hammersmith & fulham

THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA

City of Westminster

London Borough of Hammersmith and Fulham | The Royal Borough of Kensington and Chelsea | Westminster City Council

RISK MANAGEMENT GUIDANCE 2013 - 2016

GUIDANCE FOR MANAGING OPPORTUNITY AND RISK

Good risk management is informed decision making. Managing risk is something the three councils do all the time, instinctively. In managing the complex business of the Council, it is important that Shared Services think about risk consciously and manages it in a planned and effective way, so as to assist in the delivery of the services aims and objectives and thereby adding to Customer value.

Risk management is intrinsically important to the three councils, how they are governed and how they carry out their activities. The Shared Services Risk Management Strategy Statement, Policy and this guidance together explain how Shared Services plan to manage risk and to make sure that they use risk in a balanced and proportionate way to recognise threats and opportunities. If we know what risks we face, and manage them properly, we can carry on delivering excellent services to the people who live, work and visit the three Boroughs, and grasp the new opportunities that we see for improvement.

The purpose of this Guidance is therefore to provide services with a practical step-by-step guide to identifying and evaluating threats and opportunities and to putting in place cost-effective and proportionate management controls to reduce risk to an acceptable level. I hope you find it helpful.

for London Borough of Hammersmith & Fulham
for The Royal Borough of Hammersmith & Fulham
for The City of Westminster

September 2013

Contents

Contacts

London Borough of Hammersmith & Fulham — Michael Sloniowski, Risk Manager
The Royal Borough of Kensington and Chelsea
Westminster City Council

Amendments

Document review	Inclusion of Information Management	October 2014
Document review	Inclusion of Pension Fund Risk Management	December 2014
Document review	Inclusion of Assurance	March 2015

1. INTRODUCTION

1.1 This Risk Management Guidance, together with the Risk Management Strategy Statement form part of each Council's sovereign corporate governance arrangements. The aim of this guidance is to provide a practical step-by-step guide on how to identify and manage Shared Services business threats and to ensure we make the right use of opportunities. It also identifies who is responsible for specific elements of the risk management process.

The Shared Services Risk Management Strategy Statement

1.2 The Strategy Statement has been agreed by the Chief Executives of Hammersmith and Fulham, The Royal Borough of Kensington and Chelsea and Westminster City Councils. The Statement defines how risk management is applied across Shared Services and;

- outlines key aspects of what is Shared Services risk management;
- describes the Shared Services risk management objectives to measuring and managing risk;
- describes the way to Identify and record Shared Services Strategic, Change and Operational risks

Risk Management Definitions

1.3 A risk consists of the combination of the likelihood of a perceived threat or opportunity occurring and the magnitude of its impact on Shared Services objectives

1.4 Risk Management is the approach to the identification, evaluation and financial management of the risks associated with its activities.

A Standard Framework for Shared Services Risk Management

1.5 A harmonised risk management standard has been introduced to help departments and services relate to the risk management process in a clearer and simpler way. Using the standard will help you to;

- identify risks and help you to prepare improvements and innovate;
- reduce bureaucracy through the use of a single process applicable across the three councils;
- bring consistency in understanding what risks services face;
- eliminate issues from the risk & assurance registers and add value back into the business
- benchmark risks across Shared Services and departments highlighting common problems and possible solutions.

1.6 Risk Management is a process that is designed to help improve services by preparing for future events. It is a tool to help you make decisions about services and if done well can reduce the need to audit areas where risk is managed effectively.

1.7 Effective risk management requires a balance between the two extremes of being unaware of risks (thus exposing services to unnecessary loss and being ill-prepared for events that may take it by surprise) and being obsessed by risks (thus stifling innovation and possibly over investing in control measures that bring no added value).

1.8 Shared Services working recognises that this balance is not easy to achieve, but will strive to assist managers through training, guidance (such as this step by step guide to risk assessment) and regular monitoring and review of the risk management process.

2. ROLES AND RESPONSIBILITIES

Responsibility for Risk Management

2.1 It is the responsibility of all Members and employees across the three councils to have due regard for risk in performing their duties.

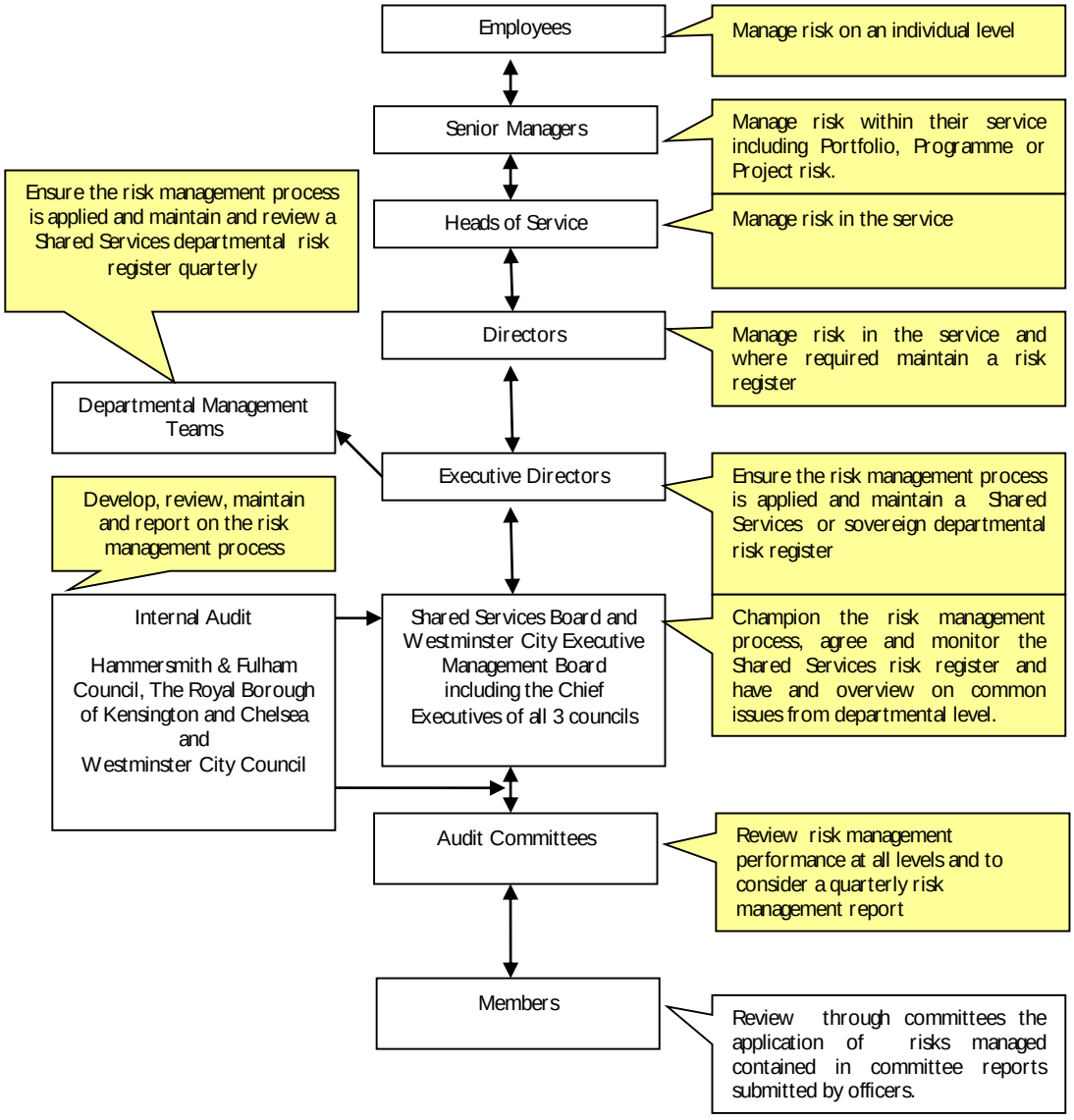
2.2 The three Councils remain individually responsible for ensuring that an effective Risk Management Strategy is in place, that it is subject to a formal review process and that there is a robust framework in place to identify, evaluate and control risks. This includes quarterly reports to Members, through an Audit Committee, on the risk profile.

2.3 The Shared Services Board for Hammersmith and Fulham and The Royal Borough of Kensington and Chelsea councils and the Westminster Strategic Executive Board (EMT) are jointly responsible for ensuring that pragmatic, robust and consistent arrangements are in place (in accordance with the approved strategy statement) for the effective management, monitoring and reporting of the Shared Services strategic, change and operational risks.

2.4 Executive Directors and their Management Teams are responsible for ensuring and maintain a robust framework to provide assurance on the identification monitoring, reporting and management of risks effectively in their business departments.

2.5 Service Managers remain responsible for the effective management of risk within their service area and to ensure that staff operating within their service adhere to the best practice principles of risk management.

2.6 Defining responsibilities for risk management is part of the Shared Services commitment to ensure that there is absolute clarity about what part an individual plays in the process. Risk management covers a vast area of each council's operations however in summary the chart below serves to identify the principal roles that officers and members fulfil.



3. RISK MANAGEMENT EXPLAINED – 'HOW'

This practical step by step guide to risk assessment follows the cycle depicted below and comprises the following steps. The process below can be used to measure the negative (threat) and positive (opportunity) sides of risk and is known as the 'balance of risk';

There are fundamentally six steps to the risk management process.

STEP 1: Objectives (Business, Service, Financial , Portfolio, Programme or Project Plans)

STEP 2: Identification (Identify risks or opportunities and owners)

STEP 3: Measurement (Assess inherent impact and likelihood and determine the 'Inherent risk score')

STEP 4: Analyse & Control (Identify and verify existing controls for suitability)

STEP 5: Mitigation and develop action plans (Assess residual impact and likelihood and determine the 'Residual risk score', plan forward actions if required)

STEP 6: Monitoring (Review the effectiveness of your controls)

STEP 1: Objectives

3.7 Risks need to be identified against service, change or operational objectives.

- Use your Business, Service, Financial , Portfolio, Programme or Project Plans as the starting point.
- Record all your findings on a Risk Register (Appendix 3 – Risk Register template)

3.8 The aim is to identify those activities and issues on which your service / activity / project is dependent. Identification of risks can be assisted by use of various headings or categories to help ensure a systematic and comprehensive approach is adopted.

STEP 2: Identification

3.9 Risks may be Strategic in nature i.e. risks which need to be taken into account in making judgements about aims and objectives (or an individual service or project) and which will often impact the entire or a significant portions of the Service or project. These risks are frequently generated and influenced by factors external to the Council / project, and by their nature, strategic risks are often best identified by those in the most senior positions whose role entails policy and strategic decision making.

3.10 Risks may be Change related and are part of the ways of transforming business through Portfolio, Programme and Project Management. This process can be equally applied to capture and manage time bound and project deliverable risk.

3.11 Alternatively the risks may be more Operational in nature. These are risks encountered by departmental managers or Services as part of their everyday business. They often impact on the availability of resources required to achieve corporate / service / project objectives; and identification of these risks is best performed by the departmental or service managers directly affected by such events.

Use PESTLE to identify and categorise risks (APPENDIX 1 Categories of risk)

3.12 Using Appendix 1 as a prompt to begin the identification of risk. Encourage team or group participation as experience of the business or service is invaluable in giving an insight into risk.

Use service plans, strategies, financial accounts, media mentions, regional or national news, inspectorate and audit reports to help you inform the process. Seek advice from other service professionals as they are a useful source of information.

3.13 Describe your risk in a language that articulates clearly what could go wrong or what opportunity could be achieved.

3.1 Risk to the Shared Services can take various forms, including:

- failure of delivery of services on which the public rely;
- risks in relation to partnerships and management of information;
- risk to the health, safety and welfare of staff and public;
- risk of loss, abuse or inefficient use of public funds;
- risk to the value and character of public property;
- risk to reputation and public confidence;
- risk to the quality and sustainability of the environment, and
- risk to the economic well-being of the three Councils.

3.14 Having identified the underlying cause, we must then allocate a risk owner – this is the person best placed to organise effective action to mitigate the risk.

STEP 3: Measurement

A risk score is essential to measure and prioritise your risk. All risks are measured using scoring. Shared Services utilises a likelihood and impact scoring system of 5 x 5 to achieve a combined score known as the exposure. (APPENDIX 2 Scoring).

LIKELIHOOD X IMPACT = EXPOSURE

First measure the risk as it stands, likelihood and impact, with no controls. This is known as the inherent risk.

Then measure the risk once you have identified the controls currently in place. This is known as the residual risk.

Not all risks can be managed, but those that can are managed using a variety of controls. The art of risk management is to apply controls that are effective and efficient in reducing the exposure.

STEP 4: Analyse & Control

3.15 Analyse the risk

3.16 This is the area where risk management can have the greatest benefit

3.17 The quality and range of controls directly influence the amount of risk the council and its services are exposed to. It is therefore necessary that once risks have been identified that the controls in place are assessed to determine if they are effective. Where controls are identified these should be set against the risk and measured for their effectiveness. Doing this gives the service and the three councils assurance that the business process is robust and less likely to fail.

STEP 5: Mitigation, communication and developing action plans

3.18 Having assessed the 'Inherent Risk Score', the next step is to identify those existing control measures in place intended to avoid, reduce or mitigate each risk identified. The control should either reduce the likelihood that a risk will occur or the impact were it to occur.

3.19 Risk can be divided into five response categories:

3.20 Tolerate: Ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the most appropriate response may be toleration.

3.21 Treat: By far the greater number of risks will belong to this category. The purpose of treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level. The actions that the Council takes in treating risk are called 'controls' which are designed to contain risk to levels considered acceptable to the Council.

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

3.23 Terminate: Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in local government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved.

3.24 Take the Opportunity: after an exercise that measures the risk and reward a decision may be made to proceed with an initiative or project that brings benefit to the organisation, community or the environment.

3.25 In line with good practice, you should communicate risks to other services areas where these may be affected. Where risks become red (significant) you should make sure they are escalated upto an appropriate level for decision or further action.

3.26 Action plans should include:

- What action is required to reduce / increase the 'Residual Risk Score' to a level considered acceptable to the Council.
- By who.
- By when.

3.27 Where these key actions are significant, they should be incorporated into the annual budget, business planning and performance monitoring processes.

3.28 Other less significant actions should be included within service level or project management plans and monitored in compliance with the Strategy.

STEP 6: Monitoring and Review

3.29 The key output of the risk assessment process is the Risk Register. A Risk Register is maintained and is updated as and when new and emerging risks are identified. The Risk Register should be monitored periodically, doing so brings benefits to the service, and not just to demonstrate compliance to the Strategy.

Don't fall into an endless cycle of risk identification

Risks are supported by a Risk Action Plan which contains:

- The risk owners' assertions on how each risk is managed.
- The risk owners' assessment of residual impact and likelihood.
- Action plans to reduce / increase residual risk.

Record all your findings on a Risk Register (Appendix 3 – Risk Register Template)

Cycle of reporting

3.30 All departments are expected to provide a quarterly update of their departmental risk register, or other register on request, for the purpose of informing the Shared Services Director of Audit, Risk Manager, Strategic Business Analyst (WCC) for the governance and reporting of risk management at Member and Executive Director level.

Timetable for review and update of your risk register.

1st Quarter – July end
2nd Quarter – October end
3rd Quarter – January end
4th Quarter – April end

4 INFORMATION RISK MANAGEMENT

4.7 'Information risk', is often not as visible as it should be, and therefore not always as well managed. The pace of technological change in the information age means new risks can appear quickly, and may not be as visible to Boards as other risks. Senior staff may wrongly assume information risks (unlike financial risks or physical threats) are secondary, and of less strategic importance. The guardianship and management of information in all its aspects (integrity, availability and confidentiality) is crucial to public service delivery.

4.8 The purpose of this section is to highlight specific issues related to the management of 'information risk'. Understanding the nature of the risks to your business from failure to manage or use information is critical.The risks of managing information may not be understood as well as other risks by Boards and Officers.Yet, in many cases, they pose just as large a risk to councils as many of the more traditional risks.

4.9 However, Boards and Officers are not being asked to treat 'information risk' separately. Instead, you are asked to manage information risk within your standard business risk framework, and assess information risks alongside all other risks.

What are 'information risks"?

Risk category	Example of risk
Governance and culture	Lack of comprehensive oversight and control (so anything can go wrong) When something goes wrong, handling it badly and not learning (so it can happen again), third parties let you down (letting down your customers and your reputation suffers). New business processes don't take information risk into account (with serious consequences).
Information management	Critical information is wrongly destroyed,not kept or can't be found when needed (leading to reputational damage or large costs). Lack of basic records management disciplines (can have wide-ranging consequences).
Information Integrity	Inaccurate information (which causes the wrong decision to be made, or the wrong action to be taken), Vital electronic information becomes unreadable due to technical obsolescence (with legal, reputational or financial consequences). Critical information is lost (with legal, reputational or financial consequences).
The human dimension	Despite having procedures and rules, staff, acting in error, do the wrong thing (and things go badly wrong). Despite having procedures and rules, 'insiders', acting deliberately, do the wrong thing (and things go badly wrong) External parties get your information illegally (and expose it/act maliciously/defraud you or your customers).
Information availability	Inappropriate disclosure of sensitive personal information (causing reputational

and use	damage or worse). Failure to disclose critical information for case management/protection (at worst leading to loss of life). Failure to utilise the value of the information asset (leading to a waste of public money). Failure to allow information to get to the right people at the right times (leading your service to fail your customers).

4.10 Where can information risks be identified?

- Risks identified through any new information systems introduced;
- Risks identified through formal projects, programmes or a portfolio;
- Outcomes of data audits;
- Risks identified and discussed at the Technical Design Stage;
- Issues highlighted through the weekly ICT Board;
- Issues raised at the Data Security Working Groups;
- Issues raised in data protection and security training sessions;
- ICT Incident management (eg breaches and security incidents – tasks)
- Any other issues identied by the Information Management team.

4.11 Specific risk assessment tools for data protection obligations.

4.12 Privacy impact assessments (PIAs) are a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow services to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

4.13 The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Key points:

4.14 A PIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies. Conducting a PIA involves working with people across Triborough, with partner organisations and with the people affected to identify and reduce privacy risks. The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly. Conducting a PIA provides benefits by producing better policies and systems and improving the relationship with individuals.

4.15 Privacy impact assessment is a process which helps to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA is used to systematically and thoroughly analyse how a particular project or system will affect the privacy of the

individuals involved.

4.16 When to use it:

4.17 The Information Commissioners Office uses the term project in a broad and flexible way – it means any plan or proposal in an organisation, and does not need to meet an organisation's formal or technical definition of a project, for example set out in a project management methodology.

4.18 PIAs are to be applied to new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when a service is planning changes to an existing system. A PIA can also be used to review an existing system, but the service needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system.

4.19 What are the risks?

4.20 There can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the service carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy. Each service will be best placed to determine how it considers the issue of privacy risks. The steps in this code can be applied to a wide range of business processes. The Councils have designed their PIA methodology to be as flexible as possible so that it can be integrated with existing ways of working.

4.21 Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

4.22 Where can it be applied?

4.23 A PIA is suitable for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where it is necessary to pool or link sets of personal data, for example in Public Health and Social Care.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of the council(s).
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

4.24 Where can I find a PIA template?
4.25 A PIA is available for download from the Information Governance page on TriBnet.

http://tribnet/About%20Tri-borough/informationgovernance/Pages/141113%20-%20Tri-borough%20Privacy%20Impact%20Assessment%20Template%20-%20final.docx

4.26 Where can I get assistance with more detail on Information risk management?
4.27 For expert advice contact the Information Management team.

5 Pension Fund Risk Management

5.7 Risk management should be considered in relation to all aspects of Local Government Pension Scheme (LGPS) management. The importance of understanding risk applies as much to the administration of the benefits as it does to the investment of funds.

5.8 The overarching risk for an LGPS fund is the possibility of not having sufficient funds to pay members' pensions. As a funded scheme, investment of funds brings a multitude of risks that need to be addressed, from ensuring that the investment strategy reflects the latest understanding of the funds liability profile, to the risk of individual stock selection in actively managed funds and the possibility of capital loss on a stock.

5.9 Administration of benefits, with the payrolls involved has its own risks. Plus, as the scheme is regulated by statute, there is always the risk of not being legally compliant. Understanding risk and how it can be mitigated requires a knowledge of all aspects of the LGPS and how an individual fund operates.

5.10 Who is involved?

5.11 Risk management is an issue for all those involved in the management of an LGPS fund. This includes the members of the pensions committee, the officers managing the LGPS fund and the fund administrator. It does not stop there, the importance of the fund having appropriate risk management is also an issue for all members of the administering authority, even though management of the fund will be a delegated function, all employers within the fund need to seek reassurance.

5.12 Responsibilities for Pension Scheme risk.

5.13 Responsibility for risk is an issue for all those involved in the managment of the LGPS. Looking at the role of the pension committee member, this includes:

- ensuring the risk strategy and risk register are kept up-to-date;
- ensuring that the fund investment strategy and the management of investments adequately examines all the risks and how these can be mitigated;
- being aware of the risks involved in custody arrangements and how they are being managed;

- taking a strategic view of the level of risk involved in actuarial valuations, the key assumptions and the suitability for employers in the fund, including the reasonableness, for example, of investment, interest rate and mortality forecasts;
- ensuring that appropriate policies are in place to deal with the admission of employers into the fund and the departure of employers;
- examining and seeking assurance that all risks around the administration of the fund are being adequately managed;
- ensuring that the risks relating to individual employers are identified and managed;
- being aware of reputational risks and regulatory and compliance risks and the action taken to manage these risks.

6 Assurance.

6.7 Assurance and Good Risk Management.

6.8 Good risk management relies on a system of current and planned controls and we rely on those controls to manage and reduce our risks. We need to be sure that current controls are in place and that planned controls are being implemented as planned; in other words, we need assurance on those actions.

6.9 Against every control (or group of common controls) and every planned action (or group of common actions) there should be the source of assurance, ideally positive, that will demonstrate to those charged with accountability (risk steering group, audit committee, senior management, board, etc) that the control is in place and working as it should or that implementation is going to plan and delivering as expected.

7 Annual Governance Statement

7.7 The purpose of the statement is to enable the Council to meet its requirements of the Accounts & Audit (England) Regulations 2015, which requires that the Council prepares an annual governance statement.

7.8 Directors Assurance

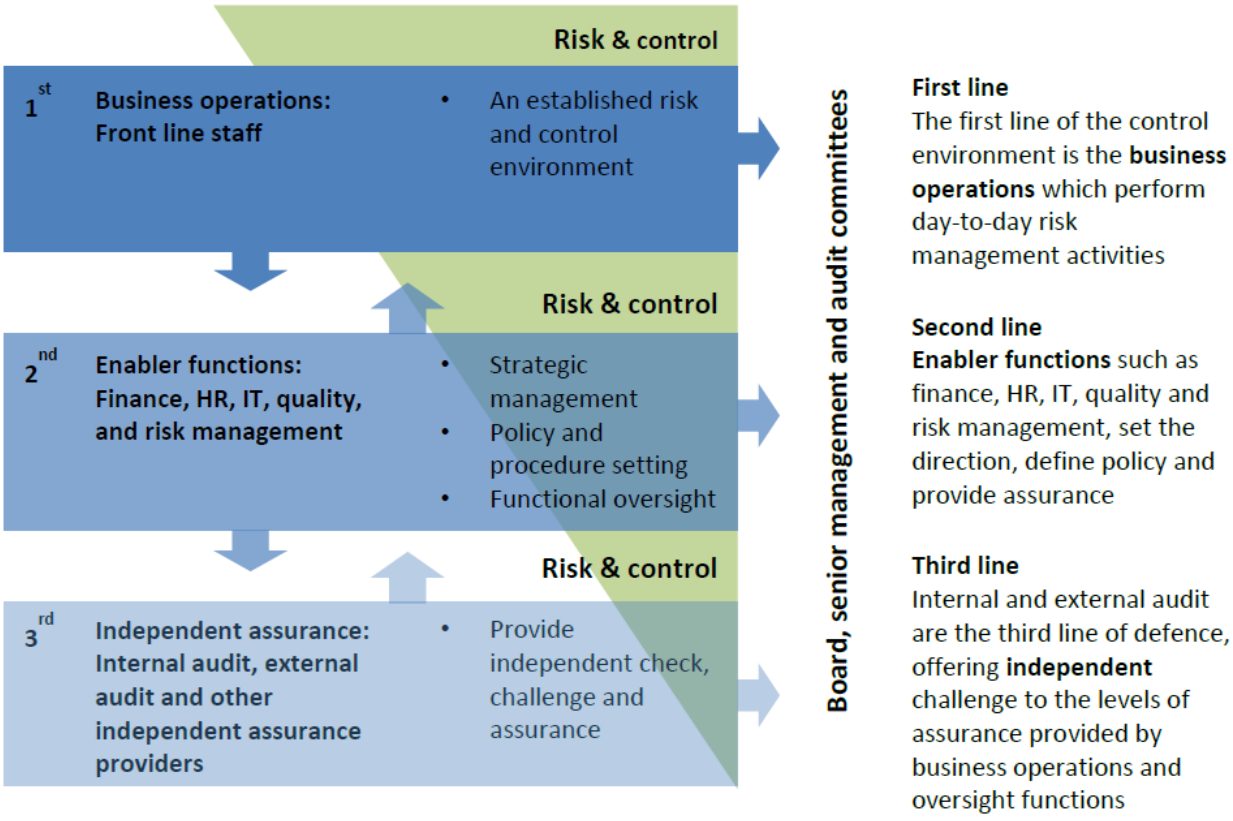
7.9 To support this process, each year Tri-,Bi and Sovereign departments are required to provide evidence that its objectives and principal statutory obligations are known and that the risks in meeting these requirements are being effectively, economically, and efficiently being managed. This process results in a Departmental Management Assurance Statement that is signed by the Executive Director confirming that this assessment has been undertaken and reporting its results. This is done for Tri, Bi and sovereign Departments and is based on Directors own Management Assurance declarations. The Statement is required to be completed and signed by the Executive Director for the current year as part of this exercise. At 31st March the Executive Director will be asked to provide the statement with any changes needing to be reported for the Annual Governance Statement.

7.10 Sources of assurance

7.11 A useful model to consider sources of assurance is the Three Lines of Defence Model as below. This model is also known as the four or five lines of defence, if external audit and any other independent assurance providers are separated out from the third line.

7.12 Although this model is commonly referred to as providing defence, it does so by implementing controls and providing assurance and could just as easily be known as the three lines of assurance or control. The model is often the starting point for an assurance map (see Risk-based Assurance Mapping), and can be used by internal auditors to identify areas to audit.

Three lines of Defence Model



8 Risk-based Assurance Mapping

8.7 An assurance map identifies all the different sources of assurance against each process or activity, allocates it to one of the three lines of defence and assesses whether it is good, bad or indifferent. It will then highlight both areas where more assurance is needed and areas which are over assured and where resources could be released.

8.8 Internal audit will typically use such a document to identify areas that do and do not need further audit activity, while senior managers and non-executive directors/members could use such a map as a significant source of the assurance that they need that operations are proceeding as anticipated. Assurance maps can be adapted to use for risks by listing the controls against each risk instead of the process or activity and proceeding in the same way.

Typical types of assurance provided at each level are shown below.

Typical Types of Assurance		
	Positive	**Negative**
1st line	Minutes of meetings (Management Team, Team meetings, Project or Programme Board, Gateway reviews, Scrutiny reviews) Checklists Reports Reconciliations (manual) Performance indicators Verbal assurance from staff (1-2-1's, appraisals, feedback from staff).	No complaints No errors identified No known problems
2nd line	Exception reports Audit tools in IT systems Reconciliations (automated) Separation of duties arrangements Results of checks built into systems	No complaints No errors identified No known problems
3rd line	Audit reports (Internal) Inspection reports eg OFSTED, CSCI Consultancy reviews Assurance from auditors (External)	

APPENDIX 1 Categories of risks (Strategic, Change, Operational)

The following categories of risk are neither prescriptive nor exhaustive, but provide a framework for identifying and categorising a broad range of risks the TriBorough services could face.

Strategic Risks (Service/Business Planning, Policy)		
Those risks relating to the achievement of the corporate objectives and service plans		
Risk	**Risk Definition**	**Examples**
Political & Policy	Delivery of central/local policy or commitments	• Decisions based on incomplete/incorrect information • Too slow to modernise/ innovate • Community planning oversights/errors
Economic/Financial	Ability to meet the Council's financial commitments	• UK/regional economic problems • Missed business or service opportunities • Unreliable accounting records • Misuse of resources or fraud • Cost of capital • Financial impact of uncontrollable legislative or other policy changes
Social	Ability to deliver objectives due to social factors	• Demographic change • Crime and disorder
Technological	Ability to optimise benefit from or capacity to cope with pace or scale of technology	• Obsolescence • Inappropriate IT strategy • Inability to implement change

	change	• Major IT or project failure
Legislative/Regulatory	Ability to manage current or potential changes in UK and/or EEC law/regulation	• Breaches • Inadequate response to legislative changes
Environmental	Risks relating to environmental consequences of pursuing strategic objectives. Lack of innovation in favour of tradition may squander opportunities to reduce waste and pollution	• Noise, contamination, pollution • Impact of planning and transport policies • Failure to buy low polluting vehicles in procurement • Failure to achieve best energy efficiency in new buildings
Competitive	Risks affecting cost, quality and/or ability to deliver best value	• Failed bids for government funds • Failure to demonstrate best value • Weak market supply
Customer/Client	Ability to meet current/changing customer needs and expectations	• Lack of consultation • Image
Partnership	Ability to work successfully with another independent organisation to achieve common ambitions	• Divergent underlying goals • Cultural differences prevent effective communications • Levels of partner commitment

Change Risks (Portfolio, Programme, Project)		
Those risks relating to Portfolio, Programme or Project Management		
Risk	**Impact**	**Examples**
People - Professional/Management	Risks associated with nature of each profession	• Poor management processes • Poor service provision
Legal	Risks related to decision-making, possible breaches of legislation and compliance with case law	• Breaches • Exposure to liability claims
Financial/Budgeting	Risks associated with financial planning and control and adequacy of internal funds	• Missed funding opportunities • Inadequate financial control • Fraud and error
Property/Physical Assets	Risks related to fire, security and health and safety (buildings, vehicles etc.)	• Loss of assets • Damage to assets • Non-compliance with Health and Safety legislation
Third party Suppliers	Risks associated with failure of partner organisation to	• Over-reliance on key suppliers • Quality issues

	meet contractual obligations	• Failure of contractors to deliver services
Partnership	Risks arising from the need to act collaboratively with another independent organisation.	• Budget, staffing or reorganisation issues affect the commitment of one of the partners. • Incompatible management or IT systems frustrate successful collaboration
Reputation	Risks relating to the Council's reputation	• Loss of image Serious mistakes taken up by the press/media
Technological	Risks relating to reliance on IT equipment and/or machinery	• IT security breach • Lack of adequate Disaster Recovery arrangements
Information	Risks relating to loss /corruption of records	• IT system failure • Accidental or deliberate destruction • Erroneous or malicious modification
Environmental	Risks relating to pollution, noise or energy efficiency of service operation	• Noise, contamination, pollution • Inefficient use of energy and/or water

Operational Risks (Business as usual, day to day risks)		
Those risks relating to the day-to-day operation of a service or support function		
Risk	**Impact**	**Examples**
People - Professional/Management	Risks associated with nature of each profession	• Poor management processes • Poor service provision
Legal	Risks related to decision-making, possible breaches of legislation and compliance with case law	• Breaches • Exposure to liability claims
Financial/Budgeting	Risks associated with financial planning and control and adequacy of internal funds	• Missed funding opportunities • Inadequate financial control • Fraud and error
Property/Physical Assets	Risks related to fire, security and health and safety (buildings, vehicles etc.)	• Loss of assets • Damage to assets • Non-compliance with Health and Safety legislation
Third party Suppliers	Risks associated with failure of partner organisation to meet	• Over-reliance on key suppliers • Quality issues • Failure of contractors to deliver

	contractual obligations	services
Partnership	Risks arising from the need to act collaboratively with another independent organisation.	• Budget, staffing or reorganisation issues affect the commitment of one of the partners. • Incompatible management or IT systems frustrate successful collaboration
Reputation	Risks relating to the Council's reputation	• Loss of image • Serious mistakes taken up by the press/media
Technological	Risks relating to reliance on IT equipment and/or machinery	• IT security breach • Lack of adequate Disaster Recovery arrangements
Information	Risks relating to loss /corruption of records	• IT system failure • Accidental or deliberate destruction • Erroneous or malicious modification
Environmental	Risks relating to pollution, noise or energy efficiency of service operation	• Noise, contamination, pollution • Inefficient use of energy and/or water

APPENDIX 2 Consolidated Risk Impact/Magnitude Guide

Scoring (Impact)

Impact Description	Category	Description
1 Very Low	Cost/Budgetary Impact	£0 to £25,000
	Impact on life	Temporary disability or slight injury or illness less than 4 weeks (internal) or affecting 0-10 people (external)
	Environment	Minor short term damage to local area of work.
	Reputation	Decrease in perception of service internally only – no local media attention
	Service Delivery	Failure to meet individual operational target – Integrity of data is corrupt no significant effect
2 Low	Cost/Budgetary Impact	£25,001 to £100,000
	Impact on life	Temporary disability or slight injury or illness greater than 4 weeks recovery (internal) or greater than 10 people (external)
	Environment	Damage contained to immediate area of operation, road, area of park single building, short term harm to the

Impact Description	Category	Description
		immediate ecology or community
	Reputation	Localised decrease in perception within service area – limited local media attention, short term recovery
	Service Delivery	Failure to meet a series of operational targets – adverse local appraisals – Integrity of data is corrupt, negligible effect on indicator
3 Medium	Cost/Budgetary Impact	£100,001 to £400,000
	Impact on life	Permanent disability or injury or illness
	Environment	Damage contained to Ward or area inside the borough with medium term effect to immediate ecology or community
	Reputation	Decrease in perception of public standing at Local Level – media attention highlights failure and is front page news, short to medium term recovery
	Service Delivery	Failure to meet a critical target – impact on an individual performance indicator – adverse internal audit report prompting timed improvement/action plan - Integrity of data is corrupt, data falsely inflates or reduces outturn of indicator
4 High	Cost/Budgetary Impact	£400,001 to £800,000
	Impact on life	Individual Fatality
	Environment	Borough wide damage with medium or long term effect to local ecology or community
	Reputation	Decrease in perception of public standing at Regional level – regional media coverage, medium term recovery
	Service Delivery	Failure to meet a series of critical targets – impact on a number of performance indicators – adverse external audit report prompting immediate action - Integrity of data is corrupt, data falsely inflates or reduces outturn on a range of indicators
5 Very High	Cost/Budgetary Impact	£800,001 and over
	Impact on life	Mass Fatalities
	Environment	Major harm with long term effect to regional ecology or community
	Reputation	Decrease in perception of public standing nationally and at Central Government – national media coverage, long term recovery

Impact Description	Category	Description
	Service Delivery	Failure to meet a majority of local and national performance indicators – possibility of intervention/special measures – Integrity of data is corrupt over a long period, data falsely inflates or reduces outturn on a range of indicators

Scoring (Likelihood)

Descriptor	Likelihood Guide
1.Improbable, extremely unlikely	Virtually impossible to occur 0 to 5% chance of occurrence.
2.Remote possibility	Very unlikely to occur 6 to 20% chance of occurrence
3. Occasional	Likely to occur 21 to 50% chance of occurrence
4. Probable	More likely to occur than not 51% to 80% chance of occurrence
5. Likely	Almost certain to occur 81% to 100% chance of occurrence

APPENDIX 3 Risk Register template
24/07/20 13

XXXX Department, Tri,BiBorough Sovereign Risk and Assurance Register

				TYPE		Inherent risk			Residual risk							
Risk Number	Tri, BiBorough / RBKC / H&F/WCC	Key risks	Consequence	STRATEGIC/CHANGE (Portfolio, Programme, Project) or OPERATIONAL Risk (Business as Usual)	PESTLE cc	Impact	Likelihood	Total	Impact	Likelihood	Total	Risk Monitoring	Responsible Officer	Existing controls	Proposed action to remedy gaps in control	Date of implementation of additional control or date of next review of risk
		There is a risk that/of…														
1	RBKC	Event Management, People are put at risk and practice is inconsistent	Potential injury to a client, reputational harm	EXAMPLE Strategic	Customer /Citizen	4	5	**20**	3	3	**9**	**Keep under review**	Director of ...	Event Management Action Plan		SMT review - end of Q2 2013
2	H&F	There is a risk that the Service may not deliver the enhanced security to Parks and Open spaces	Failure to meet the needs and expectations of our customers and politicians	EXAMPLE Operational	Human resources	4	4	**16**	5	3	**15**	**Periodic monitoring advised**	Head of …	Recruitment and retention. Maintain reputation of borough. Good staff management. Supervision/training. Quality standards. • Service user satisfaction and outcomes for service users. • Meeting professional bodies' standards & practice government and service specification	Business Plan contains an objective 6 monthly review by ELRS Management Team	SMT review - end of Q2 2013
3	BiBorough	There is a risk that fraud may not be reduced in not moving to an automated cash collection system	Financial loss to ELRS budget	EXAMPLE Portfolio	Finance	4	5	**20**	5	5	**25**	**ADDITIONAL CONTROLS DESIRABLE**	Director of ...			SMT review - end of Q2 2013
4						4	4	**16**	4	4	**16**	**ADDITIONAL CONTROLS DESIRABLE**				
5						3	3	**9**	3	3	**9**	**Keep under review**				
6						2	2	**4**	2	2	**4**	**Keep under review**				
7						1	1	**1**	1	1	**1**	**Keep under review**				
8						1	1	**1**	1	1	**1**	**Keep under review**				
8						1	1	**1**	1	1	**1**	**Keep under review**				
9						1	1	**1**	1	1	**1**	**Keep under review**				
10						1	1	**1**	1	1	**1**	**Keep under review**				