Appendix A

London Borough of Barking & Dagenham

Draft Risk Management Policy

Purpose of this Document

The London Borough of Barking & Dagenham (LBBD) has a moral and statutory duty of care to its citizens, employees, partners and assets. The Authority will meet this duty by assuring that risk management plays an integral role in the sound governance of the Council through its processes for policy and decision-making, operational management and overall performance monitoring and review.

This duty is now underpinned by a statutory requirement. The Accounts and Audit Regulations 2003 require the Authority to produce an annual Statement of Internal Control, which enforces the need for a risk management framework to be in place.

The publications 'Corporate Governance in Local Government' (CIPFA/SOLACE 2001) and 'Worth the Risk – Improving Risk Management in Local Government' (Audit Commission 2001) have highlighted the importance of Councils introducing robust arrangements for effective risk management. This has grown in importance due to the changing pressures that local authorities face (which potentially give rise to a range of new and complex risks) and an increase in the number of high profile incidents (e.g. child abuse, failing schools) which have increased demands for better risk management processes, as well as changes in the way that Council's deliver services e.g. the introduction of partnership arrangements.

This Risk Management Policy (the Policy) forms part of the Council's corporate governance arrangements and:

- Explains the Authority's underlying approach to risk management;
- Outlines key aspects of the risk management process;
- Identifies the main reporting procedures; and
- Documents the roles and responsibilities of all parties involved in the process.

As in other fields, the Authority aspires to best practice in the identification, evaluation and cost-effective control of risks to ensure that they are eliminated or reduced to an acceptable level; hence all members and employees are expected to read and adhere to this Policy.

Underlying Approach to Risk Management

Risk is defined as being the threat that an event or action will adversely affect an organisation's ability to achieve its objectives and to successfully execute its strategies. Risk management is defined as being the process by which risks are identified, evaluated and controlled. (Audit Commission 2001)

The following key principles underline the Authority's approach to risk management:

- The Chief Executive is ultimately accountable for the system of internal control and the management of risk across the whole of the Authority. The Corporate

Management Team (CMT) provides advice and challenge to assist the Chief Executive in discharging this accountability;

- There is an open and receptive approach by CMT to discussing and addressing risks within the Authority;
- A Corporate Risk Management Group (CRMG) is tasked with overseeing the implementation of the Council's Risk Management Policy and the operation of the risk management process, though in practice it delegates day to day responsibility to the Departmental Risk Management Groups (DRMGs). Chief Officers will have discretion to organise the working processes and structure of the DRMG to suit the particular needs of their department;
- Departmental Managers are responsible for risk management within their area of the business and are also responsible for notifying their DRMG, CRMG and CMT where exposure to risks is of a material nature;
- Risk management is everyone's responsibility. All risks will be formally allocated to owners;
- Regular monitoring of key risk indicators will take place by CRMG, CMT and the Corporate Monitoring Group, with oversight by the Council; and
- The role of the Corporate Monitoring Group is to provide independent assurance to the Executive and the Council with regard to the maintenance of an adequate system of internal control and the management of risk across the Authority.

Framework

Our vision is that all significant risks inherent to the Authority's business are identified, evaluated and cost effectively controlled within acceptable levels of exposure as part of the business management process.

The key objectives of the framework and policy are to ensure a consistent basis for the measurement, control, monitoring, follow-up and reporting of risk that is based on the Authority's appetite for risk, not those of individuals.

There are many ways of categorising risk and Authorities will vary in their approaches to fit their own aims and objectives. However, risk management should be integrated into all relevant management processes and LBBD has chosen to adopt the categories of risk as set out in Appendix 1.

Measurement of Risk

Top Risks and Sub Risks for all areas will be identified through risk workshops with CMT members. The impact and likelihood for each risk, before and after controls, have been considered and a 1 to 9 scoring mechanism used to give a position on a 9 X 9 matrix with scores ranging from 1 to 81, with 81 being the highest score. In order to ensure consistent application across the Authority, only the criteria for the impact and likelihood scores given in Appendices 2 and 3 should be used.

Risk Before and After Controls

In order to assess the effectiveness of controls (also known as risk management or mitigation strategies), risk is first scored before considering the operation of the Authority’s controls, this is termed the ‘Inherent Risk Score’. For each risk, the controls in place are then identified and assessed and the risk score is generally reduced to arrive at the ‘Residual Risk Score’.

The control should either reduce the likelihood that a risk will occur or the impact were it to occur. Residual risk is what is left after considering controls. Where the score after controls is still at an unacceptably high level, additional actions may be required in order to reduce the risk level further.

The Authority’s objective is to optimise its controls, i.e. the most cost-effective controls are in place for each risk and the cost versus the benefit of the control is considered. This may mean that certain risks have a high residual score because the cost of reducing the risk still further may be higher than the potential cost if the risk actually happens - the level of residual risk will however need to be considered for compliance with this policy.

Monitoring of Risks

Risk registers will be kept up to date on a ‘real-time’ basis via a regular review by Departmental Managers and DRMGs to indicate they have considered changes in the risk profile of their own departments.

The CRMG will review the risk registers on a three monthly basis, and CMT and the Corporate Monitoring Group will review the risk registers on a six monthly basis. The update may take the form of new risks, changes to or additional controls, and changes to risk scores. Key triggers for significant changes to risk registers will be new regulations, implementation of new projects, high staff turnover, changes in the external environment, risk events, and Internal Audit reviews. Roles and responsibilities are summarised below.

Using the framework above, a consistent methodology for measuring and scoring risks is applied throughout the Authority. The ‘risk appetite’ – what is an acceptable level of risk for LBBD – can be read against the following scores shown on the table below:

- A residual risk score of 12 or less is considered acceptable to the Authority and will require no further action other than to ensure the relevant controls are operating effectively. Departmental Managers should however review the controls for low risk areas carefully to ensure there is not over control.
- A residual risk score of 13 to 30 will require the implementation of additional controls unless subject to CRMG agreement and acceptance.
- A residual risk score of 31 or more will require the implementation of additional controls unless subject to CMT and Corporate Monitoring Group agreement and acceptance.
- Where the impact of risk is considered major (impact score of 8) and/or the likelihood is considered frequent (likelihood score of 9), these will be submitted to CRMG for review and acceptance.

- Where the impact of risk is considered catastrophic (impact score of 9), these will be submitted to CMT and the Corporate Monitoring Group for review and acceptance.

Impact	**9**	**9**	**18**	**27**	**36**	**45**	**54**	**63**	**72**	**81**
	8	**8**	**16**	**24**	**32**	**40**	**48**	**56**	**64**	**72**
	7	**7**	**14**	**21**	**28**	**35**	**42**	**49**	**56**	**63**
	6	**6**	**12**	**18**	**24**	**30**	**36**	**42**	**48**	**54**
	5	**5**	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**
	4	**4**	**8**	**12**	**16**	**20**	**24**	**28**	**32**	**36**
	3	**3**	**6**	**9**	**12**	**15**	**18**	**21**	**24**	**27**
	2	**2**	**4**	**6**	**8**	**10**	**12**	**14**	**16**	**18**
	1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
		Likelihood								

Red

Amber

Green

Reporting of Risks

CMT will each year approve the top risks, risk appetite and reporting protocols as part of the annual planning process in January. This will entail confirmation of the size of risk – impact and likelihood guides (Appendices 2 and 3) together with the risk appetite detailed above.

CMT will also be required to review and sign off the residual risk scores appearing in the red area on the risk matrix above in May, together with the draft statement on internal control, and in November each year. The Corporate Monitoring Group will report bi-annually to the Executive on its assessment of the adequacy of the policies and actions in place to manage those top risks residually shown as red.

In order to provide CMT and the Corporate Monitoring Group with the necessary assurance, the CRMG will review and sign off the residual risk scores appearing in the red and amber areas on the risk matrix above in January, April, July and October each year. These reviews will also form the basis of the annual assurance statements required in support the annual statement on internal control.

Project Management

An integral part of the Authority's project methodology is that all new projects require a risk register to be prepared at the outset of the project. At the beginning of the project, the focus is on identifying the key risks and what controls should be put in place to mitigate these risks. As the controls have not yet been implemented, it is the 'Inherent Risk Score' that is the primary focus as this is effectively the residual risk to LBBD. As the project progresses and controls are implemented, the residual risk score falls.

New projects change the Authority's risk profile and it is important that the CRMG is able to approve and accept these projects before implementation or any significant investment/outlay has been made. The criteria that has been established is as follows:

- An inherent risk score of 50 or more will require CMT and Corporate Monitoring Group agreement and acceptance.

The use of an inherent risk score of 50 rather than 31 (the Authority's policy as set out in the Framework above) reflects the fact that risks are being looked at before controls. Any residual risk scores that are scored at 31 or greater at the time the project is implemented would require CMT and Corporate Monitoring Group approval through the normal process of referring all risks with a residual score of 31 or more to the CMT and the Corporate Monitoring Group.

Roles and Responsibilities Summary

The Chief Executive

The Chief Executive is ultimately responsible for the management of risks and the system of internal control across the Authority's business. In discharging this responsibility, he is advised by the Corporate Monitoring Group and CMT (which is in turn advised by the CRMG). To enable the Chief Executive to sign off the annual statement on internal control, the Chief Executive receives statements of assurance from Chief Officers, in relation to key risks and internal control within their sphere of responsibility, and from the Head of Internal Audit in relation to the whole system of internal controls within the Authority's business.

Day-to-day management responsibility for the implementation of the Authority's risk management strategy has in the short term been delegated to the Head of Audit who reports to the Chief Executive on progress.

Role of the Executive

The role of the Executive is to give a steer to the Chief Executive on the adequacy of the risk management framework within the Authority and provide a robust independent challenge where appropriate. The Executive reviews the adequacy of overall risk management policy via review of reports from CMT and the Corporate Monitoring Group; and oversees the application of the Policy within the Authority.

Executive members assist CMT by bringing an independent perspective to the identification and management of risk to strategy and the delivery of objectives, and by ensuring good governance practice.

Role of the Corporate Monitoring Group

The Corporate Monitoring Group is responsible for reporting to the Executive on its assessment of the internal control system. The Corporate Monitoring Group will receive reports from CMT and the Head of Audit on the management of key risks and the application of the risk management process throughout the Authority, and will report to the Executive on its assessment of the adequacy of the policies and actions in place to manage those top risks residually shown as Red.

Role of CMT

CMT is responsible for developing and overseeing the Authority's risk management policy, for identifying and evaluating strategic risks and designing, operating and monitoring a suitable system of internal control. In this role, CMT is supported by the CRMG.

Role of the Corporate Risk Management Group

The CRMG carries out a variety of functions:

- Act as a steering group to oversee the introduction of risk management into Council and Departmental policies and to be 'drivers' of the initiative;
- Provide an ongoing review of the risk management policy and strategy for the Council;
- Take proactive measures to oversee the inclusion of risk management in the Council's Balanced Score Card and Departmental Management Teams agenda;
- Identify and profile the Councils' key strategic and generic risks and be responsible for setting up and maintaining the Council's Risk Register;
- Formulate action plans to deal with cross-departmental strategic and operational risks;
- Set up and provide training, advice and support to the DRMGs; and
- Prepare quarterly progress reports to CMT.

Role of the Departmental Risk Management Groups

The DRMGs will be responsible for implementing risk management techniques to embed risk management into their services.

Role of the Head of Audit

The Head of Audit has delegated responsibility for the development of the risk management framework, including the risk management policy within the Authority and reports to the Chief Executive and CMT on progress. Detailed implementation is led by the CRMG, which is supported by specialist advice from within Internal Audit.

Specifically:

- Internal Audit within the Authority will carry out independent reviews on the effectiveness of risk management and internal control and report the detailed results of these reviews to the appropriate Departmental Managers, CRMG and CMT;
- The reviews will be based on an annual plan agreed with CMT and approved by the Corporate Monitoring Group. A summary of results will be reported to the Corporate Monitoring Group and CMT; and
- Internal Audit will also provide advice to the CRMG, Chief Officers, Departmental Managers and other business managers on the assessment of risk and design of controls to mitigate them.

Role of Chief Officers and Departmental Managers

Chief Officers are responsible for ensuring the proper management of risks within their departments and, when requested, giving assurance to the Chief Executive. Annual assurance statements are required to support the annual statement on internal control. Chief Officers are also responsible for cascading the implementation of the risk management policy and strategy within their departments.

Departmental Managers are responsible for implementation of bottom up self-assessment processes as an embedded feature of day-to-day business processes. They are required to provide assurances to their Chief Officers in order to allow them to provide the appropriate assurances to the Chief Executive.

Categories of Risk — Appendix A1

The following categories of risk are neither prescriptive nor exhaustive, but provide a framework for identifying and categorising a broad range of risks facing each service. For this reason it is recognised that the Authority will consider the risks associated with each of the sub-categories and their interrelationships when performing its full risk assessment.

You should also consider the following risk categories and examples:

- **Political risks** e.g. failure to deliver local or central government policy.
- **Operational risks** related to physical assets, human resources, IT, service delivery and clients.
- **Legal and regulatory risks** related to compliance with legislation and regulations, EC directives, statutory duties and potential litigation.
- **Developmental risks** e.g. strategic planning, outsourcing, capital projects, re-organisation and the management of change.
- **Financial risks** related to income and expenditure e.g. major financial loss, fraud, breakdowns in financial control, financial viability of projects.
- **Reputational risks** e.g. corporate image, media coverage, and unauthorised disclosure of confidential/sensitive information.

Size of Risk – Impact **Appendix A2**

Descriptor	Impact Guide
1 None	No impact
2 Insignificant	No regulatory consequence No impact outside single objective / local system No reputational damage or adverse publicity Immaterial Financial Loss
3 Minor	No regulatory consequence No impact outside single objective / local system No reputational damage or adverse publicity Financial loss that cannot be absorbed in current year budget
4 Moderate	Minor regulatory consequence Some impact on other objectives, processes or systems No reputational damage or adverse publicity Financial loss that requires budget virement in current year
5 Significant	Limited regulatory consequence Impact on other objectives, processes or systems Limited reputational damage or internal adverse publicity Financial loss that requires a supplementary estimate
6 Significant	Significant regulatory consequence Impact on many other objectives, processes or systems Significant reputational damage or local adverse publicity Financial loss that requires a significant call on the Council's reserves
7 Substantial	Substantial regulatory consequence Impact on strategic level objectives Substantial/widespread reputational damage or national adverse publicity Financial loss reducing contingency balances below best practice levels
8 Major	Major regulatory consequence Impact on strategic level objectives Major/severe reputational damage or national adverse publicity Central Government interest/administration Financial loss that stops the Council's funding an essential service priority
9 Catastrophic	Catastrophic regulatory consequence Impact at strategic level Catastrophic reputational damage or national adverse publicity Central Government interest/administration Financial loss that has the capacity to undermine the financial solvency of the Council Closure/transfer of business

Size of Risk – Likelihood **Appendix A3**

Descriptor	**Likelihood Guide**
1 Incredible	<1% likely to occur in next 12 months / Is not judged as credible
2 Improbable	1% - 5% likely to occur in next 12 months
3 Remote	5% - 10% likely to occur in next 12 months
4 Remote	10% - 20% likely to occur in next 12 months
5 Occasional	20% - 30% likely to occur in next 12 months
6 Occasional	30% - 40% likely to occur in next 12 months
7 Probable	40% - 60% likely to occur in next 12 months
8 Likely	60% - 80% likely to occur in next 12 months / More likely than not
9 Frequent	>80% likely to occur in next 12 months / Almost certainly