Service Document Guidance:
Corporate Risk Management

1.0 Changes since the last version — Annex B

Guidance reviewed and updated to reflect:

- latest (2018) ISO 31000 Risk Management Guidelines;
- current Service Document publication protocols;
- changes to Service internal governance structures (revisions to management Boards terms of reference and introduction of Portfolio Management Office);
- new risk impact and scoring matrices.

Additions and changes relative to the 2015 Corporate Risk Management Policy are shaded grey.

2.0 Index

3.0 Purpose and scope

The purpose of this document is to provide guidance to facilitate the effective identification, analysis, evaluation, treatment, monitoring and reporting on risks that could affect the Authority's ability to deliver services to the public and / or meet its strategic objectives.

Day to day management of occupational health and safety risks and the management of risk in the community fall outside the scope of this guidance. The Service has established processes and procedures for managing health and safety based on standards set by the Institute of Occupational Safety and Health (IOSH). The identification, evaluation and treatment of risks to the public / communities is addressed via the Service's Integrated Risk Management Planning (IRMP) processes.

4.0 Risk Management Definitions

4.1 ISO 31000:2018 defines 'risk' as the "effect of uncertainty on objectives" and 'risk management' as "coordinated activities to direct and control an organization with regard to risk". However, in addition, the Authority also recognises the earlier definitions specified by the Office of Government Commerce (OGC) and 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.

5.0 Risk Appetite

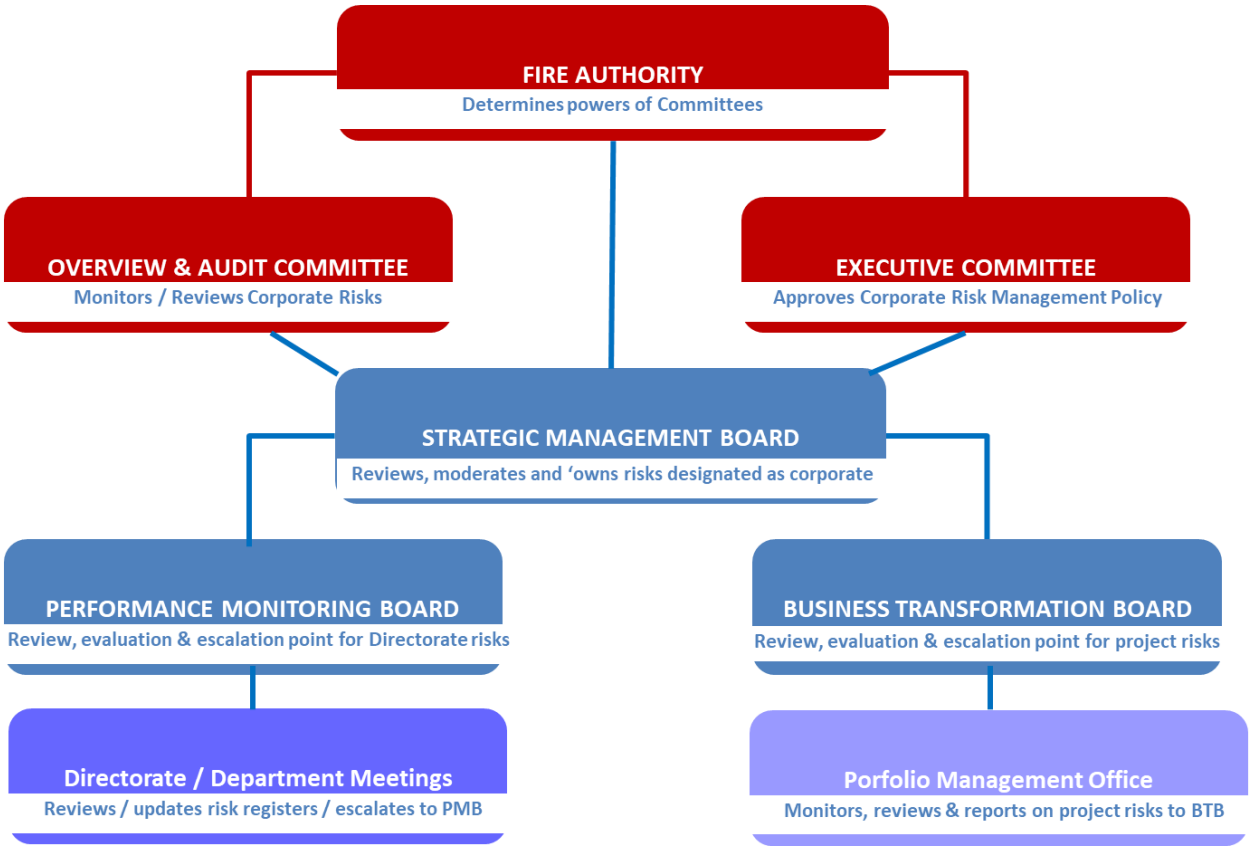
5.1 Risk appetite is the amount of risk that the Authority is willing to tolerate relative to the size, nature and degree of uncertainty associated with identified threats and opportunities. Managing risk effectively does not mean that the Authority / Service is risk averse but rather that it is aware of the risks associated with any decisions that it takes and is willing and able to accept the consequences in the event of a risk crystallising.

As a general principle, risks attracting a combined score of 20 or more on the Risk Scoring Matrix (shown at Appendix 2) 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 depending on their source and nature.

6.0 Governance Structures

6.1 Governance of Corporate Risks, and the policies and processes by which they are managed, is carried out via the Authority Committee and Service Management Structures:



6.2 Monitoring and management of corporate risks is carried out at a level commensurate with the nature and magnitude of the risk.

6.3 Risk management is embedded in the Service's core operational, support and project 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 Monitoring Board (PMB) at the discretion of the relevant Director / Head of Service if they meet the escalation criteria set out at pages 10 of this document.

6.4 All projects are required to maintain risk registers in a prescribed format. Project risk registers are monitored by the Portfolio Management Office (PMO) who refer significant risks to the Business Transformation Board (BTB) for review and, if necessary, further escalation to the Strategic Management Board (SMB). BTB meets on a regular basis aligned to the dates of Strategic Management Board (SMB) meetings.

6.5 PMB meets on a regular basis at a frequency agreed by SMB. 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 SMB for inclusion in the Corporate Risk Register.

6.6 SMB normally meets on a monthly basis. At every meeting, it reviews the current set of risks designated as 'corporate' to ensure that their status, evaluations and controls remain valid and any project risks escalated by BTB. It also reviews recommendations from PMB for risks to be included in the Corporate Risk Register escalated from Directorate / Department risk registers. If new, urgent, potential corporate risks are identified outside of the normal 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 the corporate risk management reports that are submitted to every meeting of the Authority's Overview and Audit Committee (O & A).

6.7 The O & A Committee's 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.

6.8 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.

7.0 Roles & Responsibilities

7.1 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 Service Senior Management to satisfy themselves that risks have been correctly identified, evaluated and addressed.

Raise any potential risks that they may identify to the Director of Legal and Governance, or other designated officer, via the Chairman of the Overview and Audit Committee.

7.2 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.

7.3 Directors and Heads of Service

Responsible and accountable for the identification, evaluation, recording and effective management of all risks within their Directorate / Department using the approved Authority policy and this guidance, appointing suitable persons to manage their risk registers and reporting arrangements as appropriate.

Responsible and accountable for ensuring that all risks meeting the escalation criteria at page 10 are escalated to the PMB, BTB and / or SMB for scrutiny as appropriate.

7.4 Corporate Planning Manager

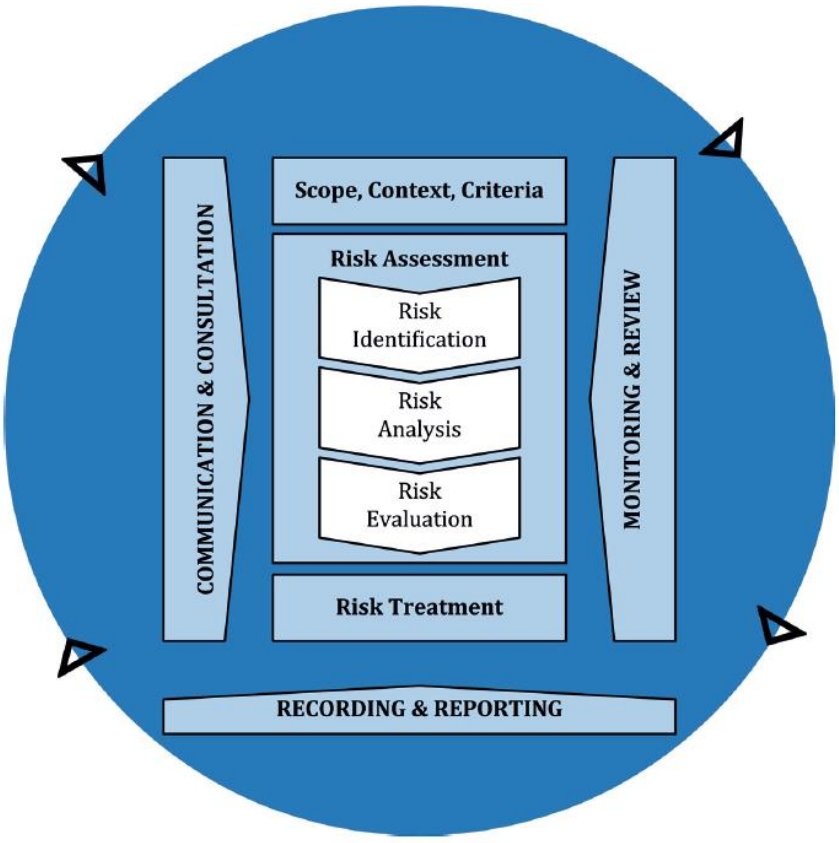
Responsible for developing, maintaining, and implementing the Authority's Corporate Risk Management Policy.

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

Liaises with the Authority Lead Member to ensure that they are regularly updated on any changes to risks recorded in the corporate risk register and consulted on any proposals for changes to the Authority's Corporate Risk Management Policy and / or guidance.

8.0 Risk Management Processes and Methods

ISO 31000:2018 specifies the following risk management process model which has informed the development of this guidance:



8.1 Identification of risks

UK Government provides a comprehensive framework for the identification of organisational risk:

Type of risk	Features and approaches	Examples
Internal	These are risks over which the organisation has some control, for example risks that can be managed through internal controls and, where necessary, additional mitigating actions. This often involves traditional risk management, such as risk registers, controls and assurance.	• Fraud • Health & safety • Capacity & capability • Data security • Delivery partners
External	This focuses on big external events/perils and then considers how to make the organisation more resilient to such events, in part because of difficulties on assessing likelihood[2]. A tried and tested approach to managing external risks is through considering the impact those external events could have on infrastructure, finance, people, operations and reputation. A common example of a resilience framework for infrastructure is a business continuity plan.	• Economic downturn • Terrorist attack • Extreme weather • Cyber attacks
Strategic	This third element concerns the organisation's raison d'être and key objectives (such as the organisation's enduring purpose and the objectives set out in the Single Departmental Plan), identifying the principal risks to the achievement of those within a set timeframe. For some this could be the lifetime of a parliament. Risks in this area would be accompanied by regularly monitoring and adjusting interventions, as necessary. Forward-looking charts are often helpful here.	Can be: • immediate impact risks to the organisation's ability to continue operating, e.g. loss of customer data; or • slow-burning risks that grow and eventually prevent delivery of objectives, e.g. staff turnover or leadership capability.

Major projects	Major projects form such a critical part of the plans for many government bodies. Experience suggests that one or two critical projects for that organisation should be considered at board level in their own right. The key is to only report to board level on the two or three that really matter This should be via whatever tools, techniques and reporting are appropriate for each.	These risks will be specific to the major project in question, and could involve: • shifting requirements • slippage in delivery timeframes • failure to deliver

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

- The analysis of external risk registers 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, project risk evaluations, formal audits (internal and external), peer reviews and formal inspections such as those conducted by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS).

8.2 Analysis of risks

In line with ISO 31000:2018 guidance, analysis of risks will consider:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

8.3 Evaluation of Risks

All risks will be evaluated against the criteria shown at Appendix 1 to determine the nature and scale of their potential impact.

Risks will then be prioritised for treatment using the 'Risk Scoring Matrix' shown at Appendix 2.

8.4 Recording & Reporting of Risks

Formal review and reporting of Corporate Risks are undertaken to every PMB and SMB meeting, and also to the Authority's Overview and Audit Committee as set out in Section 6 of this document. SMB may also consider new risks requiring urgent consideration outside of the normal reporting cycles at its weekly informal meetings if the situation demands it.

Corporate Planning will provide appropriate templates and systems for analysing, evaluating, recording and reporting risks identified at directorate and corporate levels. The PMO will do the same for project risks.

8.5 Treating 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:

Avoid	By not starting an activity or investment that gives rise to the risk.
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 risk to / share with a third party e.g. insurance, contract, outsourcing, partnering.
Tolerate	Accept the risk, by informed decision, as it is and do nothing to further mitigate it.

8.5 Risk Escalation Criteria

It is expected that the majority of risks will be managed at Directorate / Department / Project level. However, all risks scored at 12 or above (dark Amber / Red risks), using the Risk Scoring Matrix shown at Appendix 2, 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 avoiding, reducing, mitigating, controlling or eliminating the risk are considered inadequate and additional interventions or resources beyond those available within the individual Directorate / Department are required;

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

Also, other risks falling within the amber zone (8-10) on the Risk Scoring Matrix 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.