Appendix

Corporate Risk Management

LB Barnet – Risk Management Policy Statement and Strategy

Document Prepared for:	**Corporate Directors Group/Cabinet Resources Committee/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	V3		
Date Created	21 March 2012		
Status	Draft Version		
Filename	Held on "T" drive as; t\RD-Corporate Risk\ Strategy & Guidelines		
Authorisation	Name	Signature	Date
Prepared By:	Maryellen Salter		28/3/12
Checked By			
Distribution To	**Name**		**Date Distributed**

Version Control

Version number	Date	Author	Reason for New Version
Version 1	21/03/12	Maryellen Salter/Matthew Chandler	1st Draft document - revised to set out how risk will be managed with external delivery partners, and to reflect feedback obtained
Version 2	28/03/12	Maryellen Salter	Updated after CDG comments
Version 3	2/04/12	Maryellen Salter	Minor update after consultation with Lead Member

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

Risk Management Team objectives are:

No.	Objective	Workstreams:
1.	Risk Management is aligned with corporate and directorate business planning and service delivery.	• The Risk Management Team (RMT) 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. • Quarterly performance reports to include risks that have been 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 quarterly Internal Audit and Risk Management progress report.

No.	Objective	Workstreams:
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, including those risks managed by third parties.	• Quarterly Risk Management and Fraud forums that challenge risks registers from directorates.
5.	Ensure there is effective communication and consultation in the risk identification, analysis and evaluation stages of day to day risk management, including any services delivered by partners.	• Outline an appropriate risk management framework, providing 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 • Use risk champions within each directorate to disseminate information. • Consult with members regarding their risk management needs. • Standard item on the Risk 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.
8.	Ensure that the risk management framework continues to be fit for purpose	• Participation in regular benchmarking of the service, external and internal audit reviews, and revision of the risk

No.	Objective	Workstreams:
	and remains relevant.	management policy statement and strategy on an annual basis. • Put in place a model for risk management when commissioning services from third parties.
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.
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. Risk management to be embedded within the process of commissioning services.	• Revision of the Risk Management Policy and Strategy Statement for programmes, projects and partners. • Ongoing work with programmes such as One Barnet to embed risk management, including separate challenge sessions.

2.2 Risk response

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 a mitigating action plan that is tailored to the identified risk and undertaken to control the risk to within 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. When commissioning services it is necessary to assess which risks are being transferred, which risks are retained and identify whether any new risks arise. Part B of this policy considers this in more depth

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

2.3 Roles and Responsibilities

This section sets out the key responsibilities for risk management within the Council.

2.3.1 Maintenance of the Risk Management Policy

- At the highest level within the Council, the **Cabinet** will approve any major changes to the Risk Management approach.
- The Council's **Corporate Director's Group (CDG)** is responsible for approving this risk management strategy at an officer level and for ensuring that this is reviewed and updated on a regular basis.

2.3.2 Identifying and recording risks

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.

2.3.3 Summary of responsibilities

Within the Council various groups and individuals have responsibilities regarding the risk management process. Some of these are defined by the Terms of Reference set out in the Council Constitution (identified in *italics*); the remainder are based on the established practise of the Council and are formalised by means of this policy.

The Council
Full Council is responsible for ensuring that the risk management strategy covers bodies working in partnership with the Council.

The Cabinet/Cabinet Resources Committee
The Cabinet has responsibility for reviewing and approving the Risk Management Strategy and Policy document annually.

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.

The Audit committee will proactively fulfil its duty by receiving quarterly reports on risk management within the Internal Audit and Risk Management progress reports. The Audit Committee will also review updates to the Risk Management Strategy and Policy.

Deputy leader of the Council – Resources and Performance
To lead on budget and policy formulation and implementation in relation to risk management
The Deputy Leader is the Lead Member on Risk Management for the Council. Periodic review meetings occur with key officers in order to maintain oversight of risk management within the Council.

Corporate Directors Group (CDG)
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. It is also responsible for reviewing the corporate risks of the Council, and overseeing the management of directorate risks against performance on a quarterly basis.

Statutory Officers Group (SOG)

The Statutory Officer Group receives reports from Internal Audit and Risk Management regarding the adequacy of the risk management arrangements on a quarterly basis. In addition, on a monthly basis it receives reports from Internal Audit on perceived risks resulting from internal audit reviews and the status of any action plans to mitigate any perceived risks.

Risk Management and Fraud Forum
Meets Quarterly to:

- Provide a sense check on risks across the Council, ensuring consistency of approach
- Consider risks that cut across teams or directorates
- Consider risk conflicts
- Review the escalation of risks with scores of 12 or more
- Respond to any serious incidents

Risk Champions
Attend the Risk Management and Fraud Forum. Take a lead role in embedding risk management processes and policies within their directorate. Champions take a super user role in terms of the JCAD risk management system.

Service Directors and Managers
Monitor Directorate level risks and ensure an appropriate response has been implemented. Review risks against performance on a quarterly basis for reporting to CDG and include on the monthly performance monitor. Have oversight of risk management within the directorate. Seek the involvement of their Lead Council Member in determining the risk appetite for the directorate in general and for specific risks with a score of 12 or more.

All staff
All staff should have active involvement in the process of identifying and evaluating risks within their team and projects annually. Staff are required to implement actions allocated to them on JCAD, and to exercise their responsibilities for executing control activities relevant to their role.

Risk Management and Internal Audit
Risk Management Team is responsible for updating the policy, providing training and support to teams dealing with risks. The risk management team will form part of the Risk Management and Fraud Forum to provide specialist insight. They will support CDG and Audit Committee monitor risks in the Council through using JCAD reports and any other information available, for example from Internal Audit reviews.

Internal Audit will deliver the annual audit plan reviewing controls within the Council using a risk-based approach. For each review a report will be issued giving a level of assurance and/or making any recommendations for improvement. Reports will be presented in summary format to Audit Committee with a focus on those reports issued with limited or no assurance. Internal Audit will review the adequacy of risk management arrangements on an annual basis. The Chief Internal Auditor will issue an annual opinion on internal controls for inclusion within the Annual Governance Statement (AGS).

2.4 One Barnet, programme and project management

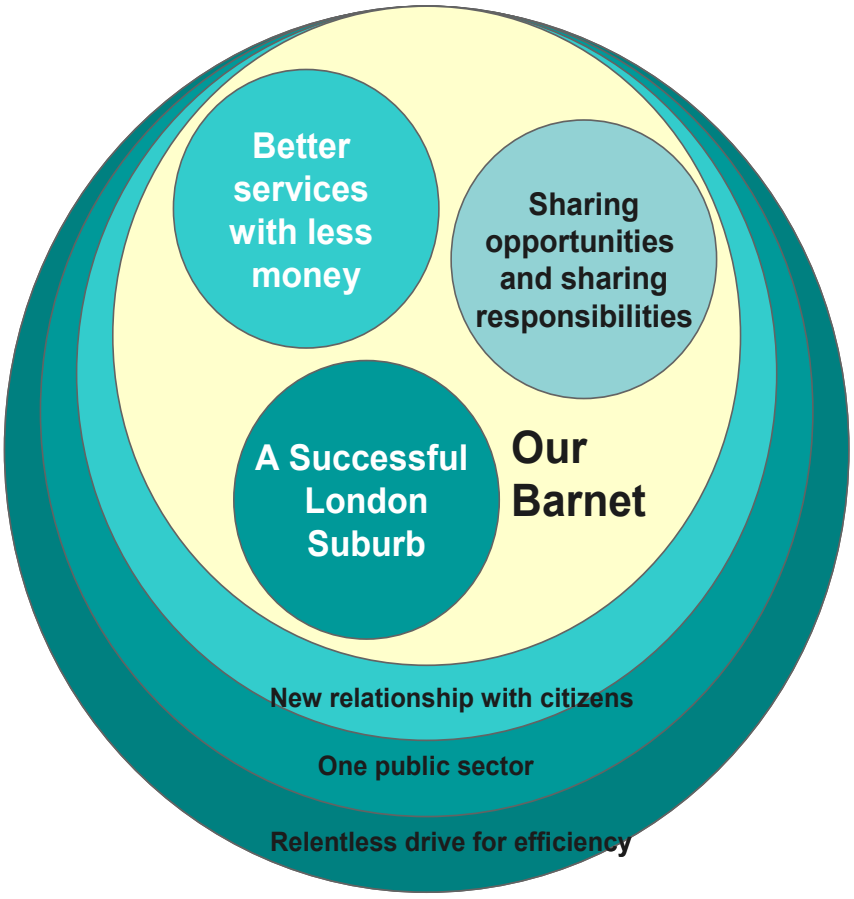

Diagram 1: Corporate Plan 2010-13

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 JCAD. 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 agreement as to the appropriate action to be taken to mitigate the risks
- Lower rated risks which are likely to be common across a number of projects, which will require attention by the Programme Board and are likely to be dependencies for other projects
- 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.

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, money laundering activities or bribes.

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 be aware 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, Anti-Bribery 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 A.

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 challenge around key risks identified 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 meetings, 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 performed on JCAD - the system 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 are summarised in Appendix A.

3.4 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 A); this will also dictate the level of management attention required. JCAD should be used for assigning risk owners and setting the frequency of review.

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.

3.5 Escalation processes

Where a risk is rated as having a score of 12 or above at a team level, this is considered to be a trigger point for further escalation process. The stages of escalation are defined in Appendix A.

3.6 Serious risk incidents

A serious risk incident is an incident that occurs which results in the Council suffering loss that is:

- financial
- reputational
- operational

Defining a 'serious incident'

The definition of a 'serious incident' shall be aligned to the risk scoring approach set out in Appendix A; incidents that occur and have an impact that meets the criteria for a risk score of 4 (Major) for impact are defined as serious. On this basis the following shall apply:

Category of incident	Trigger point for treatment as 'serious'
Financial	• A loss of >0.5% of budget • Claims of >£150k
Reputational	• National media coverage with key directorates performing well below reasonable public expectation; • Erosion of public confidence • Requirement for Member or external agency intervention • One or more fatalities • Prosecution
Operational	• Enforcement action due to compliance breach • Multiple breaches of statutory duty • Improvement notices from central government • Low performance ratings • Uncertain or non-delivery of key objective/service due to lack of staff • Unsafe staffing level of competence

Response to a serious incident

In the unfortunate event of a serious risk incident occurring a review of the events that led to that loss will be undertaken by the Risk Management Forum to foster a culture of learning from these untoward incidents.

Service Directors and Managers will be required to demonstrate to CDG and their lead Member what actions have been taken to improve the design or implementation of controls with regards to the risk recurring.

4 Reporting and Monitoring

4.1 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 could be subject to call-in from the Overview and Scrutiny Committee (OSC).

4.2 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.

4.3 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.

4.4 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 Risk Management when commissioning services

This section of the Policy applies to the specific situation that arises on outsourcing service provision to partner organisations. A summary checklist for managers covering the key aspects of this section has been included, see Appendix C.

5.1 Objectives

The 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.

Our strategy is to embed risk management in the decision making process and to align the responses to risk to corporate objectives.

The purpose of risk management in the context of commissioning services will be:

- To ensure proper identification and understanding of risks associated with commissioning a service
- To support clear allocation of responsibilities for managing and monitoring risk
- To align the response to identified risks with corporate priorities
- To provide a framework for information sharing regarding risks and performance management
- To reduce the burden to the Council of risk management procedures

5.2 Approach to risk management when commissioning services

The process of identifying risks when commissioning services has two elements

1. Considering those risks that are associated with the delivery of the service that is being transferred and communicating with the provider regarding these
2. Assessing what the new risks for the Council are as a result of commissioning services from a delivery unit

The process of risk identification, scoring, escalation and monitoring is set out in the Risk Management Policy Statement. All risk assessments should be carried out using JCAD and should apply the 5 X 5 matrix for impact and probability.

5.2.1 Identifying existing risks

Each service area should already have an up-to-date risk register on JCAD. As part of competitive dialogue it is expected that bidders will want to review the risks as perceived by the Council. It is possible that they may identify additional risks, or score existing risks differently based on their planned approach to delivering the service

It is expected that an integral part of the negotiations for contracts that there will be clear agreement on how the Council and the partner organisation will document, monitor and manage risks.

5.2.2 Identifying new risks

When considering the implications of commissioning a service from a delivery unit officers should first review the existing risk register for that service area and consider what may change as a result of the proposed commissioning move. Following this review, it is recommended that officers also consider if any different risks may arise from transferring service delivery.

Where the Council will be commissioning services in partnership with another organisation (e.g. an NHS body) it will be necessary to involve the partner in the risk identification process at an early stage. While different bodies have different risk assessment techniques and policies, the 5x5 matrix is a common approach that most organisations should be able to engage with.

5.2.3 Working with potential partners

Through the process of competitive dialogue the Council will have access to a new perspective on the risks associated with the service and the contract. Commissioners can take advantage of this to enhance their ability to manage risk. It should be noted that there may be challenges arising from these discussions, particularly if other parties use a different lexicon for risk management. Part of the dialogue process will be establishing a common ground between parties.

5.3 Understanding retained risks

One of the benefits of commissioning services will be the ability to transfer risks to delivery units however the Council may retain exposure to some risks.

It is recommended that the Council understands which risks may continue to have a potential impact upon it and ensure they are recognised and dealt with accordingly. The following points are to act as guidelines for making these decisions. However it is important to note that the exact terms of contracts and legal frameworks for commissioning services will affect the assessment of risks.

As a rule of thumb, it is suggested that any risk with a score of 10 or less on JCAD is unlikely to pose a risk to the Council if management of the associated activity has been fully transferred and the provider takes on the risk.

Of the high-extreme level risks (score of 12 or more) the following categories of risk may also be fully transferred with no residual impact on the Council:

- Health and Safety
- Internal control
- Staffing
- Some financial risks

However, risks with a High or Extreme impact that fall in the following areas are likely to still have adverse impact on the Council despite any contractual provision:

- Reputational
- Compliance
- Political
- Some financial risks

Risks that can still impact the Council are, to a greater or lesser extent, retained risks. These risks will normally be recognised and recorded within the Council. There are two ways in which this can occur:

1) The retained risks are logged individually on JCAD
2) Risks are grouped appropriately and recognised on JCAD as part of the 'new' risks associated with commissioning services

5.4 Risk appetite

Section 3.5 of this Policy identifies the importance of involving the relevant Council Members when determining the risk appetite for a given risk. This principle remains applicable when risks are being considered for commissioned services. The assessment of whether a risk with a score of 12 or more that is effectively retained by the Council should involve the lead Council Member for the service area. They should also be involved in setting the risk appetite for all such risks.

The Council's risk appetite should be set with reference to the strategy for service delivery in that area, and also considering the overall corporate plan. The process of aligning risk response with strategic priorities will help to determine which of the 'Four T's' (Treat, Tolerate, Transfer, Terminate) will be used on a given risk.

5.5 Risk allocation and responsibility

Having identified all of the risks officers will need to determine and clearly record who will take responsibility for each risk, having considered which party is best placed to deal with each risk. It is expected that the commissioning contract will be structured in order to provide an enforceable legal basis for the allocation of responsibility for identified risks. The contract should also make provision for how emerging risks will be identified and dealt with.

A risk that is considered to be retained by the Council should be reviewed to determine what the response will be within the 'Four T's' framework. Where possible the primary responsibility for executing the actions plan should lie with the provider, with appropriate monitoring arrangements in place to provide the Council with the necessary assurance. For retained risks the Council will usually employ the approach set out in this Strategy, however some variations may occur where risks are assessed as being 'joint risks'.

5.6 Dealing with joint risks

In general it is expected that dealing with any given risk will clearly allocated to either the Council or to the service provider. However a small number of risks may be assessed as being shared between parties. Such risks may be the 'retained risks' that the Council cannot fully transfer.

In these circumstances it is recommended that the Council and service provider develop a joint risk register and use this to define the actions each party will undertake in order to manage the risk to within the agreed parameters. The aim of the approach adopted will be to help develop partnership working, with all parties working together for agreed common goals.

5.7 Monitoring risks

Those risks that are retained by the Council but managed by the delivery unit will usually be monitored by the Council. Based on the guidelines above, these are likely to be risks that have a score of 12 or more. Activity regarding such risks, including any changes in conditions should be monitored quarterly.

It is recommended that commissioners consider how they will ensure that they have sufficient technical expertise available to understand and interrogate the risk and performance data that is collected from delivery units. Effective contract management by the Council will be contingent upon the ability of the Council to monitor the activity of delivery units, challenge subjective decisions and enforce the requirements of the contract.

Over the course of the service contract it is likely that the risk profile will evolve. For this reason commissioners are encouraged to make provision for ongoing reviews of risks with open dialogue taking place with providers.

5.8 Aligning risk and performance

The commissioning contract should align risk management with performance management. Partner organisations should have clear incentives to be delivering good risk management procedures. The structure of the contract and the legal framework in which the partnership operates should reflect the priorities of the Council and match the reward for partners with the achievement of corporate objectives and management of risks. Such incentives may take the form of performance related pay, a share of financial benefits or other opportunities specified in the delivery contract.

5.9 Contingency planning

Part of the risk management approach for the Council will be to have a robust business continuity plan that will deal with contingencies that may arise and prevent the provider from continuing in their role and delivering services, either in the short or long term. It should be considered what role the service provider can play in this, through the sharing of information, training exercises and joint business continuity plans.

5.10 Requirements for partner organisations

In order for the council to maintain its responsibilities for overseeing the management of the risks it will be necessary to agree a good quality system of information reporting. Commissioners should consider what form and frequency of information will be useful to them. Every service contract will be uniquely tailored; however it is desirable to have a consistent approach across the Council on key aspects of contract management. To support this, the following guidelines outline typical requirements for the service provider.

5.10.1 Risk management policies

The service contract should include a requirement that the provider of services maintains a minimum standard of risk management procedures, proportional to the size of their contract. While it will be the responsibility of providers to determine their risk attitude, there will need to be a requirement upon providers that they will collaborate with the Council to monitor and report on those risks that the Council has identified as having a score of 12 or more where the activity is ongoing.

5.10.2 Risk reporting

The contract management process should require regular (usually quarterly) reporting from delivery units on the following:

- Status and actions regarding any risks where the Council has a degree of retained risk

In addition it is recommended that there are appropriate channels for the service provider to report to the Council:

- Any new emerging risks that would score 12 or more
- Any serious risk incidents that occur

In order to support transparency and accountability, where commissioners believe it will be advantageous, providers should report annually:

- Full risk register for the services delivered, thus demonstrating the overall approach taken to assessing and dealing with risks and providing the Council with broader comfort on how risk management is treated
- Outline plan for risk management strategy in the forthcoming year

To maintain good practice on risk reporting throughout the life of the contract, it is suggested that the contract terms should specify a post-holder or group within the delivery unit that will take a lead on monitoring and reporting risks to the Council. It would be helpful for a defined committee or panel to have responsibility on the Council's part for receiving these reports. Such a group would usually work closely with performance management.

5.10.3 Information sharing

Within the contract arrangements the right of access to data associated with the service delivery for Barnet Council or its agents must be clearly established, including access for audit and assurance procedures. The scope of access and the typical inspection routines will be individually negotiated but should include appropriate opportunity for the Council to gain assurance that the provider is meeting the required performance standards and is dealing with business in a manner consistent with the Council's understanding. The Council should also consider the eventuality where there are signs of failure on the contract delivery, and whether any additional access may be required in such circumstances.

6 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: Risk assessments and escalation

6.1 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.

6.2 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.

I	Score:	PROBABILITY				
		1	2	3	4	5

M P A C T			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

6.3 Risk assessment process

The basic principles and steps involved in performing a risk assessment, the format of the assessment and use of the risk register are summarised below:

1. Provide succinct and sufficient description of the risk, its cause and consequence
2. Link the risk to the relevant strategic/ directorate business objective
3. Record the risk in JCAD using the best practice 5x5 probability–impact risk matrix (see above)

4. 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).
5. Determine the risk appetite for the identified risk and apply this in setting the approach for managing the specific risk (treat, tolerate, terminate, transfer)
6. Measure the effectiveness of existing controls
7. Identify the additional controls required to fill any gaps with the set of existing controls and to achieve the required target risk rating
8. Show any progress on actions and change in the trend of the risk rating, compared to previous updates to the register
9. Identify reasons for closing risks and store closed risks in a separate area to maintain an audit trail
10. Identify assurance mechanisms where the design and effectiveness of the controls have been tested or challenged

6.4 Risk escalation process

Risks are initially identified at a team level and responded to at this level. However when a risk has a score of 12 or above this is a trigger for considering escalation of the risk. The following stages shall apply:

1. The team should seek the involvement of their Directorate Risk Champion or other risk specialists to ensure the risk score is appropriate and consistent with this risk management strategy/policy.
2. Assuming the risk score remains as 12 or above, the risk is to be escalated by including it within the relevant Directorate risk register on JCAD.
3. All risks rated 12 and above are to be included within monthly monitors and agreed at each Senior Management Team (SMT) or equivalent for each Directorate
4. Officers should involve their lead Council Member in discussing the risk appetite and for sending monthly monitors with risks agreed at SMT.
5. Directorate level risks will be reported quarterly to the Risk Management and Fraud Forum and the reports published on-line.
6. The quarterly report for each directorate will show a summary Heat Map, identifying how many risks in each area of the probability-impact matrix. A JCAD report on all risks with an initial score of 12 or more will also be presented for each directorate. This report includes a description of the risk, the initial score, control activities, the status of the risk response, key dates, a current and a target risk score.
7. Where a Directorate level risk rated 12 or above is considered to have the potential to impede the achievement of corporate objectives, following consultation with the Assistant Directors Group, it is to be included within the Corporate Risk Register for agreement by the Corporate Directors' Group (CDG).
8. Corporate risks will be reported to CDG and Cabinet Resources Committee quarterly, more regularly if the need arises.

Appendix B: 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.

Appendix C: Checklist for risk management when commissioning services

The following checklist for use by officers when commissioning services is intended to highlight key considerations for risk management. The checklist should be used within the context of the overall Risk Management Policy, in particular commissioning services (Section 6).

1) Ensure the existing risk register on JCAD for this service is up to date
2) Engage with any commissioning partners to build a complete risk register
3) Review the JCAD risks to identify where the Council (or commissioning partnership) is likely to have to retain some element of the risk impact
4) Use competitive dialogue with bidders to
    a) Explain the risks you expect to transfer to them
    b) Obtain their views on the risks associated with the service
5) Determine the risk appetite and preferred strategy for dealing with identified risks, involving relevant Council Members for those risks with a score of 12 or more
6) Agree and formally document in the service contract who will be responsible for managing the defined list of known risks
7) Set in place monitoring protocols and put in place plans to make sure the Council has sufficient capacity to exercise its duties in monitoring
8) Make a contingency plan for service continuity