Risk Management Framework

V2

October 2016

Document control

Description	Risk Management Framework	
Version	**V2**	
Created	September 2016	
Status	**Final**	
Authorisation	**Name**	**Date**
Prepared by	Head of Performance and Risk	September 2016
Checked by	Strategic Lead for Programmes and Performance	October 2016
Cleared by	Strategic Commissioning Board	11 October 2016
Approved by	Performance and Contract Management Committee	15 November 2016 (TBC)

Contents

1. Introduction 4

2. Executive summary 5

3. Aims and objectives 8

4. Understanding risk 10

5. Risk management levels 11

6. Risk management process 12

7. Commissioned services 18

8. Projects 20

9. Annual review and quality assurance 21

Appendix A - Roles and responsibilities 22

Appendix B - Risk assessment criteria 26

Appendix C - Quarterly reporting timetable 29

1. Introduction

The risk management framework sets out the **principles and approach to managing risk** in Barnet Council, including the process of identifying, assessing and controlling risk.

What is risk?
Risk is defined as an **uncertain event** that, should it occur, will have an impact on the organisation's ability to achieve its objectives. A risk is measured by the likelihood of a perceived threat or opportunity occurring and the magnitude of its impact on the organisation's objectives.

What is risk management?
All organisations, including temporary ones such as projects, will experience uncertain events when trying to achieve their objectives. Risk management is a visible way of managing these risks in a structured, consistent and timely way that supports effective decision-making.

Why is risk management important?
Risk management plays an important role in planning and setting objectives, assessing the adequacy of internal controls and monitoring performance – essentially, helping the organisation to manage the business. Risk management is a key part of corporate processes, such as:

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

And, when fully embedded, risk management is likely to:

- Improve performance against objectives and delivery of outcomes
- Improve the identification of threats and opportunities
- Improve governance, stakeholder confidence and trust
- Establish a reliable basis for decision-making and planning
- Effectively allocate and use resources for risk treatment
- Improve organisational resilience

The risk management framework has been approved by the Performance and Contract Management Committee; and is reviewed on an annual basis by the Strategic Commissioning Board and Performance and Contract Management Committee to ensure it remains aligned with best practice and evolves with the organisation (see Section 9: Annual review and quality assurance).

2. Executive summary

This section provides a summary of the **risk management process** and outlines the **key roles and responsibilities** in ensuring that this process is managed effectively.

Risk management process (see Section 6)

The risk management process is a series of logical steps that are carried out in sequence to progress through each stage of managing a risk:

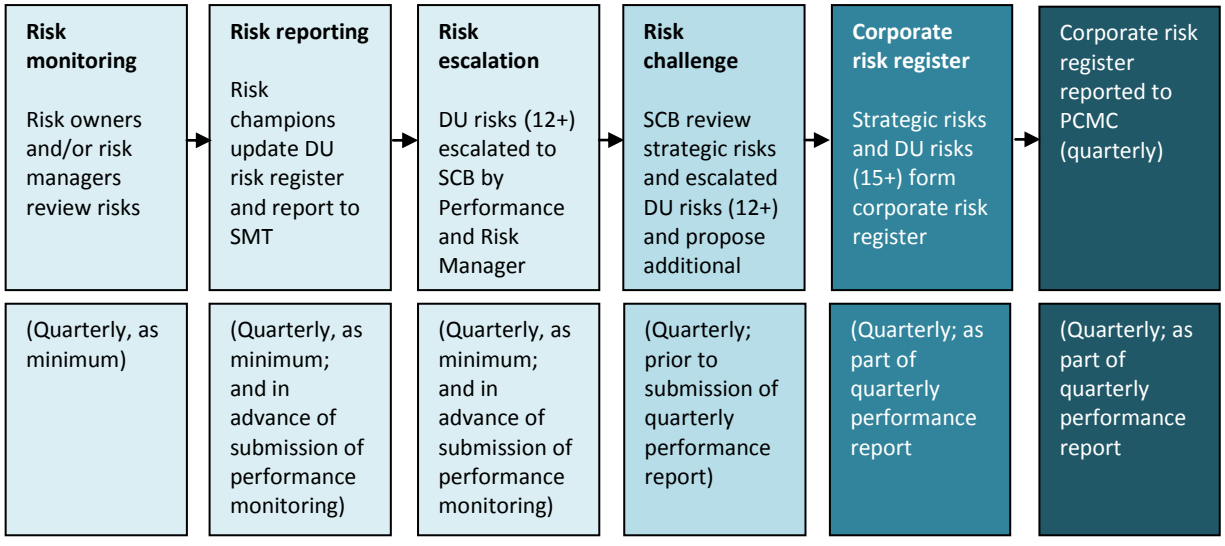
1. Risk identification
2. Risk assessment
3. Risk response
4. Risk monitoring, reporting and escalation
5. Risk appetite
6. Communication and consultation

1. Risk identification - When a risk is identified, a description should be provided on the **cause, event and consequence.** This should be written in a clear and concise way that is meaningful to all stakeholders, including members and the public, and should not contain any sensitive or commercial information (see Section 4: Understanding risk). The risk should be raised with the relevant risk champion who should ensure that it is discussed at the appropriate Board or Senior Management Team meeting. If the risk is accepted, the risk champion should add it to the relevant **risk register.** The risk should be assigned a risk owner (the senior officer) and risk manager (the most appropriate officer to manage the risk) and a category e.g. strategic or financial.

2. Risk assessment - The risk owner should assess the **likelihood** and **impact** of the risk occurring. The combination of the two scores should produce the risk score and risk rating (low, medium/low, medium/high or high). See Section 6: Risk management process.

3. Risk response - A decision should be taken on how best to respond to the risk e.g. treat, terminate, tolerate or transfer. If treating the risk, **controls and/or mitigations** should be put in place. See Section 6: Risk management process.

4. Risk monitoring, reporting and escalation



Risk monitoring - The **risk owner** is responsible for all aspects of the risk, including ensuring appropriate controls and/or mitigations are in place; and should monitor the risk on a regular basis (quarterly, as a minimum). The risk owner should **review** the controls and/or mitigations in place to determine if they are still effective and follow-up on any actions that have been proposed to help reduce the likelihood of the risk occurring. The likelihood and impact scores should be re-assessed and the combined risk score re-calculated for the residual risk.

Risk reporting - The **risk champions** should play a key role in risk monitoring and reporting. They should liaise with the risk owners and/or risk managers in their respective Delivery Units to ensure risks are regularly monitored (quarterly, as a minimum) and should keep the risk register up-to-date. They should pull together reports and attend relevant meetings to present the updated risk register (quarterly, as a minimum) and provide a level of challenge on the risk information provided. This role should be carried out in accordance with the risk monitoring timetable provided by the Performance and Risk Team.

Risk escalation - Any risks that **score 12 or above** should be escalated to the service risk register by the risk champion. The Senior Management Team should discuss the effectiveness of the controls and/or mitigations in place and review any actions being taken to further reduce the likelihood of the risk occurring. They might propose additional actions or assign resources to help mitigate the risk in the future. The risk champion is responsible for communicating any additional actions back to the risk owner and/or risk manager; and forwarding a copy of the DU risk register, including the escalated risks to the Commissioning Director.

The risk champions should highlight any **service risks that score 12 or above** to the Performance and Risk Manager and these should be escalated to the Strategic Commissioning Board for review each quarter. As above, the effectiveness of the controls and/or mitigations in place and actions being taken to further reduce the likelihood of the risk occurring should be discussed; and any additional actions may be proposed or resources assigned to help mitigate the risk in the future (which should be communicated back to the risk champion by the Performance and Risk Manager).

After Strategic Commissioning Board has met, the strategic risk register and any service risks that score 15 and above should be combined to form the **corporate risk register.** This should be reported to Delivery Unit Board, Strategic Commissioning Board and Performance and Contract Management Committee, as part of the Performance Monitoring Report, each quarter (see Appendix C: Quarterly reporting timetable).

5. Risk appetite - This is the level of residual risk the organisation is prepared to tolerate before action is considered necessary to reduce it. This has been set at a combined likelihood and impact score of 15. By setting a risk appetite, officers should be guided on the level of risk tolerated and assurance should be given that a consistent approach to managing risk has been applied across the organisation.

6. Communication and consultation - This should take place throughout the risk management process with relevant officers in the Delivery Unit and the Performance and Risk Team.

Key roles and responsibilities (see Appendix A)

There are four key roles in relation to the risk management process that ensure the process is managed effectively. These are the risk owner, risk manager, risk champion and Performance and Risk Manager.

Officer	Roles and responsibilities
Risk Owner	• Responsible for individual risks • The senior officer for the area of work that the risk relates to • Management of the risk may be delegated to a risk manager(s) (if delegated, accountability for the risk is retained by the risk owner) • Assess the risk and assign it a score for likelihood and impact
Risk Manager	• Manages the controls and/or mitigations in place • Supports the risk owner in monitoring and reporting risks (this function may be delegated by the risk owner to the risk manager but the risk owner retains accountability for the risk)
Risk Champion	• Advise officers within the Delivery Unit on the application of risk management framework, including risk identification; risk assessment; monitoring, reporting and escalation • Maintain their respective service risk register by collating information on new and updated risks through discussions with risk owners • Attend SMT meetings to present updates on their risk register, and to challenge senior management on the information on risks and delivery of actions • Ensure risks are reviewed and risk registers are up-to-date ahead of quarterly reporting (in accordance with timetable)
Performance and Risk Manager (Performance and Risk Team)	• Implement the organisation's performance and risk management frameworks and build performance and risk management capability across the organisation • Provide assurance that the strategic objectives are being delivered through effective performance and risk management arrangements • Advise senior managers on performance and risk management arrangements and provide support to the Head of Performance and Risk in annually reviewing the performance and risk management frameworks • Responsible for corporate monitoring and challenge of performance and risk data, including the co-production and monitoring of improvement plans where necessary

2. Aims and objectives

The overarching aims of the risk management framework are to **improve the organisation's ability to deliver its strategic objectives by managing risk**; creating a risk culture that adds value to operational activities; and achieving sustained benefit across the portfolio of activities.

The risk management framework supports the organisation's strategic objectives, based on the core principles of fairness, responsibility and opportunity, to make sure Barnet is a place:

- Of opportunity, where people can further their quality of life
- Where people are helped to help themselves, recognising that prevention is better than cure
- Where responsibility is shared, fairly
- Where services are delivered efficiently to get value for money for the taxpayer

The framework should help to ensure risk management is embedded throughout the organisation and involves all key stakeholders, including officers, senior managers, members and partners, by:

- Enabling the organisation to anticipate and respond to emerging risk, including from a changing operating environment
- Implementing a consistent approach to managing risk
- Ensuring risks are regularly monitored and actions to mitigate risk are effective
- Ensuring high-level risks are reviewed by the Performance and Contract Management Committee; and risk management arrangements are reviewed by the Audit Committee on a quarterly basis
- Providing oversight, challenge and assurance that risk is being effectively managed across the organisation
- Focusing effort on developing a risk aware culture and aligning resources to carry out effective risk management

The mechanics of risk management are not to simply identify risks but to implement effective controls to mitigate those risks. The risk management approach is built around **clear ownership of risks** and the identification of nominated risk managers to implement and maintain the controls, followed up by a monitoring and reporting process to ensure that those risk managers take **responsibility for the actions** agreed.

Primarily, the Strategic Commissioning Board and members should focus on the **strategic and business critical risks** that could impact on the achievement of objectives or successful delivery of outcomes; and Delivery Units/Service Providers should focus on **service risks** - whereby risks should be managed locally and escalated to the strategic level only if they become significant.

The framework is intended to support an active learning culture in which officers can learn from, and respond positively to, events as well as recognise and take advantage of opportunities. The organisation has a dedicated **Performance and Risk Team**, as part of the Commissioning Group, to ensure that this culture is embedded.

The **Performance and Risk Team** is responsible for managing the organisation's approach to risk management. The team provides support, guidance, advice and tools for enabling the organisation to manage risk. As part of this, training and development should be provided to ensure roles and responsibilities are properly understood and risk management is embedded into processes and culture through awareness raising, challenge and promoting best practice.

3. Understanding risk

What is and isn't a risk?
A risk is an an **uncertain event** that, should it occur, will have an impact on the organisation's ability to achieve its objectives. **It is not an unplanned event that has already occurred**, or will definitely happen, which is certain to affect the achievement of objectives - this is an issue.

How is risk described?
A risk is described by using the following three criteria – cause(s), event(s) and consequence(s).

- **Cause(s)** are the conditions, circumstances, drivers or activities that may result in the risk event occurring. They are the sources of the risk event or the reason why the risk could happen. A cause can be internal or external to the organisation.

- **Event(s)** are the actions, incidents or occurrences that arise from a cause that could have an effect on the achievement of objectives. Risk events can happen internally e.g. to people, processes or systems and externally.

- **Consequence(s)** are the possible consequences arising from the risk event that affect the achievement of objectives. The effects can be measured through estimating the impact on, for example, strategic/operational objectives, finances and reputation.

Who is the risk owner / risk manager?
The risk owner has responsibility for the risk in question. This should be the **senior officer** for the area of work that the risk relates to. Management of the risk may be delegated to a risk manager(s) who should be responsible for managing the controls and/or mitigations in place. [Note that if this function is delegated, the risk owner retains accountability for the risk]. The risk owner is required to assess the risk and assign it a score for likelihood and impact (see Section 6: Risk management process).

What if a risk owner / risk manager leaves?
If a risk owner or risk manager leaves the organisation, a new risk owner or risk manager should be identified and the risk register updated by the relevant risk champion. It is the responsibility of the owner of the risk register (e.g. the Delivery Unit Director) to ensure that the new risk owner is aware of his/her responsibilities in relation to the risk. It is the responsibility of the risk owner to ensure that the new risk manager is aware of his/her responsibilities for managing the risk, in relation to the controls and/or mitigations and any additional actions in place to reduce the likelihood of the risk occurring in the future.

A periodic review of risk owners (to check they are still employed by the organisation) should be undertaken by the Performance and Risk Team, as part of the annual review of the risk management framework (see Section 9: Annual review and quality assurance).

5. Risk management levels

The organisation's approach to risk management is founded upon ensuring **risk is effectively and consistently managed across all levels of the organisation**. The risk culture that emanates from the strategic leadership team throughout the organisation is essential in ensuring all levels buy into and adhere to the corporate risk process. The levels are:

- **Corporate**: the **corporate risk register** is a combined register consisting of the strategic risk register and escalated risks (15 and above) from the service risk registers. It should be reported to Performance and Contract Management Committee for scrutiny and challenge on a quarterly basis, as part of the Performance Monitoring Report.

- **Strategic**: the strategic and business critical risks are identified on the **strategic risk register**, which should be reviewed by the Strategic Commissioning Board on a quarterly basis alongside the escalated service risks. This should involve challenging the risk scores, seeking assurance on the effectiveness of controls and/or mitigations in place and recommending additional actions to reduce the likelihood of the risk occurring in the future. This level should set the tone for effective risk management across the whole organisation.

- **Service**: risks against delivery of contracts **(joint risks)** or management agreements are identified on **service risk registers**, which should be reviewed by Senior Management Teams on a quarterly basis (as a minimum). [Note that this level should include commissioning risks associated with the service; and joint risk registers with commissioned organisations e.g. Barnet Group, CSG and Re]. This level should be the key lever for the escalation of risks through to a strategic level when they become significant (12 and above).

- **Team**: risks arising from local operations are identified on **team risk registers**, which should be reviewed by Team Managers on a quarterly basis (as a minimum). Risks should be escalated to service risk registers when they become significant (12 and above).

- **Projects**: risks to projects are identified in the initial business case stage and added to **project risk registers**. Risks should be reviewed throughout the project lifecycle to ensure objectives can be achieved and reported on an exception basis to the relevant Project Board. Risk that score 12 and above should be escalated to the Senior Management Team meeting for review (quarterly, as a minimum)

6. Risk management process

The risk management process is a **series of logical steps that are carried out in sequence to progress through each stage of managing a risk**. The process is cyclical and it may be necessary to revisit earlier steps and carry them out again to ensure a complete picture of the risks in relation to the activity/outcome have been captured. The activity 'communication and consultation' deliberately stands alone as the findings of other steps may need to be communicated at any time in the process.

Fig. 1 Risk management process

1. Risk identification

Risk identification should be carried out, at a minimum, on an annual basis when objectives are set for the following year, as part of the **business planning cycle**. Risks can also be identified through inspections and audits or through business as usual activities throughout the year.

Any new risk that could impact on the achievement of an activity, objective or outcome should be identified and a description provided on the **cause, event and consequence.** This should be written in a clear and concise way that is meaningful to all stakeholders, including members and the public, and should not contain any sensitive or commercial information (see Section 4: Understanding risk). The risk should be raised with the relevant risk champion who should ensure that it is discussed at the appropriate Board or Senior Management Team meeting. If the risk is accepted, the risk champion should add it to the relevant **risk register -** this may be at project, operational or strategic level (see Section: 5. Risk management levels). The risk should be assigned a risk owner (the senior officer for that area of work) and risk manager (the most appropriate officer to manage the risk); and the nature of risk e.g.

- Business continuity
- Compliance
- Finance
- Health and safety
- Information governance

- Staffing and culture
- Strategic

The risk owner is required to assess the risk and assign it a score for likelihood and impact. The combination of the two scores should produce the risk score and risk rating (low, medium/low, medium/high or high).

2. Risk assessment

Risk assessment is the process of assessing the **likelihood** and **impact** of a risk occurring. Risks are should be on three levels:

- **Inherent (worst case)** - assessment based on the assumption that controls and mitigations currently in place do not exist. This assessment determines the reasonably foreseeable worst case scenario for the risk, which is the most adverse set of plausible circumstances and consequences for the risk described if no controls or mitigations are in place

- **Residual (current)** - assessment based on how the risk is currently being managed. It considers how well the controls and/or mitigations currently in place are working

- **Target (where you can get to**) - determination of the desired likelihood and impact levels for the risk, based on the amount of exposure the organisation is comfortable in accepting for the benefits it derives from taking the risk, and the feasibility and cost of further treatment activities. It is the position that the risk will get to once the planned additional controls have been put in place.

To ensure consistency in assessment and the ability to compare and report on the various levels of risk, the organisation has adopted a **5x5 risk matrix** to assess the likelihood and impact of the risk occurring. The risk matrix is used to evaluate the risks, so that there is an understanding of the risk exposure faced, which in turn influences the level of risk treatment that is applied to manage, reduce or prevent the risk from occurring.

A risk is broken down into likelihood and impact:

- **Likelihood** represents the statistical chance of an event taking place. This can be rare, unlikely, moderate, likely or almost certain

- **Impact** represents the expected disruption to the organisation. This is summarised as negligible, minor, moderate, major or catastrophic

Fig. 2 Risk matrix

IMPACT	Score:		LIKELIHOOD				
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost Certain
	5	Catastrophic	5	10	15	20	25

	4	Major	4	8	12	16	20
	3	Moderate	3	6	9	12	15
	2	Minor	2	4	6	8	10
	1	Negligible	1	2	3	4	5

The resultant scores from the matrix are assigned ratings (see Fig. 3). [Note that the distinction between an acceptable and unacceptable risk is a guide and will depend on the exact risk and the ability of the organisation to add further controls].

Fig. 3 Risk ratings

1-3 Low	Acceptable risk No further action or additional controls required
4-6 Medium /Low	A risk at this level may be acceptable Maintain existing controls if any, no further action or additional controls required
8-12 Medium / High	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	Unacceptable Immediate action must be taken to manage the risk A number of additional control measures may be required

Further guidance on how to determine the appropriate score for both likelihood and impact can be found in Appendix B: Risk assessment criteria. [Note that impact is assessed in different ways depending on the nature of risk]. Ensuring that all risks are assessed using the risk assessment criteria should drive consistency through the risk management framework and enable risks to be compared and reported on against a like for like basis. It also provides the organisation with the ability to map its collective risk exposure of a particular activity, objective, outcome, function(s) or indeed whole operation.

3. Risk response

Following identification and assessment, a decision should be taken on how best to respond to the risk (see '**The 4Ts'** below) and, if accepted, treatment measures should be determined to manage the risk.

- **Treat** - implement controls and/or mitigations
- **Terminate** - avoid the activity that gives rise to the risk
- **Tolerate** - take the risk
- **Transfer** - outsource the activity; purchase insurance

If treating the risk, **controls and/or mitigations** should be put in place:

- **Controls** are activities and measures that have a specific and significant effect on reducing the **likelihood** of a risk

- **Mitigations** are activities and measures that have a specific and significant effect on reducing the **impact** of a risk, should it occur

4. Risk monitoring, reporting and escalation

Risk monitoring
The risk owner is responsible for all aspects of the risk, including ensuring appropriate controls and/or mitigations are in place to manage the risk. All risks should be monitored on a regular basis (quarterly, as a minimum). This requires the risk owner to **review the controls and/or mitigations in place** to determine if they are still effective and follow-up on any actions that have been proposed to help reduce the likelihood of the risk occurring. **Monitoring can be delegated to the risk manager(s) but responsibility is retained by the risk owner**. The likelihood and impact scores should be re-assessed and the combined risk score re-calculated for the residual risk. If additional actions can be carried out to reduce the likelihood of the risk occurring still, then these should be assigned to an officer and a date for completion agreed. The risk owner should then decide if the target risk score can be reduced further.

Questions to consider as part of risk monitoring and review:

- Is the risk still relevant?
- Are the controls and/or mitigations in place effective?
- Have the actions proposed to reduce the likelihood of the risk been implemented?
- If so, has this reduced the likelihood score?
- Has anything occurred that might change the likelihood or impact score?
- Is the risk score increasing or decreasing?
- If the risk is increasing, can further action be taken to reduce the likelihood of the risk occurring?
- If the risk is decreasing, can any of controls and/or mitigations be relaxed?

Risk reporting
Risk registers should be reviewed on a regular basis (quarterly, as a minimum) by the relevant Project Board, Senior Management Team, Delivery Unit Board or Strategic Commissioning Board (see Section: 5. Risk management levels).

The **risk champions** should play a key role in risk monitoring and reporting. They should liaise with the risk owners and/or risk managers in their respective Delivery Units to ensure risks are regularly monitored (quarterly, as a minimum) and should keep the risk register up-to-date. They should pull together reports for the Project Board or Senior Management Team and attend relevant meetings to present the updated risk register (quarterly, as a minimum) and provide a level of challenge on the risk information provided. This role should be carried out in accordance with the **risk monitoring timetable**.

Risk escalation
Any risks that **score 12 or above** should be escalated to the next risk management level (see Section 5: Risk management levels) by the risk champion. The Project Board or Senior Management Team should discuss the effectiveness of the controls and/or mitigations in place and review any actions being taken to further reduce the likelihood of the risk occurring. They

might propose additional actions or assign resources to help mitigate the risk in the future. The risk champion is responsible for communicating any additional actions back to the risk owner and/or risk manager; and forwarding a copy of the service risk register, including the escalated risks to the Commissioning Director. If the risk owner or risk manager has a particular view on how the risk might be better controlled in the future e.g. extra resources, information should be provided, along with any associated resource implications, when the risk is escalated.

The risk champions should highlight any **service risks that score 12 or above** to the Performance and Risk Manager and these should be escalated to the Strategic Commissioning Board for review each quarter. As above, the effectiveness of the controls and/or mitigations in place and actions being taken to further reduce the likelihood of the risk occurring should be discussed; and any additional actions may be proposed or resources assigned to help mitigate the risk in the future (which should be communicated back to the risk champion by the Performance and Risk Manager).

After Strategic Commissioning Board has met, the strategic risk register and any service risks that score 15 and above should be combined to form the **corporate risk register.** This should be reported to Delivery Unit Board, Strategic Commissioning Board and Performance and Contract Management Committee, as part of the Performance Monitoring Report, each quarter (see Appendix C: Quarterly reporting timetable).

Fig. 4 Delivery Unit risk monitoring, reporting and escalation

Wk 1	Wk 2	Wk 3	Wk 4	Wk 5	Wk 6	Wk 7	Wk 8	Wk 9	Wk 10	Wk 11
Risk monitoring Review risks *Risk owners and/or risk managers*		**Risk reporting** Update DU risk register and report to SMT *Risk champions*		**Risk escalation** Highlight DU risks (12+) to P&R Team *Risk Champions* Escalate DU risks (12+) to SCB *Performance & Risk Manager*	**Risk challenge** Review strategic risks and escalated DU risks (12+) and propose additional actions *SCB*	**Corporate risk register** Combine strategic risks and DU risks (15+) into corporate risk register *Performance & Risk Manager* Submit to Executive Team for DUB and SCB *Head of Performance & Risk*	**Performance & risk challenge** Review performance monitoring report *DUB and SCB* Send performance monitoring report for clearance *Head of Performance & Risk*	**Publication** Submit Review performance monitoring report to Governance Team for publication *Head of Performance & Risk*		**Performance & risk scrutiny** Scrutinise performance monitoring report *PCMC*

Fig. 5 Extract of risk register for reporting

Short Risk Title	Long Description	Risk Owner	Nature of Risk	Controls in place	Inherent Risk *(without controls)*		Residual Risk *(with controls in place)*			Response Option
					Impact	Likelihood	Impact	Likelihood	Risk Score	

Where additional assurance is required on the controls and/or mitigations in place, the Strategic Commissioning Board may request a **'deep dive'** of that risk. In this instance, the risk owner would be expected to work with the Performance and Risk Team to undertake an in-depth review of the risk, including the controls and/or mitigations in place and any best practice management, and report back to the Strategic Commissioning Board the following quarter.

Any risk event that results in the organisation suffering a major impact (score = 4) is defined as "serious". If a **serious risk event** occurs, a review of the causes that led to the event and impact should be undertaken by the Performance and Risk Team and reported back to the Strategic Commissioning Board. Relevant senior managers and directors would be required to demonstrate to the Strategic Commissioning Board and Performance and Contract Management Committee what controls and/or mitigations had been in place and why these failed; how these can be strengthened going forward and any additional actions that can be taken to minimise the likelihood of the risk recurring.

4. Risk appetite

This is the level of residual risk the organisation is prepared to tolerate before action is considered necessary to reduce it. This has been set at a combined likelihood and impact score of 15. By setting a risk appetite, officers should be guided on the level of risk tolerated and assurance should be given that a consistent approach to managing risk has been applied across the organisation.

5. Communication and consultation

Communication and consultation should take place throughout the risk management process with relevant officers in the Delivery Unit and the Performance and Risk Team.

7. Commissioned services

The organisation has a responsibility when managing commissioning relationships (e.g. commercial partnerships or shared services) to ensure that **arrangements are in place for effective risk management** and provide assurance that risk are identified and managed appropriately. The purpose of risk management in the commissioning context should be as follows:

- Ensure the identification of risks associated with a commissioned service, including delivery risks, joint risks and retained risks
- Support clear allocation of responsibilities for owning, managing and monitoring risks
- Agree the risk appetite for management of risks amongst all partners
- Align the response to identified risks with strategic priorities
- Provide a framework for information sharing regarding risks management
- Distinguish the level and type of risk to the organisation 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 would be to establish clear arrangements on how the council and the commissioned organisation should document, monitor and manage risk; and that the commissioning arrangement should include a requirement that the commissioned organisation maintains a minimum standard of risk management procedures, proportionate to the size of the contract.

Transferred risks and contractual obligations
One of the benefits of commissioning services is 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. This means that ownership of the risk and controls and/or mitigations become the responsibility of the commissioned organisation.

The risk management obligations of the commissioned organisation should be written up in a template contract extract. Particular consideration should be given to the obligation of the commissioned organisation for updating and managing risks should a process change, and for periodically providing risk registers to the relevant Performance Monitoring Manager in the Commercial Team when the contract is subject to annual review. The Commercial Team is expected to share these with the Performance and Risk Team upon request.

Retained and joint risks
As part of a commissioning exercise and/or any new arrangement, risks for the council should be considered and assessed; these could be new commercial risks, retained risks and/or joint risks, where both parties have a role in managing the risk. Retained and joint risks are defined below:

- **Retained risk** – a risk that could impact the council were it to occur, and where only the council, and not the contracted party, is responsible for implementing the controls and/or mitigations needed to manage the risk

- **Joint risk** – a risk that could impact the council were it to occur, and where the contracted party is responsible for implementing some or all of the controls and/or mitigations needed to manage the risk

Any retained or joint risks (risks shared between parties) should be identified and recorded on either the Commissioning Group risk register (retained risks) or a **joint risk register** with the commissioned organisation e.g. Barnet Group, CSG and Re.

For **joint risks**, a decision should be made on which party is best placed to manage the risk and a risk owner/risk manager assigned. The risk should be assessed for likelihood and impact and the risk response agreed, including controls and/or mitigations in place and any additional actions that would help to reduce the likelihood of the risk occurring in the future. The council should remain accountable for any joint risks.

New joint risks

If any new joint risks are identified over the course of the commissioned service, the Senior Responsible Officer (SRO) within the Commissioning Group should raise this with the relevant Performance Monitoring Manager in the Commercial Team and it should be discussed at the monthly SRO meetings. If agreed, the risk should be added to the joint risk register and assessed as set out in Section 6: Risk management process.

Monitoring and reporting joint risks

All parties should work together to effectively manage joint risks. SROs should review the joint risk registers at least every quarter, prompted by the relevant Performance Monitoring Manager in the Commercial Team and adhere to the reporting requirements as set out in Section 6: Risk management process.

8. Projects

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

What are project risks?
Project risks are risks that affect the intended outputs or benefits of a project.

Project risks should be identified in the initial stages of a new project. Risks should be assessed as set out in Section 6: Risk management process and added to the **Project risk register**. This should be signed-off by the relevant Board and included in project documentation. The project tolerances and escalation process should be clearly documented within the Project Initiation Document. The **Project Manager** is responsible for maintaining the Project risk register for each of the projects that they manage.

How are project risks reported?
Project risks should be reported to the Project Board on an **exception basis** via the project highlight report. The highlight report should typically include:

- The effectiveness of controls and/or mitigations in place and any additional actions that could be put in place to help reduce the likelihood of the risk occurring
- Any changes to risk ratings (the Direction of Travel)
- Any new risks identified

The Project Board should consider what risks, if any, should be escalated to the **service risk register**. The criterion for escalation is:

- Higher scoring risks (12 and above) that need agreement on appropriate action to be taken to mitigate the risk
- Lower scoring risks that are likely to be common across a number of projects, which should require attention by the Project Board and are likely to be dependencies for other projects
- Any risks that affect the overall objectives of the project (subjective)

9. Annual review and quality assurance

To ensure the risk management framework remains fit for purpose, the organisation should undertake an annual review and refresh, where relevant. This should consider industry best practice; ongoing business management needs; and pick up on any recommendations arising from internal audits. Any changes should be approved by the Strategic Commissioning Board and Performance and Contract Management Committee.

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 the level of risk the organisation is exposed to. Internal audit should test both the design of the controls and effectiveness of these controls. Reports should be issued to management that note, where appropriate, action required if there are any deficiencies noted within the internal control environment. It is management that should be 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 should base their plan on the key risks of the organisation and this independent source of assurance should be noted within the risk registers where relevant.

Annual Governance Statement

The organisation should produce an Annual Governance Statement every year, which assesses the governance system in place and the sources of assurance obtained during the year, internal and external. The risk management framework should provide assurance to the Strategic Commissioning Board and members that risks are being properly managed.

Periodic review of risk owners

A periodic review of risk owners (to check they are still employed by the organisation) should be undertaken by the Performance and Risk Team, as part of the annual review of the risk management framework.

Appendix A - Roles and responsibilities

All officers, senior managers, members and partners should proactively engage with risk management and the potential impact of risks on achieving objectives. It should be everyone's job to identify risks and report them to their manager. Managers at all levels should be responsible for the collation and management of risks within their service area, using the relevant risk register template.

Within the organisation, officers and groups have responsibility for different aspects of the risk management framework. Some of these are defined by the Terms of Reference set out in the Constitution (identified in *italics* below).

Officer	Roles and responsibilities
Chief Executive	• Oversee delivery of the risk management framework • Review progress of the management of strategic risks in the strategic risk register • Ensure consideration of risk in agreeing the organisation's direction of travel
Commissioning Directors	• Manage strategic risks associated with their specific areas of responsibility, including any that cross business, service or directorate boundaries • Escalate risks, as appropriate, for consideration by the Strategic Commissioning Board • Undertake an annual risk review and refresh as part of the business and budget planning cycle, ensuring that any new risks that could impact on the achievement of objectives are captured and old risks are removed • As required, as a part of their delegated authority, manage the risks associated with their budget allocation and business plan • Seek assurance that a risk aware culture is appropriately embedded in their directorate • Ensure arrangements are in place for partnership and contract activities where risks are shared, so that risks are identified; joint risk registers are in place; and risks are managed and regularly monitored
Delivery Unit Directors	• Manage operational risks associated with their specific areas of responsibility • Appoint a risk champion to drive forward the risk management framework within their function • Escalate risks, as appropriate, for consideration by the Strategic Commissioning Board • Undertake an annual risk review and refresh as part of the business and budget planning cycle, ensuring that any new risks that could impact on the achievement of objectives are captured and old risks are removed • As required, as a part of their delegated authority, manage the risks associated with their budget allocation and business plan • Seek assurance that a risk aware culture is appropriately embedded in their directorate • Ensure a risk register is in place for projects and review these at least monthly • Ensure officers have an appropriate understanding of risk management and encourage them to identify risks for inclusion on the risk register

Officer	Roles and responsibilities
Commissioning Group Senior Responsible Officers (SROs)	• Manage retained and joint risks in the service area they commission, in accordance with the risk management framework • Ensure officers working within external or shared service have an appropriate understanding of risk management • Champion the benefits of risk management across their service area and communicate the organisation's approach to managing risk
Performance and Risk Manager (Performance and Risk Team)	• Implement the organisation's performance and risk management frameworks and build performance and risk management capability across the organisation • Provide assurance that the strategic objectives are being delivered through effective performance and risk management arrangements • Advise senior managers on performance and risk management arrangements and provide support to the Head of Performance and Risk in annually reviewing the performance and risk management frameworks • Responsible for corporate monitoring and challenge of performance and risk data, including the co-production and monitoring of improvement plans where necessary
Performance Monitoring Manager (Commercial Team)	• Support the management of joint risks with external service providers • Ensure joint risks are reviewed and risk registers updated on a quarterly basis • Escalate risks, as appropriate, for consideration by the Strategic Commissioning Board • Undertake an annual risk review and refresh as part of the business and budget planning cycle, ensuring that any new risks that could impact on the achievement of objectives are captured and old risks are removed
Risk Owner	• Accountable for ensuring that individual risks are managed appropriately and the impact should the risk event occur • The senior officer for the area of work that the risk relates to • Management of the risk may be delegated to a risk manager(s) (if delegated, accountability for the risk is retained by the risk owner) • Assess the risk and assign it a score for likelihood and impact
Risk Manager	• Manages the controls and/or mitigations in place • Supports the risk owner in monitoring and reporting risks (this function may be delegated by the risk owner to the risk manager but the risk owner retains accountability for the risk)
Risk Champions	• Advise officers within the Delivery Unit on the application of risk management framework, including risk identification; risk assessment; monitoring, reporting and escalation • Maintain their respective service risk register (by collating information on new and updated risks through discussions with risk owners • Attend SMT meetings to present updates on their risk register, and to challenge senior management on the information on risks and delivery of actions • Ensure risks are reviewed and risk registers are up-to-date ahead of quarterly reporting (in accordance with timetable provided by Performance and Risk Team)
Project Managers	• Identify project risks • Support the management of project risks • Ensure project risks are reviewed and risk registers updated on a regular basis • Report project risks to the relevant Board on an exception basis • Escalate risks, as appropriate, to the appropriate Delivery Unit

Officer	Roles and responsibilities
All Officers	• Identify new risks to the appropriate risk champion and/or manager • Escalate any risks that are not being sufficiently managed to the appropriate risk champion

Group	Roles and responsibilities
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 through an annual Internal Audit review which underpins the Annual Internal Audit Opinion and Annual Governance Statement.*
Performance and Contract Management Committee	*Specific responsibilities for risk management. The Committee is responsible for:* • Approving the risk management framework and ensuring it is aligned to council policy • Overseeing and challenging the effectiveness of the organisation's approach to risk management • Ensuring action taken to manage strategic risks/ opportunities is adequate and effective
Strategic Commissioning Board	• Accountable for ensuring risks are managed effectively across the organisation and for maintaining a robust risk management framework, ensuring it is effective and embedded in the business • Determine the risk appetite and prioritise strategic risks/ opportunities • Establish a control environment and culture where risk can be effectively assessed and managed • Review the strategic risk register and escalated risks from Delivery Units on a quarterly basis, along with any associated risk reports • Ensure risk is appropriately considered in all key decisions submitted to the Board for approval • Review the quarterly performance monitoring report, including high-level service risks escalated to the corporate risk register
Delivery Unit Board	• Focus on the collective delivery of outcomes across the organisation's major internal and external delivery partners • Provide scrutiny, oversight and challenge to the activities of the Delivery Units to ensure that outcomes are achieved in a collaborative manner • Ensure risks are managed effectively across the organisation and that a risk aware culture is appropriately embedded • Ensure risk is appropriately considered in all key decisions submitted to the Board for approval • Review the quarterly performance monitoring report, including high-level service risks escalated to the corporate risk register
Project Board	• Review project risks • Ensure appropriate controls and/or mitigations in place for managing project risks • Escalate project risks to the relevant Project Board, as appropriate

Group	Roles and responsibilities
Internal Audit	• Deliver the annual audit plan, reviewing controls within the organisation using a risk-based approach. For each review a report should be issued giving a level of assurance and/or making any recommendations for improvement • Present reports in summary format to Audit Committee on an exception basis for those reports issued with limited or no assurance • Review the adequacy of risk management arrangements on an annual basis • Issue an annual opinion on internal controls for inclusion within the Annual Internal Audit Opinion.
Risk Network	• Internal forum for risk champions, co-ordinated by the Performance and Risk Team • Advice on risk management approach and process for monitoring and reporting risks, including escalation/de-escalation • Ensure risks are reviewed and risk registers are up-to-date ahead of quarterly reporting • Provide guidance on best practice risk management • Provide a forum for discussion and challenge on risk scoring, ensuring consistency across the organisation • Support the annual risk review and refresh of the risk management framework

Appendix B – Risk assessment criteria

The criterion below is used for measuring the likelihood of a risk occurring within the next five years.

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Percentage	≤10%	11-25%	26-50%	51-90%	>90%
Frequency *(How often might it happen)*	This will probably never happen/recur in the next 5 years	Do not expect it to happen or recur but it is possible it may do so in the next 5 years	Might happen or recur occasionally in the next 5 years	Will probably happen/recur in the next 5 years but it is not a persisting issue	Will undoubtedly happen/recur, in the next 5 years, possibly frequently

The criterion below is used for measuring the impact of a risk, should it occur within the next five years. Some risks will impact on more than one area; where this is the case the most predominant impact e.g. finance should be used to assess the 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
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 delivery unit / council's net budget (approx.. £300k - £750k) Risk of claims less than £20k	Loss of 0.25-0.5 per cent of delivery unit / council's net budget (approx.. £750k - £1.5m) Risk of claims between £20k -	Uncertain delivery of key objectives/ saving plan contributing to a loss of 0.5 – 1.0 percent of delivery unit / council's net budget	Non delivery of key objective/ saving plan contributing to a loss of >1 percent of delivery unit / council's net budget

Impact score	1	2	3	4	5
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
			£150k.	(approx. £1.5m - £3m) Risk of claims between £150k to £1m	(approx.. £3m) Loss of major contract (s) Risk of claim > £1m
Health & Safety	No or minimal financial loss (including risk of claim) <1k	Loss of 0.1-0.25 per cent of delivery unit / council's net budget (approx.. £300k - £750k) Risk of claims less than £20k	Loss of 0.25-0.5 per cent of delivery unit / 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 delivery unit / 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 delivery unit / council's net budget (approx.. £3m) Loss of major contract (s) Risk of claim > £1m
Information Governance	No personal data involved, or personal data (not HR personal data) between delivery units and partners on Barnet network	Short-term, minimal embarrassment to an individual Involves HR personal data between delivery units and partners on Barnet network about an individual Minimal amounts of sensitive personal data about an individual Minimal amounts of sensitive and personal data released to a trusted partner outside the Barnet network (a trusted partner is a partner with ISAs in place and /or within the PSN network) Personal data (non-sensitive) released outside the Barnet	*More than a minimal amount of sensitive personal data is involved at this level* Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) The potential of a financial loss for individuals concerned HR personal data between DUs etc. about a number of individuals (e.g. a team or directorate) Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns N.B. Inform Communications Team and inform the ICO	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns N.B. Inform Communications Team and inform the ICO

Impact score	1	2	3	4	5
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
		network to a small group of individuals (e.g. a family) Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service) N.B. Minimal amounts of sensitive personal data about an individual includes: a document which only references ethnicity would be minor; a document with the equalities assessment naming an individual would be more than a small amount	information is lost, requiring resubmission of identity evidence before services N.B. Short-term safeguarding concerns with mitigations that can be implemented swiftly to contain. Potential of informing the ICO		
Staffing & Culture	Short-term low staffing level that temporarily reduces service quality (<1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/service due to the lack of staff Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/ service due to lack of staff Unsafe staffing level of competence Loss of key staff Very low staff morale No staff attending training	Non-delivery of key objective/ service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending training on an ongoing basis

Appendix C – Quarterly reporting timetable

Quarter 2 2016/17

Strategic Commissioning Board	
11 October 2016	Review Quarter 2 2016/17 Corporate Risk Register
25 October 2016	Quarter 2 Performance Monitoring Report 2016/17
Delivery Unit Board	
26 October 2016	Quarter 2 Performance Monitoring Report 2016/17
Performance and Contract Management Committee	
15 November 2016	Quarter 2 Performance Monitoring Report 2016/17

Quarter 3 2016/17

Strategic Commissioning Board	
17 January 2017	Review Quarter 3 2016/17 Corporate Risk Register
31 January 2017	Quarter 3 Performance Monitoring Report 2016/17
Delivery Unit Board	
25 January 2017	Quarter 3 Performance Monitoring Report 2016/17
Performance and Contract Management Committee	
13 February 2017	Quarter 3 Performance Monitoring Report 2016/17

Quarter 4/Annual 2016/17

Strategic Commissioning Board	
11 April 2017	Review Quarter 4 2016/17 Corporate Risk Register
TBC April 2017	Quarter 4/Annual Performance Monitoring Report 2016/17
Delivery Unit Board	
26 April 2017	Quarter 4/Annual Performance Monitoring Report 2016/17
Performance and Contract Management Committee	
24 May 201	Quarter 4/Annual Performance Monitoring Report 2016/17