AGENDA ITEM: 8 Page nos. 43 - 67

Meeting	Audit Committee
Date	24 March 2011
Subject	**Corporate Risk Management Policy Statement and Strategy**
Report of	Assistant Director of Finance – Audit and Risk Management
Summary	This report seeks to inform the Audit Committee of the revised Risk Management Policy Statement and Strategy

Officer Contributors	Maryellen Salter, Assistant Director of Finance – Audit and Risk Management
Status (public or exempt)	Public
Wards affected	None
Enclosures	Appendix A: Risk Management Policy Statement and Strategy
For decision by	Audit Committee
Function of	Council
Reason for urgency / exemption from call-in (if appropriate)	Not applicable

Contact for further information: Maryellen Salter, Assistant Director of Finance – Audit and Risk Management

1. RECOMMENDATIONS

1.1 That the revised Risk Management Policy Statement and Strategy be accepted as the policy and procedure by which the Authority will monitor and manage risk.

2. RELEVANT PREVIOUS DECISIONS

2.1 At the meeting of this committee on 18th June 2008, the risk management policy statement and strategy was approved as the policy and procedure by which the Authority will continue to manage and monitor risks.

3. CORPORATE PRIORITIES AND POLICY CONSIDERATIONS

3.1 The presence of strong risk management policies and procedures is paramount to the authority achieving all of its corporate priorities and as such impacts on all the corporate objectives.

3.2 The requirement of a Risk Management Strategy and strong risk management processes and procedures underpins our Use of Resources self assessment.

4. RISK MANAGEMENT ISSUES

4.1 Without consistent guidelines surrounding the application of risk management appropriate mitigation strategies to minimise risk may not be used exposing the Council to loss, damage or injury.

4.2 Without a risk management strategy decisions could be made without due consideration to the risks involved.

5. EQUALITIES AND DIVERSITY ISSUES

5.1 The council's revised Risk Management Strategy will support the council's approach to managing equalities and further demonstrate that a consistent approach is used to embed equalities and diversity in service delivery, where that risk has been identified within a service.

6. USE OF RESOURCES IMPLICATIONS (Finance, Procurement, Performance & Value for Money, Staffing, IT, Property, Sustainability)

6.1 When used appropriately risk management strategies can ensure that resources are used effectively within the organisation and effective decision making can take place. In addition, coupled with a rigorous assurance process to test the controls identified within the individual risk registers it can foster a positive control environment that can assist the Council to self-regulate. Given the move away nationally from external inspection this is particularly important.

7. LEGAL ISSUES

7.1 None in the context of this report.

8. CONSTITUTIONAL POWERS

8.1 Constitution part 3 responsibility for functions, section 2 responsibility for Council functions, details the terms of reference for the Audit Committee to provide independent assurance of the adequacy of the risk management framework.

9 BACKGROUND INFORMATION

9.1 Recently the corporate risk management team received feedback via three sources: external audit, internal audit and from participating in CIPFA benchmarking. There were a number of recommendations that suggested that risk management policy statement and strategy required revision. As such an exercise was undertaken to review the risk management policy statement and strategy against best practice.

9.2 Whilst the emphasis hasn't changed there have been a series of improvements that should re-focus officers and management on what the purpose of a risk management system is for. In addition, in the past the objectives for the strategy have not been linked to what action will take place to achieve this, this should give the Audit Committee additional assurance that a process of embedding risk management is starting to take place.

9.3 Another inclusion has been guidance around what officers and management intend to respond to risks, regarded as the four T's: tolerate, treat, transfer and terminate. Also, the addition of a target assessment of risk will assist those external to the service or Council to understand where officers and management are aiming to mitigate risks down to. This will allow us to consider how effective their current controls are.

9.4 Roles and responsibilities have largely not been revised, however part of the work of the corporate risk management team will be to ensure that these are better understood across the Council.

9.5 Previously the strategy and policy document had not included reference to programmes, projects and partnerships. Clearly this is an area that the Audit Committee needs to be assured that risk management arrangements are applied consistently. Hence support to the One Barnet programme office is being provided.

9.6 Developments have been made in terms of determining how risks will be defined and how they will be assessed. There has been more clarity on how to assess the probability and impact of risks and also to revise the grading of these risks from 1 (low) to 3 (high) to 1(low) to 5 (high) – this was seen as a better way of judging the importance of risks. Currently there are a number of

risks that are rated as high probability (3) and high impact (3) but the consequences of these could vary risk to risk, from merely something to slightly worry about to something of major significance. Again, this makes it difficult for those without the knowledge of the service to make a judgement on how well those risks are being managed.

9.7 Emphasis has also been made to develop a learning culture that will be championed within the Risk and Fraud Forum. This will mean that when something does go wrong there is transparency on the reasons why and what can be learned so that the same mistakes can be avoided in other services.

9.8 The Strategy and guidelines are available to all officers and management through the intranet, in addition the risk management system is a 'live' system called JCAD that can be updated at any time and can be viewed by all.

9.9 Prior to being received by the Audit Committee it has been separately endorsed by the Risk and Fraud Forum (January 2011) and Council Directors Group (February 2011).

9.10 Based on the acceptance by the Audit Committee of the revised Risk Management Strategy a programme of activity focussed on further embedding risk management across the Authority will ensure compliance. This will be supported by the Annual Audit Plan which is focused on giving assurances to the Audit Committee on those areas identified as high risk across the authority.

10 LIST OF BACKGROUND PAPERS

None.

Legal: MAM

Finance: MC/JH

Appendix

Corporate Risk Management

LB Barnet – Risk Management Policy Statement and Strategy

Document Prepared for:	**Corporate Directors Group/Cabinet/Audit Committee**

Author: **Maryellen Salter – Assistant Director of Finance, Audit & Risk Management**

Document Control

Document Description	To define the approach to managing risks across the Council		
Reference	LB Barnet – Risk Management Policy & Strategy		
Version	V8		
Date Created	30th October 2010		
Status	Final Version		
Filename	Held on "T" drive as; t\RD-Corporate Risk\ Strategy & Guidelines		
Authorisation	Name	Signature	Date
Prepared By:			
Checked By			
Distribution To	**Name**		**Date Distributed**

Version Control

Version number	Date	Author	Reason for New Version
Version 1	28/01/07	Mark Burgess	1st Draft document
Version 2	19/02/07	Mark Burgess	Includes feedback from CM
Version 3	25/02/07	Mark Burgess	Further updates
Version 4	01/03/07	Mark Burgess	Final version
Version 5	10/08/07	Mark Burgess	Updated to include fraud management
Version 6	16/05/08	Paul Lawrence/ Nikki Adams	Annual Revision and Update
Version 7	11/05/09	Paul Lawrence /Nikki Adams	Annual Revision and Update
Version 8	30/10/10	Maryellen Salter	Update in line with various external reviews, public sector best practice and the ISO 31000.

Table of Contents

1 Introduction

Risk is defined as anything that may have an impact on the Council's ability to achieve its objectives. Risk management refers to the culture, processes and structures inherent within the Council that are directed towards the effective management of potential opportunities and threats.

The Council's Risk Management policy is to proactively identify, understand and manage both positive and negative risks inherent in the delivery of our services and associated with our plans and strategies, so as to encourage responsible, informed risk taking.

The Council supports managers to being risk aware when making management decisions, not risk averse.

Risk Management is a fundamental part of best management practice for Directors, Assistant Directors, Heads of Service and other managers when planning, setting objectives, assessing adequate controls (both financial and service delivery) and monitoring performance.

Risk Management is a key way in which the Council manages its business. It is essential that risk management is embedded into corporate processes including:

- Strategic planning
- Financial planning
- Service delivery
- Policy making and review
- Project management
- Performance management
- Change management/transformation
- Business continuity planning

2 Risk Management Framework

2.1 Aims and Objectives

Our overarching aim is to improve the Council's ability to deliver its strategic priorities by managing threats and opportunities, and creating an environment that adds value to ongoing operational activities. This strategy supports the overall vision for Barnet's residents:

"Delivering high quality public services in the public sector is only possible through a partnership between Barnet's citizens and the wider public sector. We want to sustain Barnet's strengths as a suburb contributing to London's resilience in this time of uncertainty, and to London's prosperity when better economic conditions return. Access to public services must be easy and our citizens should have a favourable experience of public services."

The risk management strategy, once embedded, will contribute to the three corporate priorities:

- Better services with less money;
- Sharing opportunities and sharing responsibilities
- A successful London suburb

Corporate Risk Management Team objectives are:

No.	Objective	To achieve this the Risk Management Team will:
1.	Risk Management is aligned with corporate and directorate business planning and service delivery.	The Corporate Risk Management Team (CRMT) will undertake health checks of the risk management processes, through internal audit reviews, to ensure there is a golden thread from corporate priorities to recognition of risks to delivery of those priorities. Risks will continue to be included within the quarterly performance reports and challenged through the Risk and Fraud forum.
2.	To achieve better outcomes for the Council by being able to anticipate and respond to changing social, economic, environmental and legislative conditions to manage risk and maximise opportunities.	Inclusion of cross cutting and emerging issues within the Risk and Fraud Forum agenda. Ensuring that risks are appropriately reviewed by the Audit Committee and scrutinised on a quarterly basis through the inclusion of risks within the Assistant Director of Finance – Audit and Risk Management quarterly Internal Audit and Risk Management progress report.
3.	Provide assurances to stakeholders that risk management is being used to improve decision making. Ensure stakeholders receive adequate assurances over the controls identified by management and officers to mitigate risks.	Quarterly updates to the Statutory Officer Group updating on the risk maturity of the organisation. Quarterly reports to the Audit Committee providing oversight of corporate risks and the level of mitigating action taken by officers. Inclusion of risk management issues on any committee papers. Ensuring the internal audit plan is based on the risks of the Council and key controls are reviewed.
4.	Ensure that risks are regularly monitored and reviewed to ensure the risk treatment by officers and management is effective.	Quarterly Risk Management and Fraud forums that challenge risks registers from directorates. These will then feed into quarterly performance reporting which is challenged by the Corporate Directors Group and Cabinet Resources Committee.

No.	Objective	To achieve this the Risk Management Team will:
5.	Ensure there is effective communication and consultation in the risk identification, analysis and evaluation stages of day to day risk management.	Outline an appropriate risk management framework, including roles and responsibilities of management and officers in the key stages of risk management. The CRMT will provide training and support as and when requested. Develop JCAD (risk management system) to ensure it is aligned with the risk management strategy and allows for better reporting and analysis.
6.	To develop a risk aware culture.	Develop a common language of risk through the revision of the policy statement and strategy, establish clear roles and responsibilities at all levels within the organisation. Use risk champions within each directorate to disseminate information. Consult with members regarding their risk management needs. Standard item on the Risk Management and Fraud Forum will be to learn from instances where risk has not been effectively mitigated.
7.	Ensure resources are appropriate to carry out effective risk management.	Determine the training needs of directorates on an annual basis through risk management champions at the Risk and Fraud Forum. Resources will be flexible and use will be made of the internal audit partner.
8.	Ensure that the risk management framework continues to be fit for purpose and remains relevant.	Participation in regular benchmarking of the service, external and internal audit reviews, and revision of the risk management policy statement and strategy on an annual basis.
9.	To implement an effective risk management framework that forms a key part of effective corporate governance, including annual reporting through the Annual Governance Statement.	Revise the Risk Management Policy and Strategy Statement and ensure it is cascaded to performance leads and senior management teams through the Risk and Fraud Forum.

No.	Objective	To achieve this the Risk Management Team will:
10.	Raise awareness of the need for risk management by all those connected with the delivery of services (including partners, providers and suppliers) and in particular surrounding the transformation programme.	Revision of the Risk Management Policy and Strategy Statement for programmes, projects and partners. Ongoing work with the programme office to embed risk management, including separate challenge sessions.

2.2 Intent

Officers within the Council are committed to leading the organisation forward to continue to deliver quality services and to meet governance standards.

There is a need to create an assurance framework for the development of the Council's risk management systems and processes through the creation of an active learning culture in which people can learn from, and respond positively to, incidents and identified weaknesses. The Council has a risk management and fraud forum to ensure that this culture is embedded.

Our intention is to identify risks and proactively assess whether to treat, tolerate, transfer or terminate. The aim is to reduce the risk to the Council, where practicable, and to manage residual risk in such a way to support the achievement of the Council's objectives. This risk control/mitigation (risk appetite) is undertaken at four levels:

Tolerate
The exposure of risk may be tolerable without any further action being taken. In risks that are not tolerable, ability to do anything about them may be limited, or the cost of action may be disproportionate to the potential benefit gained.

Treat
Most risks will be treated by action taken to control the risk to an acceptable level.

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

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

2.3 Roles and Responsibilities

At the highest level within the Council, the **Cabinet** will review and approve this Risk Management Policy Statement and Strategy. The **Lead Member** for Risk management sits on Cabinet. The **Audit Committee** will review and seek assurances that robust risk management practices are in place and are effective. They will achieve this partly from

work undertaken by Internal and External Auditors and by quarterly assurance reports from the Assistant Director of Audit and Risk Management.

The Council's **Corporate Director's Group (CDG)** is responsible for approving the risk management strategy at an officer level and for ensuring that this is reviewed and updated on a regular basis. CDG is also responsible for reviewing the corporate risks of the Council, and directorate risks against performance on a quarterly basis.

The Council has the responsibility to ensure that the strategy covers bodies working in partnership with the Council. Risk management arrangements are discussed with partners on a regular basis, and with any new partners. There are currently two overarching Partnership Boards – Local Strategic Partnership (LSP) and the One Barnet programme Board. However the structure of these Boards will change following the Council's involvement in the Community Budget pilot.

It is everyone's job to identify risks and report them to their manager/ director. **Managers at all levels** are responsible for the collation and management of risks within their area, using risk registers compiled on the Council's **risk management system (JCAD).**

The prime purpose of risk management is to aid management in the delivery of value for money services. The mechanics of risk management are not to simply identify risks but to identify and implement effective controls to mitigate those risks – commensurate and balanced to the rating of the risk with the associated costs of implementation and affect on the priorities of the Council. Concise risk management is built around clear **ownership of risks** and the identification of nominated officers to implement the mitigating actions, followed up by a monitoring process to ensure that those officers take the actions agreed.

Supporting the further embedding of the risk management strategy is the **Risk Management and Fraud Forum.** The Forum consists of the **Risk Champions** - representatives from each Directorate, Corporate Anti-Fraud Team (CAFT), Service Areas, major programmes and associated risk management disciplines such as Health & Safety, Information Governance and Business Continuity. The Champions typically work at a senior management level striving to further embed risk management in their own area. The role of this Forum is to challenge the process for identifying and escalating risk from the directorates and the various risk disciplines and the efficacy of steps being taken to manage it, analyse cross cutting risks, emerging "hot spots", common risks, and potential clashes of risk.

2.4 One Barnet, programme and project management

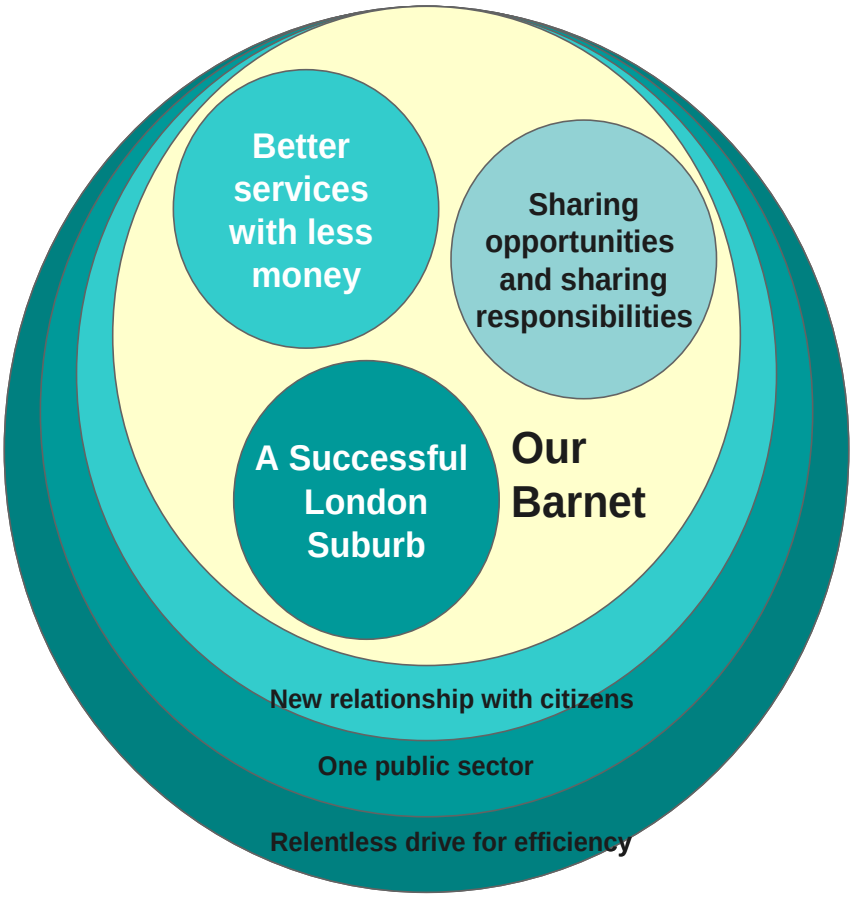

Diagram 1: Corporate Plan 2010-13

One Barnet represents a transformation programme for the Council, which because of the one off nature of the programme, will be high risk to the Council. This will be because:

1. the organisation has limited experience of undertaking the work before; and
2. the impact cannot always be predicted from the outset.

Programme level risks – are those risks which affect the intended benefits of a programme. There are two main types of programme level risks:

a) those risks which affect all or a number of projects within the programme; and
b) those risks which so substantially affect the benefits of a key project that they put the programme benefits at risk

Project level risks are those risks which affect the intended outputs or benefits of the project.

Project Managers are responsible for the development and maintenance of a **Project Risk Register** for each of the projects which they manage. The registers will normally sit alongside the associated issues log and be normally stored within the Hydra system. This is to facilitate the identification of actions which can be directly input to the appropriate project plan.
The registers will typically be compiled by holding workshops with the key stakeholders. The initial risk register will be signed off by the appropriate **Project Board** and then reported to them an exceptional basis via the normal project highlight reports. The highlight report would typically include:

- Progress on mitigating the highest scoring risks
- Any changes to the rating of the risks
- New risks identified.

The Project Board will then consider what risks if any, need to be escalated to the **Programme Risk Register**. The criteria for escalation would normally be:

- Highest scoring existing and new risks which need action to be taken by the **Programme Board**
- Lower rated risks which are likely to be common across a number of projects, which will require attention by the Programme Board
- The risks affect the overall objectives of the programme (subjective)

The **Programme Manager** is responsible for the development and maintenance of a Programme Risk Register. This register will be maintained on the corporate JCAD system for ease of joining up to the corporate reporting cycle.

The Programme Manager will chair a monthly meeting of Project Managers, acting as the **One Barnet Risk Group.** This group will:

- consider the risk highlight reports from the various Project Boards and agree what risks need to go forward to the programme risk register - key risks from the projects, common risks, new risks
- discuss updates on progress on actions in the programme risk register
- consider what risks, if any need to go forward from the programme to the **Corporate Risk Register**. Risks would need to be escalated to the corporate level, if they impact on activities outside of the scope of control of the programme
- produce a summary report on the above actions for the One Barnet **Operational Group** and **Programme Board.**.

The One Barnet Operational Group would then consider and agree the risk report from the One Barnet Risk Group and forward it to the to the outwardly facing Programme Board.

2.5 Risk management and fraud detection

It is the responsibility of every Director, Head of Service and Line Manager to ensure that their processes and procedures are protected against the possibility of any fraudulent or money laundering activities.

All Managers should complete a risk assessment of all their processes and procedures specifically looking to identify and enhance any process weakness that could allow fraudulent transactions and activities to exist, they should include reference to any previous CAFT investigations in their area's or any fraud risk identified with Internal Audit reports.

When establishing new processes and procedures or reviewing the effectiveness of existing processes and procedures managers should pay particular attention to the following areas;

Segregation of duties – where ever possible, no one person should be able to complete end to end processes which would allow fraud to go undetected.

Authorisation hierarchy – there should always be an authorisation process that required someone other than the originator to validate and authorise transactions thus ensuring that at least two people are involved in raising and authorising transactions.

Transparency – there should always be a record of the transactions processed throughout each link in the process chain allowing clear visibility of the requestor, processor and authoriser, recording date and time and action taken.

Audit trail – every process should have a recorded audit trail that is available for scrutiny. Each process should be audited regularly to ensure compliance with the requirements of the process. A full audit report should be completed detailing findings and recommended actions. The audit should be conducted by an independent party.

Any suspicion of or detection of fraudulent activities should be immediately reported to the Corporate Anti Fraud Team (CAFT) and where relevant also the Police so that a full and thorough investigation can be conducted.

In accordance with the Council's Whistleblowing policy staff may report wrongdoing to their managers. All managers must aware be of this policy, and act accordingly by passing all information reported to them to the councils Whistleblowing Officer for investigation.

All Managers and staff should be familiar with the Council's Counter Fraud Framework which include the Whistleblowing Policy and the Councils Anti Money Laundering Framework which includes information on Anti Money Laundering and Suspicious Activity. The Council has a designated Money Laundering Reporting Officer and all cases where suspicious activity is suspected should be referred to them as soon as possible.

2.6 Risk management policy

This document acts as a risk management policy which describes the Council’s objectives for, and the commitment to risk management.

3 Implementing Risk Management

3.1 Defining risks

There are a number of defined steps that managers need to undertake when considering risks and to ensure that a consistent approach is maintained. At the Council risks are usually categorised in four ways within the JCAD risk management system, and then further classified into their nature:

Risk	Nature
Strategic	Compliance
Operational	Finance
Project	Health and Safety
Business Continuity	Internal Control Checklist
	Political
	Reputational
	Staffing and Culture

These are further defined in Appendix B.

3.2 When to carry out risk assessments

Risk assessments should be carried out, at a minimum, on an annual basis at **team, directorate and corporate level**, as and when the objectives have been set for the following year, as part of the business planning cycle. Risk can also be identified through individual interviews and by workshops throughout the year. At the heart of the risk management cycle within the Council is the Risk Management and Fraud Forum which provides a sanity check on the key risks from across the various directorates as well as considering emerging and cross cutting risk.

Risk assessments should be carried out as early as possible in the life cycle of any new **project, programme or partnership**. The resultant risk register will then need to be signed off by the appropriate project/ programme/ partnership board. The key risks from the register will then need to be escalated to the appropriate team/ directorate risk register. The more complex programmes may have their own risk forum, where the key risks from across the various projects can be considered along with any emerging or common/ cross cutting risks which may need escalating to the programme risk register and the corporate risk register.

3.3 How to carry out a risk assessment

Risk assessments at any level should be carried out using the JCAD computer system which the Council uses to record, manage and report risk and associated controls and action plans. The detail of how to carry out a structured risk assessment is contained within the Risk Management User Guide.

The basic principles of the format and use of the register are summarised below:

- provide succinct and sufficient description of the risk, its cause and consequence
- link the risk to the relevant strategic/ directorate business objective

- use of best practice 5x5 probability – impact risk matrix (Appendix B)
- Include rating of risks at inherent (initial rating without any controls), residual (current rating with existing set of controls) and target stages (level of risk that the owner is prepared to accept and will drive what additional controls are required).
- setting the appetite for managing the specific risk – treat - tolerate – terminate – transfer
- measure the effectiveness of existing controls
- identify the additional controls required to fill any gaps with the set of existing controls and to achieve the required target risk rating
- show any progress on actions and change in the trend of the risk rating, compared to previous updates to the register
- identify reasons for closing risks and store closed risks in a separate area to maintain an audit trail
- identify assurance mechanisms where the design and effectiveness of the controls have been tested or challenged

Additional guidance is available at Appendix B.

4 Risk Reporting and monitoring

4.1 Day to day management and monitoring of risk

Risks are to be monitored according to the level of risk noted by the risk matrix (Appendix B); this will also dictate the level of management attention required. Directorates are responsible for ensuring all staff know how to report a risk for monitoring by Management. All risks should be discussed regularly at team meetings as a standing agenda item.

4.2 Escalation processes

Once a risk becomes unmanageable within team/directorate risk register it should be escalated into the Directorate/Corporate risk register. It is important however to put into context the instances where escalation would be appropriate. All staff should refer to the Risk Grading tool in Appendix B to assist in the grading process.

4.3 Serious risk incidents

In the unfortunate event of a serious risk incident occurring which results in the Council suffering loss: financial, reputational, or operational, a review of the events that led to that loss will be undertaken by the Corporate Risk Management Team. This will then feed into the Risk Forum to foster a culture of learning from these untoward incidents.

4.4 Performance management framework

Risk reporting will take place alongside financial and performance information on a quarterly basis, this will allow adequate analysis and linking of interdependencies to take place. The quarterly performance report will be reported to CDG, CRC and Overview and Scrutiny Committee (OSC).

4.5 Audit Committee

The Audit Committee's remit is to provide independent assurance of the adequacy of the risk management framework and the associated control environment. This includes monitoring the effective development and operation of risk management and corporate governance in the Council. As such the Audit Committee will receive quarterly reports on risk management within the Internal Audit and Risk Management progress report.

4.6 Assurances on the effectiveness of key controls

The Council wants to ensure that the controls which managers say are in place to manage the key risks, are both in place and working effectively. The annual programme of internal audit work includes resources to test the key controls specified within the risk registers, based on the level of risk involved. In addition, external audit base their plan on the key risks of the Council and this assurance should be noted within the risk registers where relevant.

4.7 Annual Governance Statement

The Council has to produce an Annual Governance Statement every year, which is an assessment of the systems the Council has in place to control and manage the services they provide. The risk management strategy and framework will provide assurance to CDG and members that risks are being properly managed.

5 Corporate Guidance & Support

Guidance notes will form an integral part of this policy and strategy document. Guidance notes will be available to everyone in the Council by publication on the intranet.

Support and advice from Corporate Risk will also be made available to support managers in this role, as and when required.

All risk champions are given training and development support to ensure that they have competence for managing risk. The Risk Management and Fraud Forum acts as a vehicle to cascade further guidance.

Appendix A: Key Deliverables for 2011-12

2010 – Position NOW	2010 -11 Deliverables	2011-12 Deliverables	2012 Deliverables
RM Strategy needs revising Some integration of RM related activity – directorate risks, corporate risks, Internal Audit, External Audit, Business Continuity, projects, programmes, partnerships, IT, Information Governance, H&S, ICC,AGS etc Reporting of risk at executive and member level in detail rather than exceptions Corporate Risk Register developed and signed off by CDG Risk Forum established Risk software tool (JCAD) implemented across authority Some inconsistency of embedding risk management arrangements Risks feature in quarterly performance reporting butu requires better linkages RM training carried out as required	Update RM Strategy and associated roles and responsibilities in line with ISO standard and current best practice Embed RM Reporting Cycle Develop approach to RM for projects, programmes and partnerships and provide support as required Role of Risk Champions and Risk Forum revised to provide more focused challenge on corporate risk register and embedding of RM Risks reported on an exception basis at CRC, Cabinet and Audit Committee Carry out internal audits of risk management in a sample of directorates to ensure consistency of application Enhanced use of JCAD rolled out across the authority Update and deliver risk training and awareness sessions through updating intranet site on RM Develop Managers RM Briefing pack	Continue to improve annual reports presented to Audit Committee on RM Quarterly compliance reviews on RM Review use of risk tools that establish risk maturity of directorates and Council RM fully embedded within each directorate and the corporate decision making process All risk registers linked to strategic objectives and priorities All projects, programmes and partnerships fully embed corporate RM strategy into their processes Development and use of Key Risk Indicators Ongoing integration of RM disciplines into a cohesive and joined up corporate governance framework	Risk appetite considered at planning stages of all new initiatives, projects, programmes and partnerships – and used to drive the associated decision making Risk management seen as an enabler by staff, management and members Risk appetite drives all risk and audit activity Corporate Risk Register informs Business Continuity Plan, audit strategies and plans Complete integration of RM disciplines into a cohesive and joined up corporate governance framework

Basic Risk Management – mainly reactive

Leading Best Practice in the Public Sector – fully proactive

Appendix B: Risk Grading tool

5.1 Defining risks

Risks fall into the following types:

Strategic – those risks affecting the medium to long term goals and objectives
Operational – those risks that managers and staff encounter on a daily basis
Project risk – are those risks which affect the intended outputs or benefits of the project
Business continuity – a risk that will have an impact on the ability to deliver services during an event of a significant disruption that threatens the ability of the organisation to deliver its services.

The nature of these categories is further expanded to the following:

Compliance – risk that will prevent compliance with legislation, policy, or strategic guidance
Finance – risk of unfavourable monetary impact covering medium term financial budgets and including income, expenditure, assets, liabilities, and reserve balances
Health and safety – a risk to the wellbeing of staff and contractors of the Council
Internal control checklist – an improvement or gap in the internal control environment of the service area identified in the annual internal control checklist process.
Political – a risk that will be out of line with the political direction of the Authority or conflict with policy
Reputational – a risk that will be visible to, or have a direct impact on, external parties which could damage the reputation of the Council
Staffing and culture – a risk that will have impact on motivation, staffing levels and or arrangements or that may be at odds with the culture of the organisation.

5.2 Risk Matrix

A risk is broken down into probability and impact. **Probability** represents the statistical chance of an event taking place. Such events are summarised into five broad stratified headings: Rare, unlikely, moderate, likely and almost certain. **Impact** represents the expected disruption to the Council. These are summarised as either negligible, minor, moderate, major, and catastrophic.

The above defines the gross or **inherent risk**, i.e. it takes no account of the controls the Council has in place or can put in place to manage the identified risk.

To offset this, Council officers apply controls to reduce the gross risk and obtain a net or **residual risk**. Officers should also describe what their **target risk** will be and the controls that are put in place should be with a view of mitigating the risk to be in line with the target. In addition, the means of prioritising them will be in relation to the four T's: terminate, transfer, treat or tolerate.

The Council has developed a risk matrix, based upon current best practice in the public sector. It is based upon a 5 by 5 matrix of impact and probability.

IMPACT	Score:		PROBABILITY				
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost certain
	5	Catastrophic	5	10	15	20	25
	4	Major	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Minor	2	4	6	8	10
	1	Negligible	1	2	3	4	5

The resultant scores from the matrix are assigned ratings as per the following table:

	1-3	Low risk	Acceptable risk. No further action or additional controls are required. Risk at this level should be monitored, and reassessed at appropriate intervals
	4-6	Moderate risk	A risk at this level may be acceptable. If not acceptable, existing controls should be monitored or adjusted. No further action or additional controls are required.
	8-12	High risk	Not normally acceptable. Efforts should be made to reduce the risk, provided this is not disproportionate. Determine the need for improved control measures
	15-25	Extreme risk	Unacceptable. Immediate action must be taken to manage the risk. A number of control measures may be required.

Probability score

The frequency based score is appropriate in most circumstances and is easier to identify.

Probability score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently

Impact

This scale should be used for guidance on descriptions of impact for assigning a risk impact score.

Impact score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Compliance	No or minimal impact or breach of guidance/statutory duty	Breach of statutory legislation Reduced performance rating from external/internal inspector	Single breach in statutory duty Challenging external or internal recommendations or improvement notice	Enforcement action Multiple breaches of statutory duty Improvement notices Low performance ratings	Multiple breaches in statutory duty Prosecution Complete system changes required Zero performance against key priorities and targets
Finance	Small loss risk of claim remote	Loss of 0.1-0.25 per cent of budget Claim less than £20k	Loss of 0.25-0.5 per cent of budget Claims between £20k - £150k.	Uncertain delivery of key objectives/loss of 0.5 – 1.0 percent of budget Claims between £150k to £1m	Non delivery of key objective/loss of >1 percent of budget Failure to meet specification/slippage Loss of major income contract
Health & Safety	Minor injury Cuts, bruises, etc. Unlikely to result in sick leave	Moderate injuries: Likely to result in 1-3 days sick leave	Major injuries: More than 3 days sick leave – notifiable to HSE	Death Single fatality	Multiple deaths More than one Fatality
Internal Control Checklist	Control is in place with strong evidence to support	Control in place with tentative evidence	Control in place with no evidence to support	Partial control in place with no evidence	No control in place

Impact score	1	2	3	4	5
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Political	Parties largely work positively together with occasional differences. Members and executive work co-operatively	Parties have minor differences of opinion on key policies Members and executive have minor issues	Members begin to be ineffective in their role Members and Executive at times do not work positively together	Members raise questions to officers over and above that amount tolerable Strained relationships between Executive and Members	Internal issues within parties which prevent working collaboratively Questions from members shift resources away from corporate priorities
Reputational	Rumors Potential for public concern	Local media coverage – short term reduction in public confidence Elements of public expectation not being met	Local media coverage – long term reduction in public confidence	National media coverage with key directorates performing well below reasonable public expectation	National media coverage, public confidence eroded. Member intervention/action
Staffing and Culture	Short-term low staffing level that temporarily reduces service quality (<1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/service due to the lack of staff Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level of competence Loss of key staff Very low staff morale No staff attending training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending training on an ongoing basis

Appendix C: Business Continuity

Business continuity plans allow officers to manage threats or incidents that have potential to disrupt the delivery of services or the conduct of Council business.

By focusing on the impact of disruptive events, BCM identifies the critical services and function the organisation depends on, and what is required for the organisation to meet its obligations to its stakeholders. This allows the Council to:

- Take steps to protect its people, premises, IT, supply chain, reputation etc
- Plan to respond effectively to disruptive events and challenges

Business Continuity Management is a cyclical process, and is designed to manage and control risks which can be described as 'low probability, high impact' events. It involves four stages:

1. understanding the organisation
2. determining the Business Continuity Strategy
3. Developing and implementing the BCM plans
4. Exercising maintaining and reviewing

It requires both leadership and ownership from senior management, and understanding and support throughout the organisation. For this reason, Business Continuity Management is a mainstream activity, which is required of all directorates/service.

The aim of BCM is to ensure the Council is resilient to interruptions in the delivery of its business critical services and to return to 'business as usual' as quickly and efficiently as possible.

The Corporate Business Continuity Toolkit requires that all services report monitoring (alongside Risk Management) to include confirmation all critical services have been identified, regularly reviewed, BC plans in place, updated and tested within the last 6 months.

Reference should be made to the Business Continuity Strategy.