief Executive. Reporting, on a regular basis, to Chief Officer Group regarding progress with corporate risks.

For the methodology to be effective there must be commitment throughout the City Council. The Council demonstrates its commitment by identifying, profiling and prioritising corporate and cross-cutting risks.

This involvement from the top will set the style and tone to cascade down the organisation. This top-down cascade will then meet the day to day operational control of risk by all involved in service delivery from the bottom-up.

LINKS TO CORPORATE PROCESSES

Risk management has clear linkages to other corporate processes. Given below are some examples of processes which are required to embed risk management into the culture of the Council.

Service Delivery Plans & Risk Registers

Service plans will contain a risk assessment/register, which identifies any risks linked to the delivery of the priorities contained in the plan. Strategic and departmental risk registers will be maintained identifying key strategic and operational risks, together with details of mitigating actions and risk owner.

The strategic risk register and departmental risk registers, will be reviewed regularly and reported to the Audit and Accounts Committee and departmental management teams, respectively.

Reports

Reports to Committees contain risk implications, to support strategic policy decisions. The Council's risk management methodology should be followed to produce these risk assessments and a summary of the findings given in reports to Members.

Projects and Change Management programmes

The Council has adopted PRINCE2 methodology for the successful conduct of all project based activities. Risk management issues are addressed at the commencement of the project planning process and continuously reviewed at all development stages.

By addressing project risks appropriately, the Council is able to take full advantage of the business opportunities that may arise from successful project management.

Partnership Working

Many of the services the council provides are done so in partnership with external organisations, hence service delivery through partnership working will be risk assessed at the outset and documented. Risk management considers risks relating to significant partnerships and to that effect the Council obtains assurance about the management of these risks.

The Council understands and manages the organisational risks regarding partnership activities as well as risks in the partnership itself.

Fraud and Corruption

The Council is committed to tackling Fraud and Corruption. Identification and addressing the risk of fraud and corruption are a key element within this risk management strategy.