Putting the Community First

APPENDIX

LB Barnet Risk Management

Risk Management Framework: Policy Statement and Procedures

Document Prepared for:	Strategic Commissioning Board/Cabinet Member for Resources and Performance /Audit Committee

Author: Courtney Davis – Risk Assurance Manager

DOCUMENT CONTROL

Document Description	To define the approach to managing risks across the Council		
Reference	LB Barnet – Risk Management Framework		
Version	V1.7		
Date Created	April 2014		
Status	Draft		
Filename	Held on “S” drive LB Barnet – Risk Management Frameworkv1.7		
Authorisation	Name	Signature	Date
Prepared By:	Courtney Davis		2 April 2014
Checked By	Maryellen Salter		2 April 2014
Distribution To	**Name** : Cabinet Member of Resources and Performance Strategic Commissioning Board		**Date(s) Distributed:** 7 April 2014 15 April 2014

Version History

Version number	Date	Author	Reason for New Version
Version 0.1	30.5.13	Courtney Davis	1st Draft document
Version 0.2	18.06.13	Maryellen Salter	Review document
Version 0.3	19.06.13	Courtney Davis	Amendments
Version 0.4	20.06.13	Courtney Davis	Amendments
Version 0.5	26.06.13	Courtney Davis	Incorporated comments from SCB
Version 0.6	02.07.13	Courtney Davis	Minor Health and Safety Amendments
Version 1.0	4.07.13	Courtney Davis	Updated version control as final
Version 1.5	2.4.14	Courtney Davis	Revisions as part of annual review of document.
Version 1.6	2.4.14	Maryellen Salter	Complete review of changes
Version 1.7	4.4.14	Courtney Davis	Modification based on MS review

Contents

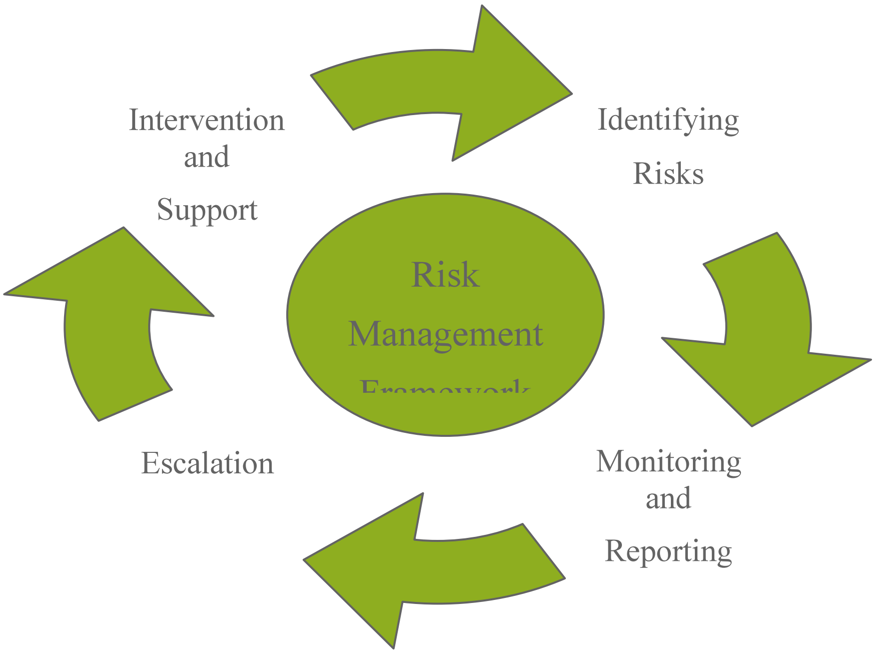
1. Introduction

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 risks inherent in the delivery of our services and associated with our plans and strategies, so as to encourage responsible, informed risk taking.

Risk Management is a fundamental part of best management practice for Directors, Assistant Directors, Lead Commissioners, Heads of Service and other managers when planning and setting objectives, assessing adequacy of 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 (but not limited to):

Strategic and financial planning	Performance management
Service design and delivery	Information Management
Policy making and review	Change management/transformation
Project management	Business continuity planning

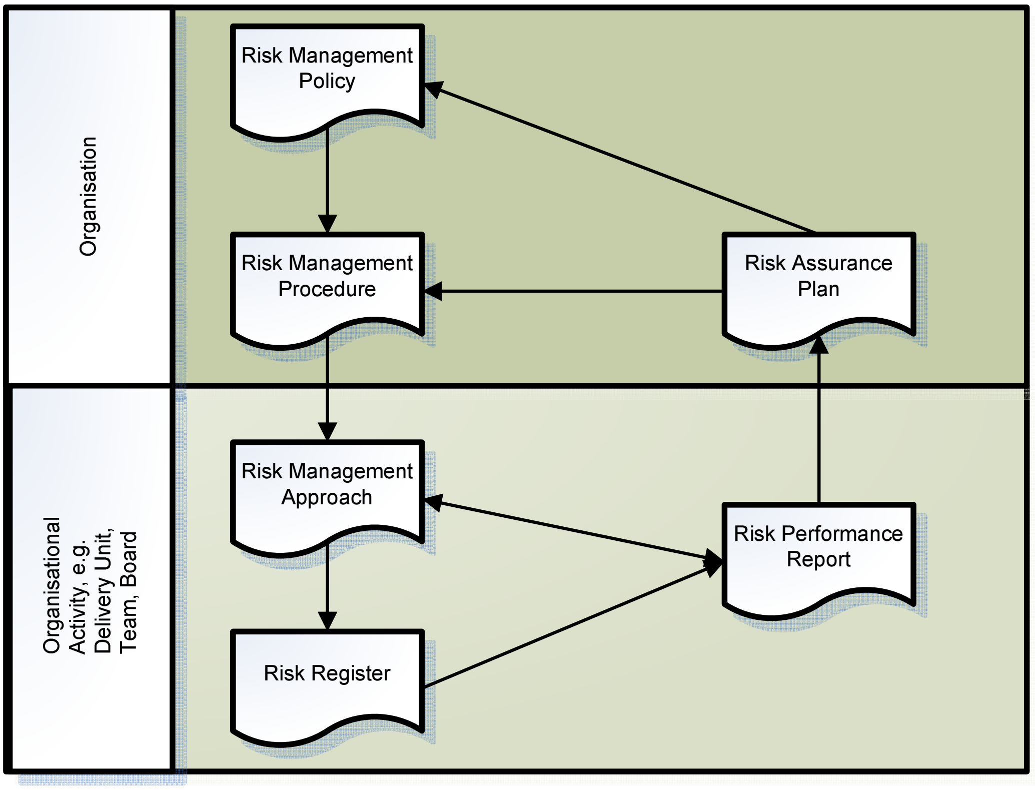
The Risk Assurance function sits within the Assurance Group and focuses on enabling the organisation to identify, monitor, report and escalate risks as well as playing an intervention and support role when required, depicted below:



The function will support and enable groups to assess their risks, assist in devising action plans and undertake gap analysis on controls. Risk management forms part of the quarterly performance management framework where risks identified (internally or joint risk with external providers) are reported quarterly and escalated as appropriate between the quarterly reporting cycle.

The Risk Management Framework, at the Strategic Organisational level, is comprised of this document, which incorporates the policy statement and procedure and the Risk Assurance plan [1] which set's the year's objectives to support the on-going improvement of risk management practice across the organisation. At organisational activity level (Delivery Unit, Team, Board) there is a risk management approach which describes how the risk management policy will be carried out for that area. Risk registers and quarterly risk performance reports also support risk management at this level and are reported at the strategic level through the quarterly performance cycle. Risk performance across the year then forms the basis of the risk assurance plan.

Risk Management Framework



At the highest level within the Council, the Performance and Contract Management Committee will approve any major changes to the Risk Management Policy. The Council's Strategic Commissioning Board (SCB) is responsible for approving this Risk Management Framework at an officer level and ensures it is reviewed annually to remain aligned with current best practice and to demonstrate that risk management evolves with the organisation. The Council participates in the Alarm CIPFA Risk Management Benchmarking Club annually as a performance assessment tool and to understand areas where standards can be improved.

[1] Internal Audit, CAFT and Risk Management Plan 2014/15

2. Risk Management Policy

2.1. Aims and Objectives

Our overarching aim is to improve the Council's ability to deliver its strategic objectives by managing threats and opportunities, creating an environment that adds value to ongoing operational activities and achieves sustained benefit across the portfolio of activities. This framework supports Barnet's strategic objectives:

1. Promote responsible growth, development and success across the Borough.
2. Support families and individuals that need it – promoting independence, learning and well-being.
3. Improve the satisfaction of residents and businesses with the London Borough of Barnet as a place to live, work and study.

The risk management framework supports achievement of strategic objectives by ensuring:

- Risk management is aligned with corporate and operational business planning and service delivery
- Risks are appropriately reviewed by the Performance and Contract Management Committee and the risk management arrangements reviewed on a quarterly basis by the Audit Committee through the inclusion of a narrative in respect of risk activity within the quarterly Internal Audit and Risk Management progress report
- Risks are regularly monitored and reviewed to ensure the risk treatment by officers and management is effective, including those risks managed by third parties
- There is a sustained effort on developing a risk aware culture and resources are appropriate to carry out effective risk management
- That the risk management framework continues to be fit for purpose and remains relevant.

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.

The Councils risk management framework is intended to support an active learning culture in which people can learn from, and respond positively to, incidents and identified weaknesses as well as recognise and take advantage of opportunities. The Council has a dedicated risk assurance function to ensure that this culture is embedded.

These aims and objectives and broad statements of approach start to define the organisation's risk appetite. Risk Appetite is a method to help guide an organisation's approach to risk and risk management; it describes the level of risk an organisation is prepared to accept before action is deemed necessary to reduce it. In conjunction with the policy statements risk appetite is gauged through the risk assessment process. By assessing the impact and probability of risks and using the guidance which provides category based examples (e.g. Finance, Health and Safety - see appendix 6.1 for guidance) people are guided on the level of risk permitted and a consistent approach across the organisation is encouraged. The Council's risk appetite should be set with reference to the corporate plan and relevant Service strategies; it is also important to involve the relevant Committee Chair when determining the risk appetite for a given risk.

2.2. Roles and Responsibilities

All Members, managers, employees and partners must proactively engage with risk management and the potential impact of risks on achieving objectives. 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).

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 practice of the Council and are formalised by means of this policy.

Performance and Contract Management Committee

Specific Responsibilities for Risk Management. The Committee is responsible for ensuring that the risk management framework is in place and aligned to Council policy.

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 Framework.

Strategic Commissioning Board (SCB)

SCB is responsible for approving the risk management framework at an officer level and for ensuring that it is reviewed and updated on a regular basis. It is also responsible for reviewing strategic risks of the Council, and overseeing the management of business and delivery unit risks against performance on a quarterly basis.

SCB "Assurance" receives reports from Risk Assurance regarding the adequacy of the risk management arrangements on a quarterly basis. In addition, on a bi-monthly basis it receives reports from Internal Audit on the outcomes from internal audit reviews and the status of any action plans to mitigate the identified risks.

Delivery Board

Delivery Board is an officer forum designed to focus on the collective delivery of strategic outcomes and the delivery of best practice across the Council's major internal and external delivery partners. Delivery Board provides scrutiny, oversight and challenge to the activities of the delivery units to ensure that outcomes are achieved in a collaborative manner. Central to the role of the delivery board is monitoring and managing performance and risk. The Board meets quarterly to review draft quarterly performance summaries, review progress against delivery of Management Agreements and the Corporate Plan including targets, finance, programmes, and risk.

Board Governance

Internal Governance Boards (enabling, programme, project) play an important role in risk management and, where available (e.g. enabling), the terms of reference will set out the risk management responsibility. Additional information on Programme and projects can be found in section 4.6.

Risk Assurance

Risk Assurance is responsible for delivering a robust risk management framework that ensures the Council meets the highest standards of risk management. Risk Assurance is responsible for updating the policy, providing training and support to teams dealing with risks. Risk Assurance will support SCB monitor risks in the Council through using JCAD reports and any other information available, for example from Internal Audit reviews.

Risk Assurance is supported by a network of Risk Champions, representatives from each area of the business and/or major programmes of work and associated risk management disciplines such as Health & Safety, Information Governance and Business Continuity. Therefore, the Risk Assurance function is a network of people working to embed risk management into processes and culture through awareness raising, challenge and promoting best practice through continuous improvement and learning.

The function plays a central role in the quarterly performance process whereby risks are reviewed for escalation from the business and delivery units to Delivery Board and SCB. It challenges on the efficacy of steps being taken to manage risks, considers cross cutting risks, emerging “hot spots”, common risks, and potential clashes of risk. Risk Champions also play a super user role in terms of the JCAD risk management system.

Service Directors and Managers

Service Directors and Managers monitor their Service specific risks and ensure an appropriate response has been implemented. Risks are reviewed against performance on a quarterly basis for reporting to Delivery Board and SCB and include on the monthly performance monitor. Service Directors and Managers have oversight of risk management and seek the involvement of the relevant Committee Chair in determining the risk appetite for the Service in general and for discussion on specific risks with a medium-high or more rating.

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.

Internal Audit

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 on an exception basis for 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).

2.3. Reporting and Monitoring

Day to day monitoring and escalation of risks is described in section 3.3; when a risk is identified a risk assessment is carried out; a medium high rating triggers a discussion with Manager/Risk Champion on the level of the organisations most appropriate to manage the risk. Once assigned, the risk owner is responsible for the management and control of all aspects of the risk including the implementation of the measure taken to control the risks; risk response actions can be delegated but ownership resides with the risk owner.

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 as well as ensuring the performance interventions and risk escalations are appropriately aligned. The quarterly performance report will be reported to Delivery Board, SCB, Performance and Contract Management Committee.

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 updates on risk management within the Internal Audit and Risk Management progress report.

Assurances on the effectiveness of key controls

The annual programme of internal audit work dedicates resources to test the key controls specified within the risk registers noted to mitigate level of risk the Council is exposed to. Internal audit test both the design of the controls and the effectiveness of these controls. Reports are issued to management that note, where appropriate, action required if there are some deficiencies noted within the internal control environment. It is management that is primarily responsible for the internal control environment and the effectiveness of it, where internal audit make recommendations management should have due regard to those recommendations in order to prevent fraud and/or error. In addition, external audit base their plan on the key risks of the Council and this independent source of assurance should be noted within the risk registers where relevant.

Annual Governance Statement

The Council has to produce an Annual Governance Statement every year, which is an assessment of the governance system in place and the sources of assurance obtained during the year, internal and external. The risk management framework will provide assurance to SCB and Members that risks are being properly managed.

3. Risk Management Procedure

The following provides guidance and instruction on how to implement the risk management policy. The primary components of the risk management process are:

1. Risk Assessment
2. Recording and Managing
3. Monitoring and Reporting
4. Intervention and Support

3.1. Risk Assessment

Risk assessment is the process of identifying risks, assessing the impact, probability and appropriate response to the risk with control actions/mitigations.

Risk assessment should be carried out, at a minimum, on an annual basis at team, service 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 inspections and audits or though workshops and brainstorming throughout the year.

Risk assessments should be carried out as early as possible in the life cycle of any new commission, project, programme or partnership. The resultant risk register should be shared as appropriate and/or signed off by the relevant board.

The following are examples of risk assessment techniques:

- Workshop and brainstorming (PESTEL, SWOT, Horizon Scanning)
- Flowcharts and dependency mapping
- Inspections and audits
- Research and review, e.g. lessons learned documents

See section four for additional subject specific guidance.

3.2. Recording and Managing

When a risk has been assessed it should be entered into JCAD, the Corporate Risk Management Tool, to ensure a consistent approach to recording, managing and reporting on risks and their associated controls and actions plans. See section five for additional information on JCAD.

The following risk categories apply and define the risk perspectives of the organisations.

- Strategic: concerned with ensuring overall business success, vitality and viability
- Operational: concerned with maintaining appropriate levels of business service
- Project: concerned with delivering defined outputs to an appropriate level of quality within agreed scope, time and cost constraints. This category also includes Programme level risks which sets the scene for the management of risk within the programme and projects and operational activities that form part of the programme.
- Joint: are concerned with shared risks between two parties (commercial, partners) where the Council retains some risk exposure and/or where both parties have a role in managing the risk.

The following table is similar in format to the risk form in JCAD and provides descriptions of the fields and drop down menu’s which need to be completed.

Corporate Plan	Select from the drop-down list the objective from the corporate plan the risk is impacting	
Category	Choose one of the following:	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/issue: are those risks/issues which affect the intended outputs or benefits of the project
		Joint Risk: shared risks between two parties (commercial, partners) where the Council retains some risk exposure and/or where both parties have a role in managing the risk
Nature of Risk	Choose one of the following: *If more than one applies please choose the one which will have the greatest impact on the council or project.*	Business Continuity: a risk that has an impact on the ability to deliver services during an event of a significant disruption that threatens/effects the ability of the organisation to deliver its services.
		Compliance: a risk that prevents compliance with legislation, policy or strategic guidance
		Financial: a risk that has a financial impact on the project and / or council.
		Health & Safety: a risk that has a detrimental effect on the wellbeing of staff or contractors of the Council
		Information Governance: a risk which will have a detrimental effect on the council or a member of the public due to the creation, distribution, archiving or destruction of information assets
		Reputational: a risk that is visible to or have a direct impact on external parties which could damage the reputation of the Authority.
		Staffing & Culture: a risk that has impacts on motivation, staffing levels and/or arrangements that may be at odds with the culture of the organisation.
		Unassigned: None of the above are applicable.
Risk Description	Provide succinct and sufficient description of the risk	
Control(s) In Place	Describe the controls that are in place to manage and monitor the issue. Controls can be either preventive or detective. Preventive controls are proactive and attempt to deter or prevent undesirable acts from occurring. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets. Detective controls attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, reconciliations, physical inventories, and audits.	
Cause/Consequence	Describe the cause of the risk and the consequences if the risk occurs	
Assigned to	Assign owner	
Status	Choose one of the following:	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. Section 4.2 of this policy considers the Commissioning perspective of risk transfer in more depth.
		Terminate: Some risks will only be treatable or containable to acceptable levels, by the termination of the activity.
		Closed: Used when closing a risk
Review every	This field sets the review period. The default is 3 months but should be reset to an appropriate interval	
Risk Assessment Section: Using the 5X5 impact and probability risk matrix (described in more detail in next section) to determine the risk profile: initial (without any controls), current (residual with existing set of controls) and target (level of risk that the owner is prepared to accept and will drive what additional controls are required). Cost is an opportunity to assess the financial impacts of the risk, e.g. extra resources (internal and external), new systems, time delays etc.		

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**; this is described as the current risk rating. 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.

	Score:		**PROBABILITY**				
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost Certain
IMPACT	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 required** **Only log in JCAD if there is a need to document and monitor or there is a possibility the risk profile may change.**
4-6 Moderate Risk	**A risk at this level may be acceptable** **Maintain existing controls if any, no further action or additional controls required**
8-12 Medium 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 High Risk	**Unacceptable** **Immediate action must be taken to manage the risk** **A number of control measures may be required**

Additional guidance on the definitions of probability and impact and examples is provided in Appendix 6.1

3.3. Risk Monitoring and Reporting

Risks are to be monitored according to the level of risk noted by the risk matrix above; this will also dictate the level of management attention required. Business and Delivery Units are responsible for ensuring all staff know how to report a risk for monitoring by Management. Regular monitoring and review is carried out by the risk owner, however risk should be discussed regularly at team meetings and one to one meetings if appropriate.

JCAD should be used for assigning risk owners and setting the frequency of review. Risks should be reviewed at appropriate intervals and the risk review process should not be overly onerous. As a general rule, risks with a higher risk rating should be reviewed more frequently while risks with a lower risk rating require less attention; however, the risk assessment should be used to decide the most appropriate review period. If the risk profile is low but is expected to be volatile then it could warrant more frequent review. Conversely, a high rated risk may not be expected to change over a 6 month period so reviewing monthly would be unnecessarily burdensome. A risk response of tolerate would also indicate that a longer review period could be appropriate.

Questions to ask during monitoring and review:

- Is the risk still relevant?
- Is there any movement in the score?
- Are the controls still in place and operating effectively?
- Has anything occurred which might change its impact and/or likelihood?
- Have potential opportunities been considered and maximised?
- Have any significant control failures or weaknesses occurred since the last monitoring exercise?
- If so, does this indicate whether the risk is increasing or decreasing?
- If the risk is increasing do I need to devise more controls or this of other ways of mitigating the risk?
- If the risk is decreasing can I relax some of the controls?
- Are controls/actions built into appropriate documented action plans?
- Are there any new emerging risks?
- Have any of the existing risks ceased to be an issue and can therefore be closed?
- If so, complete a final review to identify the reasons for closing and close the risk. Ensure that any relevant lessons learned are documented and or shared as appropriate.

Risk Escalation process

When the risk assessment is carried out consideration should be given to who is the most appropriate person to own the risk and at what level of the organisation the risk should be managed. The general guidance is that a medium-high risk rating triggers discussions with management and potential escalation of the risk. It should be noted that risk escalation is not about changing the ownership of the risk; it is about escalating the profile of the risk and raising awareness of the risk at appropriate levels in the organisation. Raising the profile of the risk could be about decision making, resources required to mitigate the risk or that the impact cuts across different perspectives of the organisation, e.g. programme, operational, strategic, and the risk should therefore be assessed from those perspectives if it hasn't been already. The following stages shall apply:

1. The individual/team/project should seek the involvement of their Risk Champion or other specialists to ensure the risk score is appropriate and consistent with this risk management framework by referencing guidance on impact and probability in appendix 6.1.
2. Assuming the risk score remains medium-high or above, the risk is to be considered for inclusion within the relevant Service risk register on JCAD and taken forward in management team meetings and 1:1 discussions.
3. All risks with a medium-high or above rating are to be included within the performance monthly monitors and agreed at each Senior Management Team (SMT) or equivalent for each Service. If appropriate, officers should seek the involvement of the relevant Committee Chair in determining the risk appetite.
4. As part of the risk assurance function; Risk Champions will participate in the quarterly performance process whereby risks are monitored to ensure they have been reviewed and updated as appropriate for reporting purposes and to agree if any risks require escalation to Delivery Board.
5. The quarterly report for each Service 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 a current score of 12 or more will also be presented for each service. This report includes a description of the risk, the current score, control activities, the risk response and a target risk score. The quarterly report is the formal mechanism for escalating risk at Delivery Board.
6. SCB risks will be reported to SCB as part of the performance reporting cycle and at Performance and Contract Management Committee quarterly. SCB risks will also be reviewed and new risks considered at SCB Assurance on bi-monthly basis.

3.4. Intervention and Support

The Risk Assurance function plays a central role in the quarterly performance process and supports Boards, Services and risk owners by challenging on the efficacy of steps being taken to manage risks, considers cross cutting risks, emerging "hot spots", common risks, and potential clashes of risk.

Support is also provided through training and development. Risk Assurance produces a training and development plan for the forthcoming year to ensure roles and responsibilities are understood and risk management is properly embedded into processes and culture through awareness raising, challenge and promoting best practice through continuous improvement and learning.

Risk Assurance will support SCB to monitor risks in the Council through using JCAD reports and any other information available, for example from Internal Audit reviews.

Serious risk incidents

A serious risk incident is an incident that occurs and that results in the Council suffering loss that is financial, reputational or operational. Incidents that occur and have an impact rating, as per the risk matrix, of 4 (major) 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 service level budget • Claims of >£150k
Reputational	• National media coverage with key Services 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

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 Assurance Function to foster a culture of learning from these untoward incidents. Directors and Managers will be required to demonstrate to SCB and Committee Chairs what actions have been taken to improve the design or implementation of controls with regards to the risk recurring.

4. Subject Specific Guidance

The policy and procedures set out in this document are appropriate for use by all disciplines; however, the following provides additional guidance on specific subjects.

4.1. Commissioning Services

The Council has a responsibility when managing commissioning relationships (commercial partnerships or shared services) to ensure that the arrangements have effective risk management procedures and to provide assurance that risks are being identified, prioritised and appropriately managed. A summary checklist for managers covering the key aspects of this section has been included, see Appendix 6.2.

The purpose of risk management in the commissioning context is as follows:

- To ensure proper identification and understanding of risks associated with a commissioned service including delivery risks, joint risks and retained risks.
- To support clear allocation of responsibilities for managing and monitoring risk
- To agree the risk appetite for management of risks amongst all partners
- To align the response to identified risks with corporate priorities
- To provide a framework for information sharing regarding risks and performance management
- To distinguish the level and type of risk to the council and to the delivery of the commissioning arrangement

At the earliest stage of the commission consideration should be given to existing risks associated with the delivery of the service. It is expected that an integral part of the commissioning exercise will be to establish clear arrangements on how the Council and the commissioned organisation will document, monitor and manage risks. It is expected that the commissioning arrangement will include a requirement that the commissioned organisation maintains a minimum standard of risk management procedures, proportionate to the size of the contract

As part of a commissioning exercise and as a result of any new arrangement risks for the Council will need to be considered and assessed; these could be new commercial risks, retained risks where the risk transferred to the new commissioned organisation but the Council retains some risk exposure and/or joint risks where both parties have a role in managing the risk.

The following sections provide more information on transferring, retained and joint risks as well as monitoring risks and sharing information.

4.1.1. Transferring and retained risks

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

The transference of risk should be agreed as part of the commissioning process and stipulated as appropriate in the contract. Transferred risks should be closed in the corporate risk management system (JCAD) and the approach to transferring and closing should be documented and auditable.

Not all risks will fully transfer, therefore 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 existing 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:

- 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
- Information
- Some health and safety and financial risks

Risks that can still impact the Council should be recorded within the Council's risk management system. As mentioned previously, it is important to involve the relevant Committee Chair when determining the risk appetite for a given risk; this principle remains applicable when risks are being considered for commissioned services.

4.1.2. Dealing with joint risks

In general it is expected that risks will be clearly allocated to either the Council or to the commissioned organisation, however, a small number of risks may be assessed as being shared between parties. In these circumstances it is essential that the Council and commissioned organisation develop a joint approach and risk register. It should be considered which party is best placed to deal with the risk and the actions each party will undertake in order to manage the risk should be clearly defined. The aim of the approach adopted will be to help develop partnership working, with all parties working together to effectively manage risk and achieve common goals.

4.1.3. Monitoring Risks

Risks should be managed and monitored regularly as part of day to day operations and escalated whenever required. It is recommended that the commissioner considers how they will ensure that they have sufficient technical expertise available to understand and interrogate the risk and performance data that is collected from the commissioned organisation. Over the course of the service contract it is likely that the risk profile will evolve therefore it is important to develop an open dialog based on common understanding of risks management (processes and terminology) and of the objectives of the partnership.

If the commissioned arrangement is subject to quarterly performance reporting; the report will include risks wholly owned by LBB, joint risks and significant operational risks (with a rating of 12 or more using LBB's scoring methodology). 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 significant changes to the risk management strategy/approach in the forthcoming year

4.1.4. 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 including non-routine access where there are signs of failure on contract delivery. 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.

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.

4.2. Business Continuity

Having in place appropriate and fully tested business continuity plans allow officers to manage threats or incidents that may occur, that have the potential to disrupt the delivery of services or the conduct of Council business.

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.

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: understanding the organisation; determining the Business Continuity Strategy; developing and implementing the BCM plans; and exercising maintaining and reviewing BCM.

4.3. 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 activity, bribery, corruption and/ or money laundering activities. It is important that you are familiar with the Council’s Counter Fraud Framework (which includes the Fraud Policy, Anti-bribery Policy, Whistleblowing policy and Anti-Money Laundering) and the principles, responsibilities and requirements that are set out within them.

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/or related fraud activities to exist, they should include reference to any previous CAFT investigations or reviews 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 in relation to fraud prevention;

- Verification of information
- Segregation of duties
- Authorisation hierarchy
- Transparency
- Audit trail and record keeping

For further advice on fraud related risks you should contact the CAFT directly.

4.4. Health and Safety

The Council recognises that effective management of health and safety supports the delivery of our services for the residents of Barnet. As part of the overall risk management culture and process, good health and safety management will help reduce injury and loss, help promote a healthy workforce, help protect all who are affected by the Council’s activities and ensure we comply with our legal duties. Forming part of the Council’s Health and Safety Management System, our Health and Safety Policy explains what is necessary to manage health and safety effectively and in line with legislation. It identifies roles and responsibilities and provides specific guidance on health and safety risk assessment techniques, implementing and reviewing controls as well as special guidance on issues relating to special risk groups.

The risk management principles of the Councils Health and Safety policy are in accord with the principles established within this framework. It is recognised, however, that as a discipline in its own right, health and safety practice, risk management tools and techniques can be specialist in nature. Therefore, please refer to the Corporate Health and Safety Policy and, in particular, the Managing Health and Safety Arrangement for additional information and guidance.

4.5. Information Management

It is important to ensure information risks are addressed as part of business as usual and at the start (and throughout) any new commission/project and should include not only risks to the organisation but also any potential risk to individuals whose information we are handling. The Data Protection Compliance Toolkit is a tool to aid Staff/Managers in assessing risk and compliance with the Data Protection Act principles and direct them to appropriate Council policies/guidelines. The toolkit can be found on the intranet under the Information Governance policies page.

4.6. Programmes and Projects

This guidance should be used in conjunction with the Corporate Project Management toolkit.

Definitions:

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.

Roles and Responsibilities:

Project Managers are responsible for the development and maintenance of a **Project Risk Register** for each of the projects which they manage. In the case of information risks an Information Governance Impact Risk Assessment will also need to be completed (see Appendix D). 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.

5. Additional Information

The following documents can be found on the intranet in the Risk Management section.

https://employeeportal.lbbarnet.local/home/departments-and-services/central-services/risk-management.html

- Risk Management Framework
- Risk Champion Role Profile
- JCAD User Guide
- JCAD Barnet User Guide
- JCAD Reporting Guide
- Risk Champions Contact Information

Advice and support can be provided by the Risk Assurance Manager, and/or Risk Champions. All risk champions are given training and development support to ensure that they have competence for managing risk. For subject specific advice, please contact the relevant team.

Additional training either on Risk Management or JCAD can be provided upon request. Group training is the preferred approach; however, exceptions can be made for 1:1 training if it is essential.

6. Appendix

6.1. Probability and Impact Examples

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 or recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not persisting issue	Will undoubtedly happen/recur, possible frequently

Impact score

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**
Business Continuity	No or minimal disruption (< 1 hour) to service or conduct of Council business	Disruption to service or conduct of Council business of < 1 day	Disruption to service or conduct of Council business of < 3 days	Disruption to service or conduct of Council business of > 3 days	Disruption to service or conduct of Council business of > 7 days

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	No or minimal financial loss (including risk of claim) <1k	Loss of 0.1-0.25 per cent of council's net budget (approx £300k - £750k) Risk of claims less than £20k	Loss of 0.25-0.5 per cent of council's net budget (approx £750k - £1.5m) Risk of claims between £20k - £150k.	Uncertain delivery of key objectives/ saving plan contributing to a loss of 0.5 – 1.0 percent of council's net budget (approx £1.5m - £3m) Risk of claims between £150k to £1m	Non delivery of key objective/ saving plan contributing to a loss of >1 percent of council's net budget (approx £3m) Loss of major contract (s) Risk of claim > £1m
Health & Safety	Minor injury Cuts, bruises, et Unlikely to result in sick leave	Minor injuries: Likely to result in 1-3 days absence	Moderate injuries: Likely to result in 4-9 days absence	Major injuries: prescribed major injury or condition (RIDDOR Reportable)	Fatality
Information Governance	No or minimal impact upon customer/staff information governance rights. No or minimal customer/ staff harm or distress. No or minimal impact upon authority / third party confidentiality of data.	Minimal/ moderate impact upon customer/ staff information governance rights. Minimal/moderate customer or staff harm or distress. Minimal/ moderate impact upon authority / third party confidentiality of data. Non-compliance with best	Non-compliance with IG polices and statutory duties. Breach / incident involving personal data or sensitive / confidential data. Breach or incident not reportable to governing body. E.g. ICO or FSA.	Non-compliance with IG polices and statutory duties. Breach / incident involving significant personal data or sensitive / confidential data. Breach or incident is reportable to governing body. E.g. ICO or FSA.	Significant failure of compliance with IG polices or statutory duties. Immediate action required to mitigate and contain breach / incident. Breach or incident is reportable to governing body. E.g. ICO or FSA

Impact score	1	2	3	4	5
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
		practice.			
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 services 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

6.2. Commissioning Services Checklist

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 4.2)

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 procurement process (e.g. 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 Officers and Committee Chairs 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