APPENDIX 2

The London Borough of Hammersmith & Fulham

Risk Management Standard And Policy

2011 - 2014

Version 3 (2011 review)

INDEX

London Borough of Hammersmith & Fulham

Risk Management Standard

1. Introduction

The council has adopted a risk management standard to help departments relate to the risk management process in a clearer and simpler way. Using the standard will help you to;

- bring consistency in understanding what risks the council and services face.
- eliminate issues from the risk & assurance registers and slim down the process for departments.
- benchmark risks across services and departments highlighting common problems and possible solutions.
- identify risks and help you to prepare improvements.

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.

The approach that Hammersmith & Fulham in managing risk is summed up by the following risk management goal and objective.

Goal

Managing Risk Effectively

Objective

To demonstrate that risks are managed within a clearly defined structure that is beneficial to the organisation, the community, environment its stakeholders and partners.

Definition

The London Borough of Hammersmith & Fulham defines risk as:

‘the chance of something happening that would have an impact on the achievement of Hammersmith & Fulham’s Objectives’

Risk Management Policy 2011 - 2014

Hammersmith & Fulham Council provides a diverse range of services to the community and visitors to the area. In order to secure these services some amount of risk taking is inevitable. However the Council recognises that effective Risk Management will improve strategic, operational and financial management by helping to maximise opportunities, minimise losses and maximise resources for the services it provides.

It is the Policy of the Council to adopt a risk based process that has a series of well defined steps to support better decision making through understanding of risks, whether a positive opportunity or negative threat and their likely impact.

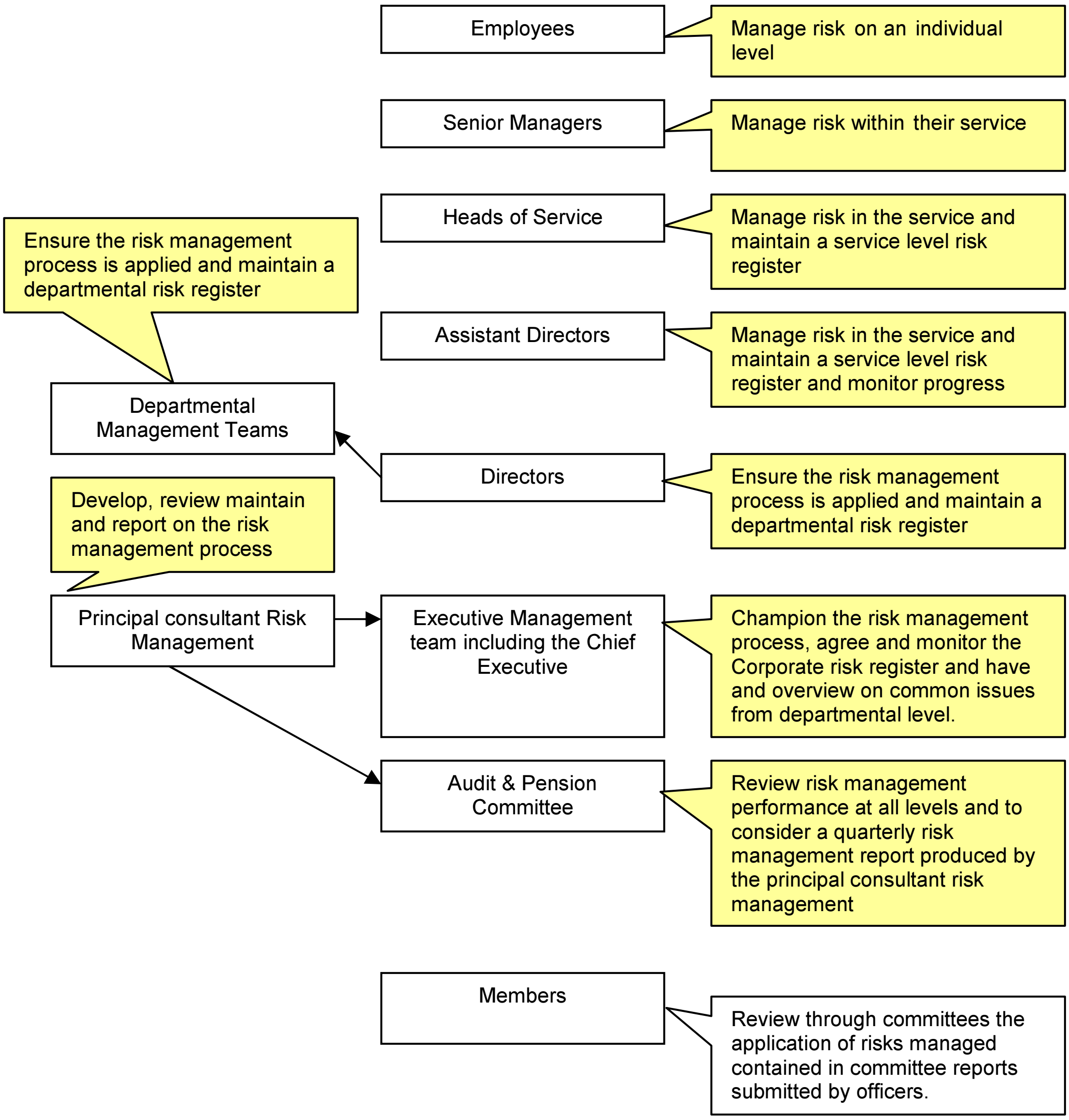
This Policy seeks to enforce the commitment shown by the Council and Executive Management Team to a risk managed culture by ensuring that every Member and employee has regard for the management of risks in order to:

- Achieve its Corporate Aims, Objectives and Values
- Ensure compliance with its statutory obligations
- Safeguard its employees, Members, service users and all other persons to whom the Council has a duty of care
- Protect its assets, including property, equipment, vehicles and other resources and reduce undesirable associated losses
- Improve performance and service delivery and provide resilient services
- Prudently manage the councils finances through effective Treasury Management and control of income and debtors
- Manage information securely through good data quality and information management protocols
- Minimise waste, fraud and poor value for money
- Support better project management
- Protect the reputation of the Council

This Policy statement has the support of the Council, which recognises that achievement of these identified risk management objectives will benefit the whole community.

2. Roles and responsibilities

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



The role of individuals

All individuals within the organization have a responsibility for contributing to the management of risk, uncertainty and opportunity. Embedding risk management within the organization involves incorporates risk management into each individual's job description, so that they;

• understand the risks that relate to their roles and their activities;
• understand how the management of risk relates to the success of the organization;
• understand their accountability for particular risks and how they can manage them
• understand how they can contribute to continuous improvement of risk management;
• understand that risk management is a key part of the organization's culture; and
• report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

The role of the risk owner

The risk management process is likely to identify a number of risks that need to be actively managed. These should be assigned a risk owner who is accountable for:

• owning the risk;
• overseeing the development and maintenance of an appropriate control environment;
• monitoring the risk where there is material change in its status; and
• reporting on the risk.

While the risk owner has overall accountability for the risk and its management, they might not own or operate the control(s) which relates to the risk. In this case, the role of the risk owner is to oversee that the control(s) is(are) owned, fit for purpose and operating effectively.

3. Risk Identification

The Council has taken the positive step of integrating the systematic identification and management of risks into its Service and Financial Planning process. This ensures that risk management is embedded into the Council's planning cycle and is an operational responsibility, not the exclusive domain of a specialist officer or division. It also recognises that the value of the Council is generated through service delivery and so the strategy for managing risks stems from that.

Directors and Heads of Service are required to identify the threats to achieving corporate or service objectives. Guidance on risk management is provided during the service and financial planning process. The Principal

Consultant, Risk Management is charged with providing active support and involvement in this process by;

- Providing advice to officers on risk management.
- Helping officers to understand what risk is and reinforcing the opportunities that risk management can present.
- Facilitating risk identification, assessment and mitigation.
- Ensuring that a consistent approach to risk management is applied, including a common understanding of terminology and definitions.
- Linking risk assessments carried out in other divisions and departments to help in identifying potential crosscutting risks.

4. Risk Classification

The tables below set out the main categories of risk the Council is likely to encounter. It provides the starting point for officers in the risk identification process.

Strategic Risks

Risks that need to be taken into account in judgements about the medium to long term goals and objectives of the council.

These include;

Political	Failure to deliver either local or central government policy or to meet local manifesto commitments.
Economic	Those affecting the ability of the council to meet its financial commitments. Investments and management of debt.
Social	Changes in demographic, residential or socio-economic trends.
Technological	Capacity or ability of the council to deal with the pace/scale of technological change including the consequences of internal technological failures.
Legislative	Current or potential changes in national or European law.
Environmental	Ecological consequences of progressing the council’s strategic objectives.
Competitive	Cost or quality issues in respect of the ability to deliver Best Value.
Customer/Citizen	Failure to meet the current and changing needs and expectations of customers and citizens.

This is known as PESTLEcc. and is an accepted method by which risk is classified.

Operational Risks

Risks that managers and staff will encounter in the daily course of their work.

These include;

Professional	Risks associated with the nature of the profession such as social work service concerns over children at risk, housing service concerns as to the welfare of tenants.
Financial	Those associated with financial planning and control.
Legal	Those related to possible breaches of legislation.
Physical	Fire, security, accident prevention and health & safety.
Contractual	Failure of contractors to deliver services or products at agreed cost and specification
Technological	Reliance on operational equipment, ITC systems or machinery
Environmental	Pollution, noise or energy efficiency of ongoing service operations

5. Risk Measurement

Risks are assessed on their impact and likelihood of occurrence.

All risks should be quantified by using a standard form of measurement. The use of a basic 5 by 5 calculation is the approved method. Where exposure to risk is measured based on the multiplication of likelihood and associated impact.

i.e. If a risk has a very high likelihood and a very high impact it will receive a combined rating of 25.

In order to help with risk measurement a standard consolidated form of look up tables has been designed to assist those tasked with risk assessment. These are expressed in the following set of tables;

Look up tables

Likelihood/Probability

Risk	Score	Probability
Very Low	1	Virtually impossible to occur 0 to 5% chance of occurrence.
Low	2	Very unlikely to occur 6 to 20% chance of occurrence
Medium	3	Likely to occur 21 to 50% chance of occurrence
High	4	More likely to occur than not 51% to 80% chance of occurrence
Very High	5	Almost certain to occur 81% to 100% chance of occurrence

Impact/Magnitude

Consolidated Risk Impact/Magnitude Guide

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,

Impact Description	Category	Description
		short term harm to the 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
	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

Impact Description	Category	Description
		falsely inflates or reduces outturn on a range of indicators

6. Risk Owners

Risk Owners are identified and empowered to manage risks based upon the action proposed in mitigation of the risk. The risk owner must be the person or group who has the responsibility for ensuring that action in response to risk is appropriate and who has the authority to ensure that action is taken. By assigning responsibility and management of risks to risk owners, the Council will be better placed to;

- Produce an Annual Assurance Statement
- Ensure that the identification of risks is an ongoing task
- Monitor and comment on how well risks are being managed
- Identify actions in progress to address risk issues

7. Departmental Risk & Assurance Registers and Corporate Risk Register

Once risks have been identified departmental risks are produced to capture relevant information. These should be maintained on an ongoing basis but as a minimum quarterly or in line with the agreed business planning process. A copy of the register should be retained by the department and a history of changes kept. Copies should be sent electronically to the Principal Consultant, Risk Management, Finance & Corporate Services Department ext. 2587.

Timetable for submission of departmental risk & assurance registers are

1st Quarter – June end
2nd Quarter – September end
3rd Quarter – December end
4th Quarter – March end

The submissions should not be a complex process as many registers will require a few amendments only.

Corporate Risk Register

The key risks of the Council should be recorded on a separate register. Under the control of the Executive Management team the register should identify which risks affect its medium or long term objectives. A periodic review of risks should be established informed in part by findings from departmental registers and other sources including internal and external audit and reports from other regulators or inspectorates. The Corporate Risk Register should be shared with the Principal Consultant, Risk Management, Chief Internal

Auditors Members and the Executive Management Team. A periodic timetable is suggested as follows;

Timetable for review and update of the Corporate risk register.

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

8. Risk prioritisation and escalation

Risks are prioritised within risk registers by their exposure rating. The higher the exposure the greater the risk. A traffic light system is employed to distinguish risks that require intervention, red risks, risks that require management amber risks and risks that require monitoring, green risks. Where it becomes apparent that a risk or group of risks remains high after controls are in place then the matter should be referred to management for action.

9. Risk Tolerance and Appetite

The amount of risk acceptable is a judgement of the potential frequency that an incident may occur or indeed the size of the impact that may result from a single or chain of events or a combination of both. Both scenarios are dependant on the range of controls available and their effectiveness. Where a risk or number of risks are in the red area they should be at the point of intervention and clarification from management sought as regards the appropriateness of any mitigating action planned to reduce the exposure.

10. Controls

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 Council assurance that the business process is robust and less likely to fail. The allocation of controls to an individual or a group is necessary to provide focus and ownership of the risk area. Unallocated risk has the potential of drifting unchecked.

Definition of Internal Control:

Internal control is the process, effected by management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

a. Reliability of financial reporting,
b. Effectiveness and efficiency of operations, and

c. Compliance with applicable laws and regulations.

Types of Internal Controls:

1. Detective:

Designed to detect errors or irregularities that may have occurred.

2. Corrective:

Designed to correct errors or irregularities that have been detected.

3. Preventive:

Designed to keep errors or irregularities from occurring in the first place.

Limitations of Internal Controls:

No matter how well internal controls are designed, they can only provide reasonable assurance that objectives have been achieved. Some limitations are inherent in all internal control systems. These include:

1. Judgement:

The effectiveness of controls will be limited by decisions made with human judgment under pressures to conduct business based on the information at hand.

2. Breakdowns:

Even well designed internal controls can break down. Employees sometimes misunderstand instructions or simply make mistakes. Errors may also result from new technology and the complexity of computerized information systems.

3. Management Override:

High level personnel may be able to override prescribed policies and procedures for personal gain or advantage. This should not be confused with management intervention, which represents management actions to depart from prescribed policies and procedures for legitimate purposes.

4. Collusion:

Control systems can be circumvented by employee collusion. Individuals acting collectively can alter financial data or other management information in a manner that cannot be identified by control systems.

Internal Control Objectives:

Internal Control objectives are desired goals or conditions for a specific event cycle which, if achieved, minimize the potential that waste, loss, unauthorized use or misappropriation will occur. They are conditions which management want the system of internal control to satisfy. For a control objective to be effective, compliance with it must be measurable and observable.

Internal Audit evaluates system of internal control by accessing the ability of individual process controls to achieve seven pre-defined control objectives. The control objectives include authorization, completeness, accuracy, validity, physical safeguards and security, error handling and segregation of duties.

Authorization

The objective is to ensure that all transactions are approved by responsible personnel in accordance with specific or general authority before the transaction is recorded.

Completeness

The objective is to ensure that no valid transactions have been omitted from the accounting records.

Accuracy

The objective is to ensure that all valid transactions are accurate, consistent with the originating transaction data and information is recorded in a timely manner.

Validity

The objective is to ensure that all recorded transactions fairly represent the economic events that actually occurred, are lawful in nature, and have been executed in accordance with management's general authorization.

Physical Safeguards & Security

The objective is to ensure that access to physical assets and information systems are controlled and properly restricted to authorized personnel.

Error handling

The objective is to ensure that errors detected at any stage of processing receive prompt corrective action and are reported to the appropriate level of management.

Segregation of Duties

The objective is to ensure that duties are assigned to individuals in a manner that ensures that no one individual can control both the recording function and the procedures relative to processing the transaction.
A well designed process with appropriate internal controls should meet most, if not all of these control objectives.

Major Components:

1. Control environment:

Factors that set the tone of the council, influencing the control consciousness of its people. The seven factors are (ICHAMPDO):

I - Integrity and ethical values,
C - Commitment to competence,
H - Human resource policies and practices,
A - Assignment of authority and responsibility,
M - Management's philosophy and operating style,
D - Director's and Audit & Pension Committee participation, and
O - Organizational structure.

2. Risk Assessment

Risks that may affect the council's ability to properly record, process, summarize and report financial data:

Changes in the Operating Environment
New Personnel
New Information Systems
Rapid Growth or reduced demand
New Technology
New Lines, Products, or Activities
Corporate Restructuring
Accounting rule changes

3. Control Activities

Various policies and procedures that help ensure those necessary actions are taken to address risks affecting achievement of entity's objectives (PIPS):

P - Performance reviews (review of actual against budgets, forecasts)

I - Information processing (checks for accuracy, completeness, authorization)
P - Physical controls (physical security)
S - Segregation of duties

4. Information and communication

Methods and records established to record, process, summarize, and report transactions and to maintain accountability of related assets and liabilities. Must accomplish:

a. Identify and record all valid transactions.
b. Describe on a timely basis.
c. Measure the value properly.
d. Record in the proper time period.
e. Properly present and disclose.
f. Communicate responsibilities to employees.

5. Monitoring

Assessment of the quality of internal control performance over time.

What can happen when Internal Controls are weak or non-existent?

When Internal Audit recommends improving controls within a department, there are often three basic arguments for not implementing our recommendations:

1. There is not enough staff to have adequate segregation of duties.
2. It is too expensive.
3. The employees are trusted and controls are not necessary.

These arguments represent pitfalls to unsuspecting management. Each argument is in itself a problem that needs to be resolved.

1. The problem of not having enough staff or other resources should be discussed with management. In most cases, compensating controls can be implemented in situations where one person has to do all of the business-related transactions for a department.
2. If implementing a recommended control seems too expensive, be sure to consider the full cost of a fraud that could occur because of the missing control. In addition to any funds that may be lost, consider the cost of time that would have been spent by the department during the time of an investigation of the matter, and the cost of hiring a new employee. Fraud is always expensive and the prevention of fraud is worth the cost.
3. Finally consider the issue of trust. Most employees are trustworthy and responsible, which is an important factor in employee relations and departmental operations. However, it is also the responsibility of

administrators to remain objective. Experience shows that it is often the most trusted employees who are involved in committing frauds.

11. Dealing with risks

Having identified and measured risks one of the following proportionate actions can be selected;

- Treat the risk – agree an action to manage the risk to an acceptable level
- Transfer the risk – possibly by purchasing additional insurance or bonds
- Terminate the risk – stop the current system or process and introduce a new system
- Tolerate the risk – if nothing reasonable can be done to control the risk because it may be out of the service or the council's sphere of influence
- 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.

12. Raw and residual risk

Most of the Council's risks are already subject to some degree of management. The actions listed above will therefore include existing and additional activities within the purview of the risk owner. The effectiveness of the action is judged on the basis of its success in reducing the likelihood of the risk and / or minimising the impact should it occur.

The risks are then re-evaluated in light of the suggested mitigation. These risks are then called residual risks and are to be entered onto the risk register.

Risk owners are encouraged to pro-actively share information relating to risks with colleagues in other divisions and departments to ensure that shared risks are identified and joint controls implemented.

13. Monitoring Arrangements

The ongoing requirement to monitor the risk management process and ensure the validity of risk ratings is satisfied by identifying risk owners who must regularly review their divisional risk logs together with the corporate risk register, make any necessary changes and report to senior management annually.

Members and the Executive Management team must take a strategic view of risks by assessing the highest priority risks against the Council's top objectives and priorities.

This responsibility includes the identification of the top risks, i.e. those that have the highest threat to the Council's objectives and which therefore require regular strategic input.

Members must satisfy themselves that the risk management system is functioning effectively and in a manner that they have approved. On-going review and an annual assessment can achieve this.

On-going review will be achieved through consideration of risks outlined in committee reports. In this way no decisions are taken without an analysis of the associated risks. This is effectively a process of continuous assessment to ensure that all significant aspects of the Council's business have been addressed.

The annual assessment will consider issues identified through the service and financial planning process, the work of Internal Audit and other assurance providers and any changes since the last assessment in the way the Council identifies and manages risks.

The on-going review and annual assessment will be instrumental in establishing the risk appetite and tolerances that Members require within the Council.

14. Audit & Pension Committee

The role of the Audit & Pension Committee is to receive information from officers that highlight the effectiveness of the control regime, management of risk, compliance with accounting practices and protocols and the performance of the authority more generally. Quarterly reports on risk management are submitted by the Principal Consultant Risk Management based in Internal Audit, Corporate Finance Division. Information from the departmental risk registers and other relevant sources will be used to communicate to members any relevant movement or variance in the risk profile.

15. Performance Management

The collation of Performance Data enables the organisation and services through transparency of information and monitoring against indicators. These indicators range from those which are required by statute and those which are set locally. It is important therefore that the quality of information that is collected by officers is consistent and accurate. A key risk for the council therefore is the validity of information. Comparison of the risk registers against performance indicators reveals commonalities in some cases. Appropriate risk treatment should be applied where indicators show that performance is deteriorating or failing to improve any necessary re-allocation of resources should be made balanced against the size of the risk. Regular testing of the quality of data captured is the responsibility of the departments and will be potentially be considered as part of the analysis of the Statement of Internal Control process.

16. Partnerships

Partnerships come in a number of forms, some are managed through firm contractual agreements others through Service Level Agreements and multiagency forums that see the council participating where community objectives are key. Significant partnerships, whether by value or by the nature of the desired outcome, should be risk assessed. It is the responsibility of the Department to ensure that where partnerships are formed that appropriate governance arrangement in place including the responsibility for risk management, assessment and reporting.6

17. Annual Assurance Statement

The Annual Assurance Statement is a legal requirement and is published each year along with the financial accounts. Departments contribute to this process by maintaining their risk & assurance registers throughout the year. Identified risks should be actively managed and the registers tabled for discussion quarterly at departmental management team meetings. The registers also assess assurance of the controls against risk. These assurances are independent reviews external to the core service area and can be identified through review bodies such as external audit, internal audit , regulators and inspectors. A panel of officers analyses the quality of information held in the registers and summarises the main control weaknesses of the authority for action. These control weaknesses are then assessed by a high level group, the Assurance Statement Panel comprising the Leader of the Council, Chief Executive and Director of Finance and Corporate Services. Once these are agreed they are then submitted to the Audit & Pension Committee for ratification and subsequent publishing along with the annual accounts.

Model Directors Annual Assurance Statement

HEAD OF DEPARTMENT ANNUAL ASSURANCE STATEMENT

Department: **Period: 2010/11**

Purpose

The Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for and used economically, efficiently and effectively. The council also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness. In discharging this overall responsibility, the council is responsible for putting in place proper arrangements for the governance of its affairs, facilitating the effective exercise of its functions, and which includes arrangements for the management of risk.

Accountability

As a Head of Department and member of the Executive Management Team, I am accountable for maintaining a sound system of assurance, risk management and internal control within my Department that supports the achievement of the Corporate and Department's objectives and principal statutory obligations, and for reviewing their effectiveness at least annually. The system of internal control is based on an ongoing process designed to identify the risks to the achievement of these objectives, to evaluate the nature and extent of those risks, to manage them efficiently, effectively and economically, and to gain assurances that the controls in place are working effectively.

Assurance

As a Head of Department I have responsibility for reviewing the effectiveness of the systems of risk management, internal control, and assurance. My review of their effectiveness has taken into account the following and is based on operating lines of defence:-

- Operational Management Internal Controls
- Risk Management Compliance
- Internal Audit and outcomes from reviews of services by other bodies including Inspectorates, external auditors etc.

The system of internal control is designed to manage rather than eliminate the risk of failure to achieve objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness.

I am satisfied that a sound system of internal control has been in place throughout the period and is ongoing. This is evidenced through the departments risk and assurance registers that are maintained throughout the year and reviewed by the Departmental Management Team

OR INCLUDE THE BELOW STATEMENT IF ANY SIGNIFICANT RISKS ARE TO BE DECLARED

*(I propose to take steps to address the matters identified in the attached risk & assurance register in order to enhance the adequacy of the directorate's internal controls. I am satisfied that these steps will enhance the system of internal controls and I will be monitoring to ensure their implementation and operation.)**

Signed:

Director of

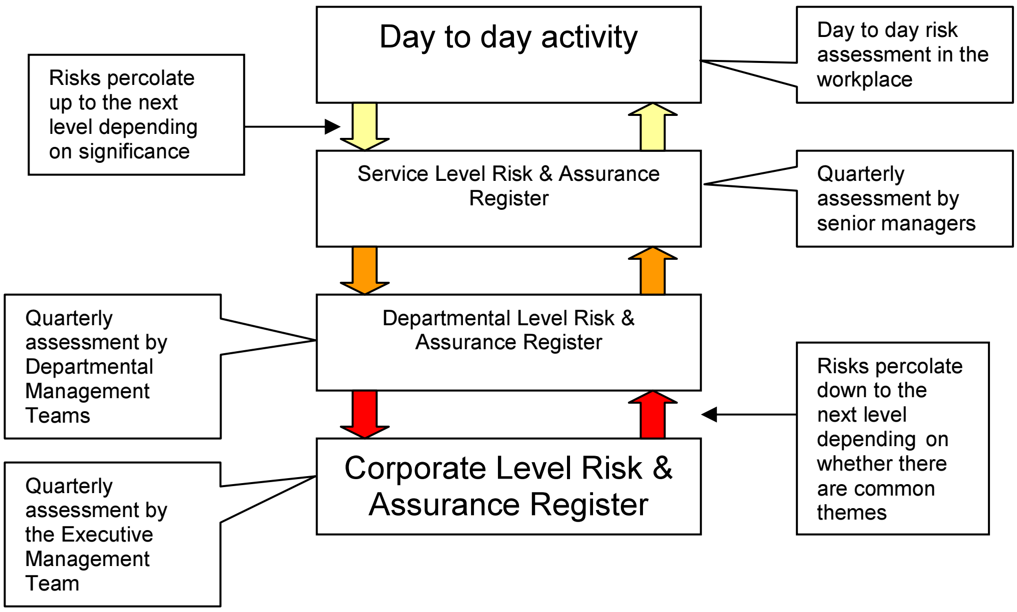
Date

18. Risk & Assurance Register

There are certain must haves in a risk register and the process of maintaining it also fits within a framework. A copy of the template for H & F risk registers can be accessed through the following link also attached as **Appendix A.**

\\LBHF\Root1\
FCS-Risk-Managemer

In the risk management hierarchy the process of maintaining register is outlined as follows;



19. Projects

Projects undertaken should comply with the Project Management toolkits guidance and procedures. The toolkit has separate risk monitoring arrangements designed to maintain transparency of the project in line with PRINCE 2 methodology. It is expected that Project Managers will maintain an appropriate risk register throughout the lifespan of the project. These may be subject to audit and inspection at any time by audit or the council's appointed risk consultant. Significant projects or issues that become apparent as the project develops may be required to be identified on the departmental or Corporate risk register.

20. Proximity of risk

Quite simply consider when the risk is likely to occur. For example in a construction project the risk of a contractor failing to deliver tiles for a roof on a new building would probably come fairly late in the timeline of the entire lifespan of the project, however planning permission and securing sufficient finance for the scheme would emerge as risks fairly early in project planning. It is always important to prioritise risks in logical order. Not all risks occur at the same time and this is inextricably linked to fluctuations in the likelihood and sometimes the impact of risks occurring. Risk Registers should therefore not remain static and be a dynamic tool for decision making in management. A history of risk & assurance registers should be maintained by the responsible officer accordingly.

21. Risk Assessment models

A variety of acceptable risk assessment tools can be and are widely used in the council. These assist with the identification, assessment and response to risk.

Tools	Identification	Assessment	Response
Risk Questionnaires	✓		
Risk Checklists / Prompt Lists	✓		
Risk Identification Workshop	✓	✓	
Nominal Group Technique	✓	✓	
Risk Breakdown Structure	✓	✓	
Delphi Technique	✓	✓	
Process Mapping	✓	✓	
Cause and Effect Diagrams	✓	✓	
Risk Mapping / Risk Profiling	✓	✓	
Risk Indicators	✓		
Brainstorming / " thought shower" events	✓		
Interviews and focus groups	✓		
"What if ?" workshops	✓		
Scenario analysis / scenario planning / horizon scanning	✓	✓	✓
Hazard and Operability Study (HAZOPs)	✓	✓	✓
PESTLE (Political, Economic, Sociological, Technological, Legislative, Environmental) Analysis	✓	✓	✓
SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis	✓	✓	✓
Stakeholder Engagement Matrices	✓		✓
Risk Register / Database	✓	✓	✓
Project Profile Model (PPM)	✓		✓
Risk Taxonomy	✓		
GAP Analysis: Pareto Analysis	✓	✓	

Probability and Impact Grid/Diagrams (PIDs) Boston Grid	✓	✓	
CRAMM	✓	✓	✓
Probability Trees		✓	
Expected Value Method		✓	
Risk Modelling / Risk Simulation (Monte Carlo/ Latin Hypercube)		✓	
Flow charts, process maps and documentation		✓	
Fault and event tree modelling;Failure Mode Effects Analysis		✓	
Stress Testing	✓	✓	
Critical Path Analysis (CPA) or Critical Path Method (CPM)		✓	
Sensitivity Analysis		✓	
Cash Flow Analysis		✓	
Portfolio Analysis		✓	
Cost-Benefit Analysis		✓	✓
Utility theory		✓	
Visualization techniques, heat maps, RAG status reports, Waterfall charts, Profile graphs, 3D Graphs, Radar chart, Scatter diagram		✓	✓

<u>APPENDIX A</u>

25/05/2011 11:26

Risk & Assurance register for xxxxxxx

								Inherent risk			Residual Risk												
STRATEGIC / OPERATIONAL	PESTLEcc	Risk Number	Council Priorities	Objectives (no more than 10)	Principal Statutory Obligations	Key risks	Consequences	Impact	Likelihood	Total	Impact	Likelihood	Total	Risk Monitoring	Responsible Officer	Existing controls	Gaps in Controls	Assurances (What tells you that the controls are effective)	Gaps in Assurance	Proposed action to remedy gaps in control or assurance	Date of implementation of additional control or date of next review of risk	Open / closed	Residual / Inherent Diff
						What could prevent this objective being achieved?											Y/N		Y/N				
								5	5	25	5	5	25	ADDITIONAL CONTROLS DESIRABLE								Open	0
								4	4	16	4	4	16	ADDITIONAL CONTROLS DESIRABLE								Open	0
								3	3	9	3	3	9	Keep under review								Open	0
								2	2	4	2	2	4	Keep under review								Open	0
								1	1	1	1	1	1	Keep under review								Open	0
										0			0	Keep under review								Open	0