DERBY CITY COUNCIL

AUDIT AND ACCOUNTS COMMITTEE
19 FEBRUARY 2007

ITEM 12

Report of the Head of Audit and Risk Management

RISK MANAGEMENT METHODOLOGY

RECOMMENDATION

1.1 To note the risk management methodology used to produce the Council's risk registers.

SUPPORTING INFORMATION

2.1 This Committee's role is to review and approve the Council's risk management policy and strategy and to review the content of the strategic risk register, the adequacy of associated risk management arrangements and the arrangements for departmental risk registers.

2.2 One key element of the risk management framework is the methodology that is used for identifying, assessing and managing risks. The guidance notes provided as part of the annual business planning cycle contained the Council's current risk management methodology. The methodology, attached at Appendix 2, provides Members with information on how the risk registers will be compiled.

For more information contact:	Richard Boneham, Head of Audit and Risk Management, 01332 255688 richard.boneham@derby.gov.uk
Background papers:	
List of appendices:	Appendix 1 – Implications Appendix 2 – Risk management methodology

IMPLICATIONS

Financial

1. None directly arising.

Legal

2. None directly arising.

Personnel

3. None directly arising.

Equalities impact

4. None directly arising.

Corporate objectives and priorities for change

5. The functions of the Committee have been established to support delivery of corporate objectives by enhancing scrutiny of various aspects of the Council's controls and governance arrangements.

APPENDIX 2

Derby City Council
Risk Management Methodology

November 2006

Introduction

Risk Management is about better decision making, it is about making an informed decision on an issue by understanding all of the associated risks. When risks are identified, analysed and prioritised it is possible to create management action plans that identify the current controls and show where controls are lacking. The aim is to eventually reduce the risk to acceptable manageable level

The Council's Risk Management Strategy sets out the approach that the Council is taking to embed risk within the organization. This document outlines the risk methodology to be used within the Council's risk management framework. There are five elements to the risk cycle:

- Risk identification
- Risk analysis
- Risk prioritisation
- Management of Risks
- Monitoring of progress and mitigation.

It is essential to know what your risks are if you are going to manage them. For the Council many risks can be cross cutting for this reason the risks should be included on a central risk register as well as departments maintaining their own risk registers.

Basically a risk register records what the risk is, who is responsible for managing the risk, what the risk score is, what actions controls are in place or need to be put in place to manage the risk, and the review date. (See Appendix A)

The first step in creating a risk register is to include the identification of risk in the business planning cycle. The aim is for departments to actively identify, analyse and prioritise risk as part of the business planning process and then build into their business plans, management actions and controls to mitigate the risks. The risks identified will form a departmental risk register. Although the business planning process is an annual cycle it is expected that these risks will be reviewed at least half yearly and that any new risk will be identified and included on the departmental risk register as soon as possible.

Step 1 - Risk Identification

This involves identifying potential risks relating to the Council's objectives. These may arise because of the general environment in which we are operating or in relation to specific decisions being made or options being considered. All types of risk should be considered at this stage.

Risk identification should be carried out using service objectives (or the objectives of the project or partnership) considered against the following prompt list of types of risks. This stage must be repeated regularly to ensure that new risks arising are identified and brought into the risk profile as appropriate.

Types of Risk:

- *Competitive*
- *Customer/Citizen*
- *Economic*
- *Environmental*
- *Financial*
- *Legal*
- *Legislative/Regulatory*
- *Managerial/professional*
- *Physical*
- *Political*
- *Reputational*
- *Social*
- *Technological*
- *Partnership/Contractual*

Step 2 - Risk Analysis

This is the process of reviewing the risks identified so that similar risks can be grouped and classified according to the likelihood of them occurring and the impact they would have.

Significance/Impact of Risk

5 Very High	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 £1,000,000 Adverse national media attention – National televised news report Litigation almost certain and difficult to defend Breaches of Law punishable by imprisonment
4 High	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 over £100,000 Adverse national media attention – National newspaper report Litigation to be expected Breaches of law punishable by fine only
3 Medium	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 over £10,000 Adverse regional media attention – Televised or news paper report High potential for a complaint litigation possible Breaches of regulations/standards
2 Low	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 over £1,000 Adverse local media attention – Local news paper report Breaches of local procedures/standards Unlikely to cause complaint/litigation
1 Very Low	Loss of a service for up to one day Objectives of the individual are not met No injuries Financial loss between £0 – 999 No media attention No breaches in Council working practices No complaints/litigation

Probability/Likelihood of Risk

5 Very High	Likely to occur at least once a year
4 High	Likely to occur once in every three years
3 Medium	Likely to occur once in every ten years
2 Low	Likely to occur once in every ten to twenty years
1 Very Low	Likely to occur once in every twenty years or more

The descriptions are applied as follows:

- Firstly the likelihood and impact of the risks identified need to be considered as if no controls exist – this will give you the inherent risk.
- Secondly the likelihood and impact of the risks will then need to be considered after the existing controls have been identified and evaluated as to their effectiveness – this will give you the residual risk. Internal Audit can help in the identification and effectiveness of controls.

- Then there will need to be consideration of what the target risk is. This is level of risk that is acceptable/tolerable, and the level at which you intend to manage that risk down to either immediately or over time.

Step 3 - Risk Prioritisation
Once the residual risks have been classified they need to be mapped onto a matrix as shown below.

IMPACT

LIKELIHOOD

	1	*2*	*3*	*4*	*5*
5					
4					
3					
2					
1					

The colours are a “traffic light” system that will show how controls in place have influenced where residual risks will be mapped e.g. the inherent risk could place a risk within the red zone, but because controls are in place, are evaluated as being effective and consistently applied the residual risk could fall within the amber or green zone.

The risk appetite is the level of risk the authority is prepared to swallow. On the above matrix anything appearing in the red zone exceeds the authority’s appetite and anything appearing within the green area is acceptable.

Red Zone	Controls and/or mitigating actions need to be put in place to reduce the risk to an acceptable level. Effort should be focussed on reducing the risk of any items appearing in this zone and hence moving these to the orange or green zone.
Amber Zone	The risks in this zone will require ongoing monitoring to ensure they do not move into the red zone. Depending on the workload involved in addressing the red risks it may be appropriate to develop controls/mitigating actions in order to control these risks.

Green Zone	The existing controls and/or mitigating actions are sufficient and may be excessive. Any more resources committed to reducing these risks still further are likely to be wasted. Consideration should be given to whether it is appropriate to relax the level of control present in this area.

Step 4 - Management of Risks

This process involves the following:

- Setting the risk appetite, this requires a decision to be made on the degree to which risks are tolerable (advice on this can be sought from the Head of Audit and Risk Management). This can vary from risk aversion (avoiding risk) to risk taking, and will depend upon the nature of the business. The result of this is to set the level at which risks can be tolerated and therefore accepted,
- Assessing whether to accept, control, modify or transfer the risk, or how to respond to the opportunity, based on the availability of resources,
- Documenting the reasons for the decision taken,
- Implementing the decisions,
- Assigning ownership to manage the risks to specific officers, and,
- The completion of an action plan – this is required for all risks identified as inherently high risks, detailing existing controls, as assessment of their effectiveness and recording where the evidence that the controls are operating can be found. The action plan also has a space to record what further controls along with who is responsible for these.

Controls are the tools that managers use to manage their services. They are the methods used by managers to assure themselves that they are achieving the council aims and service objectives, and that the service is being provided in the most efficient and effective way. The cost and robustness of existing or additional controls is a key consideration at this point and needs to be balanced against the potential consequences (reputational, financial etc) if the event occurred. The cost of implementing and operating a control should not normally exceed the maximum potential benefit.

Accepting risk means that you intend to manage the risk within your existing management routines. Risks should only be accepted where officers believe that the residual risk is tolerable to the service area, i.e. where they fall within the green zone of the matrix.

Controlling risks means that you identify additional action(s) to be taken that will reduce the likelihood and/or impact if the event occurred. Controls can be:

- *Preventative* - such as physically restricting access to hazardous chemicals, insisting on two signatories, ensuring segregation of duties within a system, implementing authorisation limits, or restricting levels of access on IT systems. These controls help to stop the risk occurring in the first place.

- *Detective* – such as quality checks, alarms, exception reports, accident reports, financial reports such as budget monitoring reports, and reviewing insurance claims. These will show when something has gone wrong – perhaps a trigger event that can alert you that the risk event is more likely to occur.
- *Directive* – such as procedure manuals, guidance notes, instructions, training. These advise on how to carry out processes safely but if they are not adhered to they will not prevent risk events occurring.

Modifying risks means that you change the activity or the way in which it is carried out because adding controlling mechanisms would not help to reduce likelihood and/or impact.

Transferring risks means using an insurer or other third party to cover the costs of losses should a risk materialise. However, care needs to be taken to accurately specify the risks to be covered. Making arrangements with others such as joint working, partnerships or contracting out to provide services could also be used to transfer risks e.g. transfer of the housing stock. However, other risks can arise from these arrangements and the responsibility of providing the service may still rest with the Authority. When transferring risks to other parties, ensure that risks registers detail where liability and accountability lie between the parties.

Eliminating risks – means ceasing to carry out the activity because modifying it or controlling it would not reduce the risk to an acceptable level.

Step 5 - Monitoring progress and reviewing the risks

The risk management process is ongoing and cannot be viewed as a one off exercise. Monitoring progress and reviewing the risks is a key stage of the risk management process. It is necessary to monitor the action plans developed at Step 5 and to regularly report on the progress being made in managing risks so that the achievement of the Authority's aims and the service objectives is maximised and losses minimised.

Reviewing risks to ensure that they remain up-to-date and relevant must also be done because;

- Previously identified risks may change over time; some may become less of a hazard, for example once all the affected staff have been trained. Others may become more likely if a key milestone is approaching such as the end of a funding stream.
- New risks identified will need to be added.
- Monitoring progress and reviewing risks should take place on at least a half yearly basis and more frequently if there are many changes or a project is progressing rapidly.

- Risks can also be reviewed in a number of other ways, for example, scheduling in a periodic agenda item at the unit meeting or undertaking a facilitated workshop.

APPENDIX A

RISK REGISTER

Owned by **Date:**

Risk No	Risk Description	Inherent Risk
1	Brief description of the risk e.g. Failure of a key supplier of a contracted out service	Initial analysis of impact and likelihood of risk without controls in place e.g. Impact :High Likelihood : High

Action/controls already in place	Adequacy of action/control to address risk	Residual Risk	Required management action/control	Target Risk	Responsibility for action	Review frequency	Key dates
Details of control(s) in place or any mitigating actions e.g. Continual contract monitoring in place	Evaluation of the control or action e.g. Satisfactory.	Analysis of impact and likelihood of risk with controls in place e.g. Impact :High Likelihood : Medium	Details of (further) controls or actions required to mitigate the risk	Details of level of risk that is acceptable or tolerable	Name of responsible officer	Details of how frequently the risk needs to be reviewed	e.g. Date of next scheduled review