Information Asset Owner:	Head of Service Development
Protective Marking:	Not protectively marked
Page :	1 of 10

Policy:	**Corporate Risk Management**

To:	Document Type:	✔	Document Summary:
• Fire Authority Members • Brigade Managers • Area Commanders • Group Commanders • Station Commanders • Support Service Directors • Support Service Managers	Policy	✔	The purpose of this document is to set out the Authority's policy, structures, processes and methodology for the management of corporate risks.
	Assessment		
	Procedure		
	Guidance Note		
	Technical Note		
	Information		
	Safety Critical		
Keyword: Risk			
Please note that as Documents are frequently updated, if you print a document, its accuracy cannot be guaranteed, always check for latest version.			

Document History

1.1   The Authority's first Corporate Risk Management Policy was approved by the Combined Fire Authority in August 2006.

1.2   The policy was updated in September 2010 to reflect good practice guidance published by the Office of Government Commerce (OGC) in its publication "Management of Risk: Guidance for Practitioners".

1.3   The policy and accompanying guidance was reviewed and updated following the outcomes of an Internal Audit review of Corporate Risk Management, the findings of which were presented to the Overview & Audit Committee in December 2014. This found the policy to be out of date and not reflective of the current process operating within the Authority.

Policy:	Corporate Risk Management

Contents

Version:	V 1.1	**Status of document:**	Draft
Author:	Corporate Planning Manager	**PIA:**	
Issue Date:	9 February 2015	**Review Date:**	January 2018
File Name	2015 Corporate Risk Management Policy		

1.0 Policy Statement

1.1   Buckinghamshire and Milton Keynes Fire Authority (the 'Authority') recognises that risk management is a vital activity that underpins and forms part of our vision, values and strategic objectives, including those of operating effectively and efficiently as well as providing confidence to our community. Risk is present in everything we do and it is therefore our policy to identify, assess and manage key areas of risk on a pro-active basis. We seek to embed risk management into the culture of the Authority and Buckinghamshire Fire and Rescue Service (the 'Service') and the behaviour of all people involved in the management, operation and development of the Authority and Service. Risk management needs to be embedded throughout all processes, projects and strategic decisions, including procurement and contracting which will ensure that the management of partnerships and third party relationships are included within the scope of our risk management policy.

1.2   The aim for our risk management framework is that it will be fit for purpose, reflect our size and the nature of our various operations and make optimal use of our skills and capabilities.

1.3   In order for risk management to be effective and become an enabling tool, we must ensure we have a robust, consistent, communicated and formalised process across the Service. In order to obtain a clear picture of which risks will threaten the ability of the Authority to achieve its objectives it is important the level of risk which the Authority considers acceptable for the organisation to be exposed to, its 'risk appetite', is defined.

1.4   This risk management policy and supporting documentation form an integrated framework that supports the Authority and Service in the effective management of risk. In implementing our management of risk system we seek to provide assurance to all our stakeholders that the identification and management of risk plays a key role in the delivery of our strategy and related objectives. We will involve, empower and give ownership to all of our staff in the identification and management of risk. Management of risk activity will be regularly supported through discussion and appropriate action by the senior management. This will include a thorough review and confirmation of the significant risks, evaluating their mitigation strategies and establishing supporting actions to be taken to reduce them to an acceptable level. Managing risks will be an integral part of both strategic and operational planning and the day-to-day running, monitoring, development and maintaining of the Authority and Service.

2.0 Risk Management Definitions

2.1   The Authority recognises and has adopted the Office of Government Commerce (OGC) definitions of 'risk' and 'risk management' published in "Management of Risk: Guidance for Practitioners (2011)":

Definition of Risk		Definition of Risk Management
An uncertain event or set of events that will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact.		Systematic application of principles, approach and process to the tasks of identifying and assessing risks, and then planning and implementing risk responses.

3.0 Risk Appetite

3.1   Risk appetite is the amount of risk that the Authority is willing to tolerate relative to the size, nature and degree of certainty associated with the pursuit of any related opportunities. Managing risk effectively does not mean that the Authority is risk averse but rather that it is aware of the risks associated with any decisions that it takes and is willing and able to accept the consequences for the Authority and Service in the event of any risk crystallising.

As a general principle risks attracting a combined score of 15 or more on the Probability and Impact Grid (shown at Appendix B) will be considered intolerable by the Authority and prioritised for treatment in order to eliminate or reduce the risk to acceptable levels. However, the Authority, at its discretion, may elect to tolerate risks at this level or deem lower levels of risk to be intolerable on a case by case basis.

4.0 Governance Structures

4.1   Governance of Corporate Risks, and the policies and processes by which they are managed, is carried out via the Authority Committee and Service Management Meeting Structures:
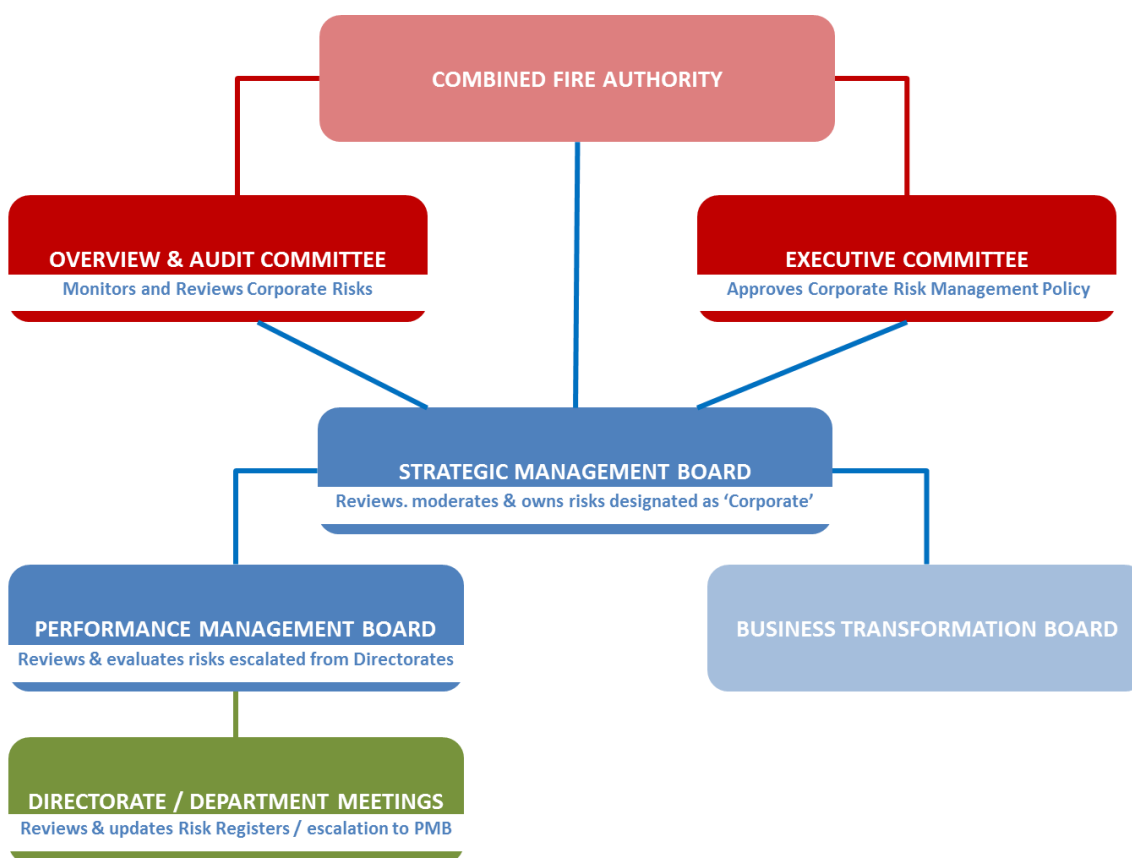
4.2   Monitoring and management of corporate risks is carried out at a level commensurate with the nature and magnitude of the risk.

4.3   Risk management is embedded in the Service's core operational, support and change management processes. Risks with the potential to become Corporate Risks are captured and evaluated in Risk Registers maintained by all significant business units within the Service (typically at Directorate level). These risks are regularly reviewed in Directorate Management Meetings and may be escalated to the Performance Management Board (PMB) at the discretion of the relevant Director / Head of Service if they meet the escalation criteria set out at pages 9-10 of this document.

4.4   PMB meets on a quarterly basis. It reviews the content of the Corporate Risk Register and evaluates risks escalated from Directorate level and, subject to that evaluation, may recommend them to the Strategic Management Board (SMB) for inclusion in, or removal from, the Corporate Risk Register.

4.5   SMB meets on a monthly basis. Each month it reviews the current set of risks designated as 'corporate' to ensure that their status, evaluations and controls remain valid. On a quarterly basis it also reviews recommendations from the Performance Management Board for risks to be included in, or removed from, the Corporate Risk Register. If new, urgent, potential corporate risks are identified outside of the quarterly review cycle these may be escalated directly to SMB by Directors or Heads of Service via the Corporate Planning Manager. SMB is also responsible for reviewing quarterly risk management reports to the Authority's Overview and Audit Committee (O & A).

4.6   O & A meets on quarterly basis. Its Terms of Reference require it:

1. To monitor the effective development and operation of risk management and corporate governance within the Authority.

2. To consider reports dealing with the management of risk across the organisation, identifying the key risks facing the Authority and seeking assurance of appropriate management action.

4.7   The Authority's Executive Committee meets six times a year. The Financial Regulations, at Section C, state that the Executive Committee is responsible for approving the Corporate Risk Management Policy after considering recommendations from the Overview and Audit Committee.

5.0 Roles & Responsibilities

5.1 Authority Members

Hold the Chief Fire Officer / Chief Executive accountable for the effective management of risk throughout the Service via the Overview and Audit Committee.

Approve, via the Executive Committee, the Authority's Corporate Risk Management Policy.

Review, via the Overview and Audit Committee, the Corporate Risk Register and associated reporting.

Challenge Brigade Managers, Directors and Heads of Service to satisfy themselves that risks have been correctly identified, evaluated and addressed.

Raise any potential risks that they may identify to the Head of Service Development, or other designated officer, via the Chairman of the Overview and Audit Committee.

5.2 Chief Fire Officer / Chief Executive

Accountable for the effective management of risk throughout the Service and ensuring that appropriate processes and systems are in place to ensure this.

5.3 Directors and Heads of Service

Responsible and accountable for the identification, evaluation, recording and effective management of all risks within their Directorate / Department using approved Authority policies and procedures.

Responsible and accountable for ensuring that all risks meeting the escalation criteria at pages 9 -10 are escalated to the Performance Management Board or Strategic Management Board for scrutiny as appropriate.

5.4 Corporate Planning Manager

Responsible for developing, maintaining, and implementing the Authority's Corporate Risk Management Policy.

Maintains the Corporate Risk Register and risk identification, recording, evaluation and reporting processes for use across the Authority / Service.

Information Asset Owner:	Head of Service Development
Protective Marking:	Not protectively marked
Page :	8 of 10

Policy:	Corporate Risk Management

6.0 Risk Management Processes and Methods

6.1 Identification of risks

Corporate risks can emerge from a variety of sources including:

- Authority / Service processes & systems

- People (staff, CFA members, partner organisations, contractors, the public)

- Buildings & equipment

- Contracts

- Partnerships arrangements & activities

- The policies, actions and activities of Central Government

- Other external Political, Economic, Social, Technological, Environmental or Legal (PESTEL) factors

Service Managers will use structured methods to assist with the identification of risks emanating from such sources including:

- The analysis of external risk registers and analyses such as the National Risk Register and Thames Valley Local Resilience Forum Community Risk Register.

- Application of the PESTEL framework and / or other horizon scanning tools

- The outputs of self-assessments, formal audits (internal and external) and Peer Reviews

6.2 Evaluation of Risks

All risks will be evaluated against the criteria shown at Appendix A to determine their probability and the nature and scale of their potential impact.

Risks will then be prioritised for treatment using the thresholds defined in the 'Probability and Impact' Grid shown at Appendix B.

6.3 Recording & Reporting of Risks

Evaluated risks are recorded using a common format at both Directorate and Corporate levels. This is shown at Appendix C.

Formal review and reporting of Corporate Risks is undertaken on a quarterly basis to the Performance Management Board (PMB), Strategic Management Board (SMB) and the Authority's Overview and Audit Committee as set out in Section 4 of this document. SMB may also consider new risks requiring urgent consideration outside of the normal quarterly reporting cycle at its formal monthly meetings or weekly informal meetings if the situation demands it.

6.4 Managing Risks

Methods appropriate to the nature and scale of the risks should be employed to control and manage them. Typically these will include one or a combination of the following methods:

Terminate	This involves methods such as stopping the activity or process or divesting of the asset giving rise to the risk.
Treat	Implement control measures that reduce the likelihood and / or the impact of the risk to acceptable levels.
Transfer	Transfer the cost of the risk to a third party e.g. insurance, contract, outsourcing
Tolerate	Accept the risk as it is and do nothing to further mitigate it.

6.5 Risk Escalation Criteria

It is expected that the majority of risks will be managed at Directorate level. However, all Directorate risks scored at 15 or above ('Red' risks), using the Probability and Impact Grid shown at Appendix B, must be escalated to PMB for review. PMB **will** escalate these risks to SMB if they meet at least one of the following criteria:

1. The means of reducing, mitigating or controlling the risk are considered inadequate and additional interventions or resources beyond those available within the individual Directorate are required;

2. The nature and scale of the risk is such that it cannot be effectively monitored and managed at Directorate level.

Also risks falling within the amber zone on the Probability and Impact Grid may, at the discretion of the line Director or Head of Service, be elevated to PMB for review and potential escalation to SMB if they consider that they are of a pan-organisational nature and / or there is insufficient capacity, resources and / or means of treating it at Directorate level with the consequent potential for it to become 'intolerable' (red zone).

SMB will act as the final point of review for potential corporate risks for inclusion in the Corporate Risk Register which will then be subject to scrutiny by the Authority's Overview and Audit Committee.