

## **RISK MANAGEMENT POLICY (September 2006 – March 2009)**

### **INTRODUCTION**

1. The aim of this policy is to further embed risk management at Mid Bedfordshire District Council. This policy document contains details to assist Managers on the processes to follow, to help achieve the objective of effective Risk Management.

### **CONTENTS OF THIS POLICY**

2. To provide detailed guidance on the following areas:-
  - Roles and Responsibilities;
  - Risk Identification Process;
  - Different Types of risk;
  - Risk Financing;
  - Analyse the Risks;
  - Risk Register Contents;
  - Maintenance of Risk Registers;
  - Frequency of Risk Register reviews;
  - Mechanism for communicating Risks;
  - Risk reporting;
  - Risk Management Training;
  - Learning process;
  - Effective arrangements for Risk Management;
  - Risk Register content review;

### **ROLES & RESPONSIBILITIES**

3. In order to ensure the successful implementation of the risk management strategy, clear roles and responsibilities for the risk management framework and process are needed. These are listed below.

<b>Group/Individuals</b>	<b>Role/Responsibilities</b>
Ethics and Standards Committee	<ul style="list-style-type: none"> <li>• Approving the Risk Management Strategy and Policy</li> <li>• Receive regular updates of the corporate risk register</li> <li>• Receive a report from the Audit Manager stating whether effective risk management arrangements operated</li> <li>• Receive a report from the Audit Manager stating whether annual statement of assurance on Risks and Controls are obtained</li> </ul>
Leader of the Council	<ul style="list-style-type: none"> <li>• Meeting with the Chief Executive to ensure that strategic risks are monitored</li> </ul>
Portfolio Holders	<ul style="list-style-type: none"> <li>• Meeting with relevant Directors / Deputy Chief Executive to ensure that operational risks are monitored</li> </ul>
Chief Executive	<ul style="list-style-type: none"> <li>• Overall responsibility for ensuring that strategic risks are effectively managed within the Council</li> <li>• To provide an annual statement of assurance on</li> </ul>

	strategic risks
Deputy Chief Executive	<ul style="list-style-type: none"> <li>To coordinate / act as Officer Champion for risk management</li> </ul>
Management Team	<ul style="list-style-type: none"> <li>Contribute towards the identification and management of strategic and cross cutting risks</li> <li>Regularly review the corporate risk register</li> <li>To act as the Council's coordinating group on Risk Management to assist the Chief Executive, rather than having a separate group established.</li> </ul>
Directors / Deputy Chief Executive	<ul style="list-style-type: none"> <li>Overall responsibility for identifying, analysing and scoring operational risks for their divisions</li> <li>Ensuring operational risk registers are regularly reviewed</li> <li>To provide annual assurance on the effectiveness of controls in place to mitigate / reduce risks within their divisions to an acceptable level</li> <li>To maintain awareness of and promote the risk management strategy and policy to all relevant staff</li> <li>Ensure that risk management is incorporated into service and project plans</li> </ul>
All Service Managers	<ul style="list-style-type: none"> <li>Contribute towards the identification and management of operational risks for their division</li> <li>To maintain awareness of and help promote the approved risk management strategy and policy to all staff.</li> </ul>
Internal Audit Manager	<ul style="list-style-type: none"> <li>To facilitate the maintenance of the corporate risk register.</li> <li>To receive / maintain a copy of all risk registers held</li> <li>To independently review / report to Ethics and Standards Committee on the compilation / regular review of corporate / operational risk registers</li> <li>To ensure the risk management strategy and policy documents and corporate risk registers are published on the MBDC web-site</li> </ul>
All Employees	<ul style="list-style-type: none"> <li>To highlight to management any risks arising and contribute to the control process to mitigate the risks to an acceptable level</li> </ul>

## RISK IDENTIFICATION PROCESS

4. Much care must be taken to prevent risk identification / monitoring and reporting becoming a timely and costly industry in itself. Management should only measure those risks that can be, and need monitoring, to help ensure Corporate and Operational objectives are achieved. The Corporate and Operational objectives of the Council should provide the starting point for any management of risk. Managers should not think about risk in the abstract, but concentrate on events that might effect the Councils achievement of its objectives. Strategic risks linked to the Corporate Objectives and Operational risks linked to service and project plans need (as a minimum) to be identified and monitored.

5. **Strategic Risks** - It is up to the Chief Executive, Management Team and the Leader of the Council to determine important Strategic risks that could prevent the Council from achieving its Corporate Objectives. Assurance providers / indicators should be identified and progress made should be reported / monitored to contribute towards management of such risks. The Corporate Risk Register being the means used to record, monitor and report the Strategic risks. The size of the register is not prescribed, but should be appropriate to the size and risks facing the authority.
6. **Operational Risks** – It is up to the Directors / Deputy Chief Executive in conjunction with Portfolio Holders to determine important Operational risks that could prevent achievement of Operational Objectives, as stated in service and project plans. Only those risks that are of a concern need recording and monitoring. However, these should include contingency or disaster recovery plans. Assurance providers / indicators should be identified and progress made should be reported / monitored to contribute towards management of such risks. The Operational Risk Register being the means used to record, monitor and report the operational risks. The extent of the register is not prescribed, but should be appropriate to the size and risks facing the service/project area.
7. **Cross Cutting Risks** – All involved in the risk management process, including the Chief Executive, Management Team and the Leader of the Council, etc. should consider whether any Corporate / Operational activities result in cross cutting risks on other areas of the Council. The relevant management should liaise to determine the appropriate method of treating any cross cutting risks.
8. **Projects & Contract Risks** – All new projects and contracts should have had their various risks considered before being approved. In the case of a project, the risks should be defined in the Project Initiation Document. In the case of a contract, the relevant Director is responsible for ensuring relevant risks have been considered. The relevant Director to ensure all significant contracts e.g. in excess of £200,000 in value each year, should be subject to annual financial checking on the viability of relevant contractors. If any projects / contracts are deemed “Major” by any of the Management Team or Chief Executive, they should be added to the Corporate Risk Register, and monitored until the project / contract is deemed “well controlled”, after which it can be removed. Otherwise projects / contracts should be recorded and monitored on Operational Risk Registers.

## DIFFERENT TYPES OF RISK

9. Financial Risk e.g. loss of income or greater expenditure than anticipated is the primary risk identified and measured. However, this is just one of several different types of risk that can be measured. It is not just the impact of an event happening in financial terms that need to be evaluated, but also the potential damage that such an event could have upon other things such as the reputation of the Council. Examples are given of the many different types of risks that Members / Officers may wish to consider need monitoring: -

<b>Strategic risks</b>	
Political	Linked to possible failure to deliver Council objectives or central Government policy
Economic	Affecting the ability of the Council to achieve its

	commitments
Social	Relating to the Council's ability to meet the effects of changes in demographic, residential or social-economic trends
Technological	The ability to identify technological changes and using technology to meet changing demands
Legislative	The ability to meet the legislative demands affecting the Council
Environmental	Relating to the environmental impact of the Council's service delivery
Best Value	The need to demonstrate 'Best Value' in service delivery
Customers	The ability to understand the changing needs of our customers

<b>Operational risks</b>	
Professional	Associated with the professional competence of Council officers and the recruitment and retention of staff
Financial	Associated with the financial resources and related controls
Legal	Relating to potential breaches of legislation
Physical	Related to physical damage, security, accident prevention and health & safety
Contractual	Associated with the failure of the Council's contractors to deliver services or products to the agreed cost and specification
Technological	Associated with reliance on operational equipment
Environmental	Associated with pollution, noise, energy efficiency and community safety
Best Value	The need to demonstrate Best Value in "service delivery"
Customers	Associated with the ability to engage all our customers and the identification of their changing needs and related issues of equality.

## **RISK FINANCING**

10. Management should consider if and how insurance could be used to mitigate Corporate / Operational risks. The three options available are:

- Retention – internal (insurance) sources of funds.
- Transfer – external (insurance) sources of funds.
- Hybrid – internal/external (insurance) sources of funds.

11. It could be that risk financing is not appropriate for identified risks. However, if applicable, Managements need to:

- Consider the ease or difficulty of implementing the chosen option.
- Establish fund sources e.g. allocating costs, to offset the consequences of drawing on fund sources.
- Review whether the risk financing method chosen over time is still appropriate.

- To consider whether the insurance cover is necessary, either via an external supplier or internally via insurance fund and whether the level of cover is appropriate.

## ANALYSE THE RISKS

12. Having identified the risks to be measured, a method of measuring the risks should be followed. To encourage consistency, a simple 3 x 3 “Risk Model” or map is used, to score the identified risks in terms of likelihood and impact. A broad definition for each element of the grid is shown on the model to assist scoring. Although scores are always judgemental, they should be soundly reached.

## Risk Model

High	<b>Important risks - may potentially affect provision of key services or duties</b> 6	<b>Key risk- may potentially affect provision of key services or duties</b> 8	<b>Immediate action needed - serious threat to provision and/or achievement of key services or duties</b> 9
<b>IMPACT</b>	<b>Monitor as necessary - less important but still could have a serious effect on the provision of key services or duties</b> 3	<b>Monitor as necessary - less important but still could have a serious effect on the provision of key services or duties</b> 5	<b>Key risks - may potentially affect provision of key services or duties</b> 7
Low	<b>No action necessary</b> 1	<b>Monitor as necessary - ensure being properly managed</b> 2	<b>Monitor as necessary- less important but still could have a serious effect on the provision of key services or duties</b> 4
	Low	<b>LIKELIHOOD</b>	High

## RISK REGISTER CONTENTS

13. The identified risks, once analysed and scored should be recorded in a risk register. There should be one risk register for strategic risks known as the Corporate risk register and a number of risk registers for operational risks e.g. at least one Operational risk register for every division as a minimum. Although large divisions may have several Operational risk registers. The number being up to the Director to determine. However many of risk registers are maintained, it will contain details of the following: -

- The Risk description
- The Gross Risk Score (i.e. before existing controls applied)
- The Residual Risk Score (i.e. after controls applied)
- The Target Risk Score (i.e. what risk score is acceptable)
- Risk Owner
- The Key Controls in Place
- The Risk Indicators (i.e. what will show risk is being controlled or not)

- Action required (i.e. where Residual Risk score exceeds Target Risk score over time)

## **MAINTENANCE OF RISK REGISTERS**

14. Each Division is responsible for maintaining their own Operational Risk Registers. Copies of these Operational registers should be forwarded electronically to the Audit Manager who will maintain a central file, containing all Operational Risk registers.
15. The Audit Manager is responsible for maintaining the Corporate Risk Register.

## **FREQUENCY OF RISK REGISTER REVIEWS**

16. The Corporate Risk register will be reviewed by the Management Team on a quarterly basis i.e. at the end of June, September, December and March. The Audit manager to facilitate such reviews, by obtaining information from assurance providers. The results of Corporate Risk register reviews will be reported to the Ethics and Standards Committee, before being published on the MBDC web-site.
17. The Operational Risk registers will be reviewed at least twice during the year e.g. mid way through the year and in March, to enable a risk assurance statement to be completed, covering the whole financial year. Directors/Deputy Chief Executive to determine whether the risk register needs reviewing more frequently, depending upon the importance of the activity/event and perceived risks. However, Operational risk registers should be reviewed within one month of any additional services / personnel being added to a Division.

## **MECHANISM FOR COMMUNICATING RISKS**

18. The risk management process to be effective needs mechanisms to report identified risks 'top down' and "bottom up". Starting with the Corporate Objectives and the identification and control of these and other strategic risks, rolling the process down where applicable to an operational level.
19. If staff have concerns, or identify strategic risks that have been missed, these should be fed back to the Audit Manager who facilitates the maintenance of the Corporate Risk register. Any such information will be reported to Management Team for consideration, when the strategic risks are next considered or more promptly, if the need arises. This is because all staff need to be aware that they are part of the process in assessing / reporting strategic risks, not just Directors and the Deputy Chief Executive who make up the Management Team.
20. Similarly, Directors and the Deputy Chief Executive should discuss progress made against identified operational risks with their staff, through team meetings. The operational risks when scored should be recorded on the Operational risk register. Links need to exist, so that any operational risks that are assessed of concern e.g. are scored 7, 8 or 9 on the risk model, are reported by the Director or nominated Officer to the Audit Manager. These risks are to be added to the Corporate Risk register and reported to Management Team for consideration, when the Strategic risks are next considered or more promptly, if the need arises. These high operational risks are to be monitored by Management Team, with corrective actions

agreed. Only when these risks have reduced to an acceptable level will they be removed from the Corporate Risk register.

## **RISK REPORTING**

21. The following arrangements will be followed:

- Strategic Risks – the Audit Manager will maintain the Corporate Risk register. Updating of the Corporate Risk register will require input from Assurance Providers. The updated Corporate Risk register being reported quarterly to Management Team and Ethics and Standards Committee, highlighting any changes in the risk scores, either up or down from the previous period. At the year-end, the Chief Executive to sign off an assurance statement stating if all significant Corporate Risks have been identified; whether the Corporate Risks have been reviewed, and scores awarded are appropriate to the risks identified.
- Operational Risks – Each Director/Deputy Chief Executive will maintain Operational Risk registers under their control. A copy of all Operational Risk registers to be forwarded to the Audit Manager, who shall maintain a comprehensive library of all risk registers. At the year-end, Director/Deputy Chief Executive to sign off an assurance statement, stating if all significant Operational Risks have been identified; whether the Operational Risks have been reviewed, and scores awarded are appropriate to the risks identified.

## **RISK MANAGEMENT TRAINING**

22. Directors and Managers are responsible for cascading the risk management process for new staff to follow. Risk Management training will be arranged, if requested by Directors / Managers or Members and within budgetary constraints by the Audit Manager. Any problems in providing sufficient training to carry out risk management processes should to be reported to the Chief Executive, as Head of Paid Service in the first instance. If training issues are not resolved, this fact is to be reported to the Ethics and Standards Committee by the Audit Manager, as they oversee the effectiveness of risk management arrangements.

## **LEARNING PROCESS**

23. Directors, Service Managers and Officers operate the risk management practices. Any good ideas that evolve to further improve the risk management process to be forwarded to the Audit Manager, who will facilitate the sharing of good practices / ideas with other Directors.

## **EFFECTIVE ARRANGEMENTS FOR RISK MANAGEMENT**

24. In order for the risk management arrangements to be determined as effective, certain tasks will be needed to be carried out:-

- a) The Corporate Risk register to be reviewed four times in the year;
- b) Operational Risk registers to be reviewed at least twice per year;

- c) If the residual risk exceeds the target risk, corrective action been agreed and monitored;
  - d) If the residual risks on Operational Risk Registers are scored a 7, 8 or 9, they were added to the Corporate Risk Register;
  - e) Operational Risk registers were reviewed within one month of any additional services / personnel being added to a Division;
25. The Audit Manager will report in June each year to the Ethics and Standards Committee, whether the above risk management arrangements have been followed, to help demonstrate effective risk management.

### **RISK REGISTER CONTENT REVIEW**

26. Following any changes to the Corporate Objectives or a Council election (May 2007) the Corporate Risk register should be reviewed with the Leader, to ensure all important risks are identified, measured and monitored.
27. Following any new Service Plan being issued, the Operational risk registers should be reviewed with relevant Portfolio Holders, to ensure all important risks are identified, measured and monitored.

Revised September 2006