APPENDIX 2

City of London Corporation

RISK MANAGEMENT POLICY AND STRATEGY (INCLUDING THE RISK MANAGEMENT PROCESS GUIDE)

DUDLEY, PAUL

ANNOTED VERSION 1.1 – FOR 2021 UPDATE

Endorsed by Audit and Risk Management Committee: (May 2021)

Table of Contents

SECTION 1 – Risk Management Policy Statement

Introduction

1.1 The City of London Corporation is the governing body of the Square Mile dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally successful UK. It aims to contribute to a flourishing society, support a thriving economy and shape outstanding environments by strengthening the character, capacity and connections of the City, London and the UK for the benefit of people who live, learn, work and visit here. Its unique franchise arrangements support the achievement of these aims.

1.2 The Square Mile is the historic centre of London and is home to the 'City' – the financial and commercial heart of the UK. The City Corporation's reach extends far beyond the Square Mile's boundaries and across private, public and charitable and community sector responsibilities.

1.3 The City of London Corporation ("the City Corporation") is responsible for ensuring that its business is conducted in accordance with the law and proper standards of governance; that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively; and that arrangements are made to secure continuous improvement in the way its functions are operated.

1.4 In discharging this overall responsibility, the City Corporation is responsible for putting in place proper arrangements for the governance of its affairs and facilitating the effective exercise of its functions, which includes arrangements for the management of risk.

1.5 Well managed risk taking should be recognised by all managers and staff within the City Corporation as being fundamentally important to effective service delivery, maximising opportunities for innovation in service development and adapting to change. It underpins the City Corporation's values of Relevant, Reliable, Responsible and Radical.

1.6 Only by active management of risks will the City Corporation be able to meet its corporate aims and outcomes which in turn will enhance the value of services provided to the City.

1.8 The City Corporation aim's to be an exemplar of good practice and continue to meet its statutory responsibility to have in place satisfactory arrangements for managing risks, as laid out under regulation 4 of the Accounts and Audit Regulations 2015:

"The relevant body is responsible for ensuring that the financial management of the body is adequate and effective

and that the body has a sound system of internal control which facilitates the effective exercise of that body's functions and which includes arrangements for the management of risk."

1.7 The effective management of risk is at the heart of the City Corporation's approach to delivering cost effective and valued services to the public as well as being an important element within the corporate governance of the organisation.

1.8 Consequently, all staff and managers must understand the importance of well thought through and managed risks in decision making and adopt an approach that will help identify, assess, ~~acting to~~ manage them ~~and~~ as well as reviewing progress.

2.0 The Policy Statement

2.1 The City Corporation recognises and accepts its legal responsibility[1] to manage its risks effectively, has adopted a proactive approach to well thought through risk taking (balancing opportunity and risk) to achieve its objectives and enhance the value of services to the Community.

2.2 The overall aim being to increase the likelihood of delivering on the Corporate Outcomes and key corporate and service objectives by supporting innovation, encouraging creativity, minimising threats and providing an environment that risk management is seen as adding value to service delivery.

2.3 This policy applies to all departments and institutions of the City Corporation. [2]

3.0 Policy Objectives:

a) Ensure that risk management effectively supports the **corporate governance** of the City Corporation.

b) Maintain and Improve **leadership** and **collaboration** of risk management activity across the City Corporation.

c) **Integrate** risk management into the **culture** of the City Corporation as well as to its key management processes including corporate and service business planning processes, programmes, projects, performance and financial management.

[1] Accounts and Audit Regulations 2015 (as amended)
[2] The City of London Police have adopted their own risk management policy and process. ~~statement.~~ Bridge House Estates have adopted a risk protocol (2021) based upon the City's Risk Management Policy and Strategy.

d) Ensure that the **risk management process** for identifying, evaluating, controlling, reviewing, reporting and communicating risks across the City Corporation is in line with **Best Practice**, consistently applied, understood and owned by all relevant staff.

e) Ensure that the Summit Group, Grand/Service Committees and the Audit and Risk Management Committee, external regulators and other stakeholders obtain necessary **assurance** that the City Corporation is managing and mitigating its business risks effectively:

f) **Continuously improve** risk management through learning and experience and actively **Communicate** to the City Corporation's risk management approach to all employees and stakeholders.

4.0 These key objectives will be achieved by:

- Ensuring that the City Corporation's risk management strategy (which includes clear roles and responsibilities) is in line with current standards and best practice guidance.
- Demonstrating dynamic and effective management, reporting and challenge of risks at both Officer and Member levels. This provides assurance to external regulators, the public at large and other stakeholders that the City Corporation is managing /mitigating its risks and in line with good corporate governance practice.
- Complying with all relevant statutory requirements.
- Recognising that effective Partnership working can be part of the ways that risks are mitigated..
- Providing opportunities for shared learning and training on risk management across the City Corporation.
- Embedding, supporting and promoting effective risk management.

5.0 Appetite for risk

5.1 The City Corporation will minimise unnecessary risk and manage residual risk to a level commensurate with its status as a public body so that:

- The risks have been properly identified and assessed.
- The risks will be appropriately managed, including the taking of appropriate actions and the regular review of risk(s).

5.2 The City of London Corporation will also positively decide to take risks in pursuit of its strategic aims where it has sufficient assurances that the potential benefits justify the level of risk to be taken.

6.0 Roles and Responsibilities

6.1 Management and staff should be familiar with, and competent in, the application of the City Corporation's risk management policy, and are accountable for the delivery of that policy within their areas of responsibility. A full set of roles and responsibilities is set out in Risk Management Strategy.

7.0 Review

7.1 This policy will be reviewed and, where appropriate, updated, on an annual basis.

Approved:

Signed…….	Signed……
John Barradell	
Town Clerk	Alderman Alex Barr – Chairman Audit and Risk Management Committee

Date: ~~28 January 2020~~

SECTION 2 – Risk Management Strategy

2.0. Introduction

The aim of this risk management strategy is to set out a formal and structured approach to identifying, assessing, managing and reporting risk within the City Corporation (known as the risk management framework). It should be read conjunction with the Risk Management Policy Statement as well as the risk management guidance for officers.

The following sections include:

- a description of the components of the risk management framework,
- the levels of risk that the City Corporation has identified, the reporting arrangements including those to ~~Grand~~Grand/Service Committees,
- criteria for escalating risks from one organisational level to another and applying the City Corporation's risk appetite to corporate risks.
- A list of the roles and responsibilities for Committees, senior management groups and officers involved in the risk management framework.

By adhering to this strategy, the City Corporation will be better placed to ~~meet~~ achieve ~~all~~ its Corporate Outcomes and objectives in an efficient, effective and timely manner.

Every risk is linked to a business objective and this strategy will help enforce a proactive stance to managing these risks, ensuring that less time is spent reacting to situations and more time is spent taking advantage of opportunities.

The City Corporation's risk management framework is an integral part of the City Corporation's overall corporate governance arrangements as well as supporting the delivery of the Corporate Plan.

Listed below are some of the benefits of successfully implementing this strategy:

- Protecting and enhancing the City of London Corporation's reputation
- Improve organisational resilience
- Increase the likelihood of achieving its goals and delivering outcomes
- Improve the identification of opportunities and threats
- Improve governance, stakeholder confidence and trust
- Establish a reliable basis for decision making and planning
- Effectively allocate and use resources for risk mitigation

2.0 The risk management framework

The framework consists of the following components:

4.0 Levels of organisational risk

To ensure that risk is managed at the appropriate level within the City Corporation the following levels of risk have been identified:

Corporate - if they occurred, would have a significant impact on the City Corporation as a whole (or significant part of) and/or the successful delivery of its corporate outcomes and its ability to exercise its functions. See Appendix 2 for the characteristics of a corporate risk.

Departmental - if they occurred, would seriously inhibit the achievement of the aims and objectives of the department. They differ from Corporate risks in that they usually only impact on one department, rather than cutting across several departments.

Service – if they occurred would usually concern failure to achieve service objectives. Service risks are those concerned with maintaining an appropriate level business service to existing and new service users.

Team – those risks concerned with team related objectives. These will be lower order risks, often those regarded as business as usual.

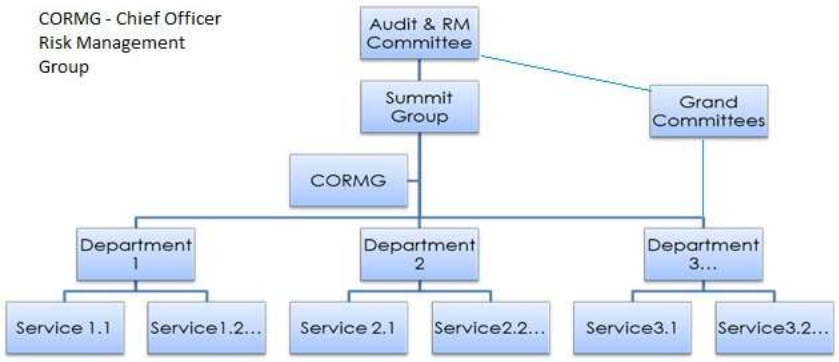
Programme/Project - their impact is limited to the programme/project's outcomes, budget, or timescales.

5.0 Review and reporting of risk registers

The following section outlines the reporting arrangements for these levels of risks.

The diagram below illustrates the reporting lines from service/team level to departmental and corporate levels. Below is a set of criteria which provides guidance on escalating/de-escalating a risk from one level to another.

There is a cyclical quarterly reporting process that is now embedded within the City Corporation. The diagram below shows the hierarchy of reporting lines from departments to Committees.



Note: Summit Group may be retitlied and with a revised Chief Officer membership following the implementation of the 2021 Target Operating Model changes

Formatted: Font: 10 pt, Not Bold, No underline

Formatted: Font: 10 pt

Formatted: Font: 10 pt, Not Bold, No underline

Corporate risks – all corporate risks must be owned by a Chief Officer and as such should be reviewed and updated, together with their department's risks, on at least a quarterly basis. They should be reviewed by the departmental management team.

Chief Officers who own corporate risks must report them to their relevant service committee/Grand Committee[3] at least quarterly (although for schools may this is termly). The format of this report has been agreed by Summit Group and available on the Intranet risk management page.

[3] CoL Reporting risk information to Grand Committees

Corporate risks are reported quarterly to the Chief Officer Risk Management Group (CORMG) working on behalf of the Summit Group, to review all corporate risks as well as make recommendations for new corporate risks received from Chief Officers. CORMG will apply criteria to assess the suitability of a risk to be approved as a corporate risk. (see appendix 2)

Summit Group subsequently receive a quarterly risk update report and may approve new risks to be added or existing risks to be escalated on to the corporate risk register or de-escalated to the relevant departmental risk register.

The quarterly risk report is presented to the Audit and Risk Management Committee by the Chamberlain. Any new corporate risks must be endorsed by this Committee.

Departmental - departmental risk registers must be reviewed on at least a quarterly basis at their respective Departmental Management Team Meeting (DMT).

They may also take the opportunity to any new identify new risks as well as recommending to CORMG, departmental level risks which may to be suitable for inclusion in the Corporate Risk Register.

The Chief Officer is responsible to approving recommendations for a departmental risk to be considered as a corporate risk by CORMG.

Departmental risks, together with any corporate risks owned by the department, must be reported their respective Grand /Service Committee on at least a quarterly basis. (Note, the three schools report termly)

The Grand/Service Committee may make recommendations to the Audit and Risk Management Committee in respect of existing corporate/departmental risks or other matters for their consideration.

All red departmental risks are reported, at the same time as all corporate risks, to CORMG. These risks are also included in the quarterly risk updates to Summit Group and the Audit and Risk Management Committee.

Service – within each department there will be individual divisions, groups or functional areas. For this purpose, these are known as services and each may have a service level risk register. (Note that some departments are relatively small and may not require or need service risk registers). Service level risk registers must be reviewed at least quarterly by service management team meetings. Risks may be recommended for escalation to the departmental management team to consider for inclusion in the departmental risk register.

Team – within each service area there may be individual teams. Team level risk registers, where they exist, should be reviewed quarterly by the team management team.

Programme/Project – Programme/Project-related risks are identified from the outset during the initial risk assessment. Further risk assessments are should be undertaken at the beginning of every new stage of the project. Regular project team meetings are used for monitoring progress in manging these

risks as well as horizon scanning for project risks. Project risk guidance is available on the Intranet Project Management intranet page.

5.Escalation criteria

Risks may be escalated or de-escalated from one level organisational level to another (e.g. from departmental to corporate level). The guidance below sets out the factors to be taken into consideration when escalation/de-escalation should occur.

A risk may be moved to a higher level in the organisation (escalated) for the following reasons:

- The risk becomes unmanageable at current level
- The risk is outside of the appetite boundaries (see para 6 below)
- The risk remains very high even after control measures have been fully implemented
- The risk impacts on more than one department/functional area
- The risk is directly related to an organisational objective

De-escalation

A risk may be moved to a lower level in the organisation (de-escalated) for the following reasons:

- The risk can be controlled and managed at a lower level
- The risk rating has decreased significantly or is not considered to be critical to the achievement of a corporate /departmental objective.
- The risk is below appetite boundaries (se para 6 below).
- The risk will only affect one department/project or programme/functional area and is better controlled locally.

Note: Escalation/de-escalation of a risk is not automatic and will depend upon the judgement of senior management or senior management groups as to whether this should take place. There may be reasons why a risk should remain at a particular level e.g. it's the level best placed manage it.

6.Risk appetite

The City Corporation's ~~in its~~ Risk Management Policy outline~~d in broad terms~~, its approach to taking risk (i.e. risk appetite) in that it will seek to minimise taking any unnecessary risks but also to reduce risk to an acceptable level to a public body. It ~~will~~ also seeks to take risks to achieve its strategic /corporate outcomes/objectives, but these will be considered and well thought before such risks were taken.

Risk appetite is defined as *"the amount of risk and organisation is willing to accept*" so by articulating how much and type of risks which is acceptable it

provides a basis for making judgements on the balance of the benefits and the taking of the risk.

The City Corporation has set risk appetite levels for ten categories of risk and these aremust be applied to all corporate risks. The following diagram shows relative risk appetites for each of these categories of risk.

Risks which are scored in the shaded area would be regarded as above risk appetite.

The risk appetite levels are indicative given the spread and complexity of risks within each category. These indicative risk appetite levels will be used for corporate risks ~~will are included on the corporate risk register~~ only.

For risks below corporate level, officers must have regard to the indicative risk appetite ratings above when determining whether to escalate or de-escalate a risk (see para 5 above).

(Note: Risks which have the same current and target risk scores will be recorded as "accepted "in risk register reports. No target risk date is required in such circumstances. Detailed guidance is available on the risk management intranet site for officers who use the Pentana Risk system to generate risk reports.

Formatted: Font: (Default) +Headings (Calibri Light), 13 pt, Font color: Accent 1

7.Effectiveness of the City Corporation's risk management framework

The City Corporation will periodically review the effectiveness of its risk management framework through either an external benchmarking exercise or review, internal audit review or self-assessment. The Policy and Strategy will be reviewed annually.

8. Roles and responsibilities

The following sets of the roles and responsibilities of officers and groups within the risk management framework.

Court of Common Council

- To receive annual assurance from the Audit and Risk Management Committee on the effectiveness of the City Corporation's risk management framework and its application.

Audit and Risk Management Committee

- Provide assurance to the Court of Common Council on the effectiveness of the risk management framework and its application. (The Chairman is the Member Risk Champion).
- Review the effectiveness of risk management arrangements · Provide comment and challenge on risk management activity and progress.

Grand Committees/Service Committees

- Oversee the significant risks faced by Departments in the delivery of their service responsibilities.

Summit Group (or successor Chief Officer Group following the implementation of 2021 Target Operating Model changes)

- Promoting, steering and monitoring risk management for the Corporation. The Summit Group oversees the strategic elements of risk management.

- Overall accountability for risk management across the City Corporation including ensuring the corporate risk register is a live and up to date record of the current risk exposure
- Set the tone for risk management, promote the benefits of effective risk management and lead by example in embedding the risk management framework
- Regularly discuss and review the corporate risk register and associated risk reports.

Chief Officer Risk Management Group (CORMG)

On behalf of Summit Group:

- To review and scrutinise all Corporate and Red Departmental Risk Register on a quarterly basis or more regularly if required.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Add space between paragraphs of the same style, No bullets or numbering

- To assure the Summit Group that there are robust and effective risk mitigation strategies and actions in place to manage these risks.
- To review any risk, which is recommended by a Chief Officer, to be added to the corporate risk register and make a recommendation to the Summit Group for inclusion/non-inclusion.
- To receive suggestions made by the Audit and Risk Management Committee on areas of corporate risk that need further consideration.
- To keep under review the outcome of the Audit and Risk Management Committee Risk Challenge sessions and consider any wider corporate lessons learnt.

Chamberlain (the City Corporation's lead officer for risk management)

- Overall leadership for the effective delivery of the City Corporation's risk management function in accordance with industry best practice.
- Ensure the risk management framework is aligned and embedded with the City Corporation's approach to and disciplines for sound corporate governance and strong internal control.
- Advice on the development of the City Corporation's risk management framework
- Review and sign off updates to the City Corporation's risk management framework.

Chief Officers

(Extract from Financial Regulations 2021)

Chief Officers must have regard to the requirements and /or guidance issued by the Chamberlain and adhere to the City's Risk Management Policy and Strategy.

Specifically, Chief Officers are responsible for:

- Ensuring that risk management is integrated into business planning, programme and project management and finance planning.
- Ensuring that there are appropriate management arrangements for the continuous identification, assessment, mitigation, monitoring and reporting of risk within the department.
- Maintaining corporate and departmental, service, team risks on the corporate risk system and use system generated reports for management and Committee reporting purposes.
- Reporting their corporate and departmental level risks to their relevant Committee(s) in accordance with the Guidance on reporting risk information to ~~Grand~~Grand/Service Committees.
- Appointing a senior officer to act as the departmental risk co-ordinator to promote effective risk management within the department, liaise with

the Corporate Risk Manager and ensures it complies with the City Corporation's Risk Management Policy and Strategy.
- Reducing the risk of significant service disruptions by ensuring that they have in place appropriate and robust business continuity plans.

Departmental Management Teams (DMT)

- Ensure adherence with the Risk Management Policy and Strategy
- Champion the benefits of effective risk management
- Take ownership for risks within their function and ensure risk registers are regularly discussed, reviewed, updated and escalated as appropriate

Service Managers

- Manage risks effectively in their service area, in accordance with the risk management framework
- Ensure their staff have appropriate understanding and training on risk management
- Champion the benefits of risk management across their service and communicate the corporate approach to managing risk.
- Escalate serious risks to the departmental management team as appropriate.
- identify training needs; and
- Take account of risk management issues when setting staff performance targets.

Risk Management Group

To assist in developing and embedding the City of London Corporation's risk management framework, promoting the development of consistent and effective risk management across the organisation. This Group provides a forum to share best practice relating to the identification, monitoring and mitigation of risk.

Departmental risk co-ordinators

- Provide risk management support for their functions
- Cascade, communicate and promote the risk management framework as directed by the Corporate Risk Manager to drive consistency across the organisation on the management of risk.
- Attend Risk Management Group meetings.
- Support updating of departmental risks on to the corporate risk management information system.

Corporate Risk Manager ·

- ~~Develop guidance, tools and training to support the business to manage risk effectively in accordance with the risk management framework.~~
- Embed the Risk Management Policy and Strategy and process to drive consistency in its application.
- Develop guidance, tools and training to support the business to manage risk effectively in accordance with the risk management framework.
-
- Provide support and training on the risk system and wider risk training.
- Provide assurance, support and challenge to the business on all areas of business risk management.
- Report on corporate and other risks to the Audit and Risk Management Committee and support the work of the Committee in its risk management role.

Programme and project managers must:

- Follow the Project risk management guidance which is now part of~~.~~ ~~(This is currently being developed as part of~~ the Project Management Academy project~~)~~. See Intranet

Risk owners must:

- seek out relevant expertise to help in the assessment of risk and appropriate control measures.
- review and report on the proximity and status of assigned risks.
- identify risk action owners for implementing control measures; and
- escalate risks to the ~~directorate~~ departmental or corporate level as and when necessary.

Risk action owners must:

- ~~put in place~~Implement actions to control risks, drawing on the advice of relevant experts.
- monitor risk and control measures; and
- feedback on the progress in implementing controls and their effectiveness.

Internal Audit is expected to:

- use risk assessment to inform its annual audit plan.

- carry out risk-based audits, evaluating controls and providing an opinion of levels of assurance.
- carry out periodic audits to test the suitability and implementation of the risk management framework; and
- make recommendations for improving risk management practices.

Employees ·

- understand the City Corporation's approach to risk management.
- make active and effective use of risk management in their work.
- Suggest new risks to their managers

SECTION 3 – Risk Management Process Guide

Introduction

This guide outlines the risk management process adopted and used by the City of London Corporation. It should be read in conjunction with the City Corporation's Risk Management Policy Statement and Strategy.

This guide will be useful for all staff to gain an understanding of the City Corporation's risk management process. For managers it should it help them to create some time and space to anticipate, plan effectively, act proactively and deliver on their objectives and report progress in managing risks to higher levels of management.

It outlines the definitions of risk and risk management as well as explaining the five key steps in the cyclical risk management process, the tools that may be helpful in each step which, includes the City Corporation's risk matrix as well as a glossary of terms.

This guide is supported by a range of tools and other resources on the Intranet risk management intranet site.

Where and when should risk management be applied?

Risk management can be applied to all business activities for example in setting strategic aims and objectives, organisational change, business planning, programme/project planning, options appraisals, procurement, commissioning, change programmes, improvements in services, projects and programmes.

The appropriate risk management approach depends upon the importance of the planned business activity to the achievement of City Corporation outcomes/ departmental objectives. The more important the planned business activity the more rigorous and robust the risk management approach needs to be.

The City Corporation's risk management framework sets out the formal process for the application of risk management to business risks.

The Risk Management process

What is 'risk'? Simply put a risk is a potential future event that could affect the delivery of one or more objectives. The City Corporation has adopted the following formal definition of risk[4];

"The effect of uncertainty on objectives"

This guidance focuses on the uncertainties which potentially could have a significant impact on the achievement of the City Corporation's objectives and

[4]ISO 31000:2018 Risk Management

the stakeholder's confidence in the way the City Corporation delivers its services (i.e. the uncertainties that matter).

In managing risk, the City Corporation seeks to minimise, though not necessarily eliminate, threats as well as maximise opportunities - (see the City Corporate's Rrisk Mmanagement pPolicy).

What is risk management?

Risk management is an umbrella term for the identification, assessment and control of risk. The City Corporation have adopted the following formal definition[5]:

> ***"coordinated activities to direct and control and organization with regard to risk"***

Risk management is a cyclical five-step process that sets out to control the level of risk and to reduce its effects.

The five-step risk management process is described briefly below but is set out in more detail later in this document.

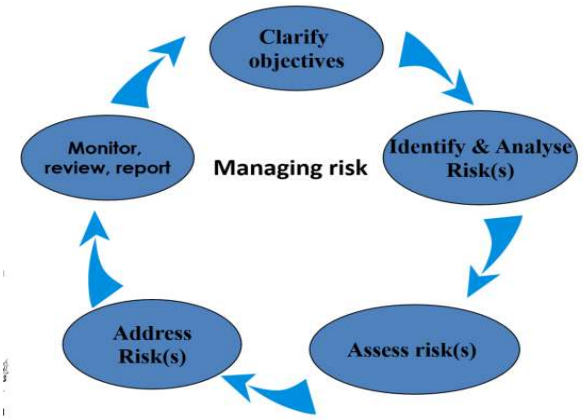


Fig 1 – The Five Step Risk Management process

Brief overview the steps in the risk management process

Clarify objectives: Understanding the context of the planned business activity (e.g. objectives within a business plan) is the first step – the aim being to provide sufficient information on what needs to be achieved. This would include, for example, ensuring that the objectives are clear, agreed and understood by all stakeholders, determining the level of detail required by the risk process, the degree of risk (how much risk do we want to take) of the planned business activity and strategic importance.

[5] ISO 3100:2018 Risk Management

Identify risks: This step involves identifying the risks that could adversely impact on the success of the planned business activity. Having clear and concise risk descriptions is essential for the following steps.

Assess risks: The significance of the identified risks should be assessed so they can be prioritised. Assessment is undertaken using the City Corporation's criteria for likelihood and impact (see appendix 3).

Address: This step involves developing actions that will influence either the likelihood or impact (or both) of the risks occurring. These actions need to be appropriate, achievable and affordable. The risk should be modified as a result of the actions taken.

Implement, Monitor and review: The identified actions must be implemented. Progress in managing risks as well as identifying new risks must to be assessed, monitored, and reviewed/reported regularly at management meetings and where appropriate at Committee meetings. If necessary, new risks and actions may be added and existing risks/actions removed.

How to apply risk management

This section provides guidance on the use of a risk management process that can be applied to activities at corporate, departmental, service and team levels within the City Corporation.

.

It needs to be applied sensibly and the level of risk management should be proportionate to the risks and the importance of achieving the planned objectives.

The five-step risk management process is explained detail below together with the tools that would be useful and the key outputs from each step.

To assist with a successful use of this process several ~~specific~~ tools have been produced. Information about each tool is included on the Risk Management Intranet page on ColNet.

Step 1: Clarify Objectives

It is difficult to think about risks in isolation, so the first step is to be clear about the objectives and key deliverables and other internal and external factors that may affect the delivery of the planned activity.

This will include an understanding of:

- The planned activity's objectives and what success will look like.
- The scope of the activity.
- The assumptions that have been made.
- The internal and external stakeholders and their relative influence

- The external factors that might affect the planned activity
- The City Corporation and its capabilities, as well as its objectives and strategies that are in place to achieve them.

Tools

The tools that will be helpful include:

- PESTLE (Political, Economic, Social, Technological, Legal and Environment) analysis (External risks)
- SWOT (Strengths, weaknesses, opportunities, threats) analysis (internal risks). This will help highlight potential risk areas that need to be addressed.
- Stakeholder Analysis - a method of identifying the key stakeholders and their influence over the planned activity.

See the Intranet risk management intranet site for more information.

Reference to internal compliance documents such as financial regulations, contract regulations as well from external sources – regulations, best/ practice guidance, professional/industry standards etc may also be useful at this stage.

The key output from this stage should be a clear understanding about the activity's objectives, some of the key external and internal issues including stakeholder concerns and the likely risk management approach required.

Step 2: Identify (and Analyse) risks

The risk identification step is focussed on the risks (positive or negative) to achieving the planned activity's objectives.

Consultation is likely to be needed with staff/managers who have a good understanding of the business activity and other stakeholders, asking the following questions:

- What might prevent the achievement of the stated objectives?
- Has it gone wrong before?
- Who should own this risk?
- When should we start managing this risk?
- How and when can the risk happen?

It may also be helpful to think about the sources of the risk for example, the introduction of new legislation/regulation, budget savings, new technology, and new ways of working, may all give rise to risks. Using the headings as a prompt to think about the things that could get in the way will be a fruitful way to identify risks.

An example prompt list to identify risks is set out below.

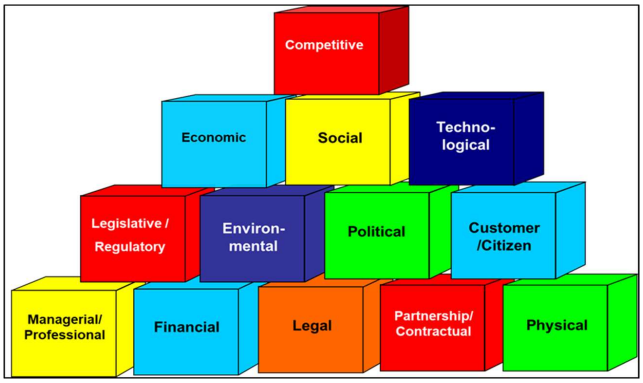


Fig 2 – Example risk prompt list

During the identification stage the following information needs to be gathered:

- A set of risks that have been described clearly and plainly, using the cause, the 'risk event' and the potential effects statement. An example is set out below:

  Risk Title: Minibus fleet

  Cause: As a result of lack of capital funding to replace the ageing minibus fleet

  Risk event there is a risk that current vehicle reliability levels will fall in the next 12 months,

  Effects: leading to higher vehicle maintenance costs, increased pressure of revenue budgets, client service disruption and increased vehicle hire costs,

- The nature of the risk – for example, political, financial, reputation, and more; and
- The name of the individual taking responsibility for the risk (i.e. the risk owner).

Tools
There are various tools that can be helpful identifying risks including horizon scanning, risk check lists, prompt lists, one to one interviews with key staff. See Intranet - Risk Management page.

The key output is a list of risks (described in the cause- risk event -effect statement) produced that are aligned to the planned activities objectives and

each with a named risk owner. Risks should be recorded on a risk register. The City Corporation uses a risk management information system to record and report its business risks.

Step 3: Assess Risks (4x4)

Every risk should be assessed to help determine how much management attention is given to managing the risk. This is done by ranking the risks with a set of scores determined by their individual likelihood (how likely is it for that risk to occur?) and impact (what is the consequence of the risk occurring?) rating.

The City of London Corporation uses a 4-point scale and the multiple of the likelihood and impact give us the risk score, which is used to determine the risk profile. This is explained in the quick risk management guide ~~location~~ on the risk management page - Intranet

Scoring risk is best done with those stakeholders who have a good understanding of the planned activity and coming to a consensus. Scoring risks in this manner can help avoid bias and improve ownership of the identified risks.

Risks need to be scored based on current risk (i.e. the risk score as of today and considering existing controls) and target risk score (the target risk score to be achieved by a certain date after the completion of all related actions). Both risk (current and target) scores need to be added on the risk register.

By plotting the current risk score on the risk matrix (Fig 3 below) it is the possible to determine a ranking by risk score of the identified risks. The more important the risk, the more management action will be required.

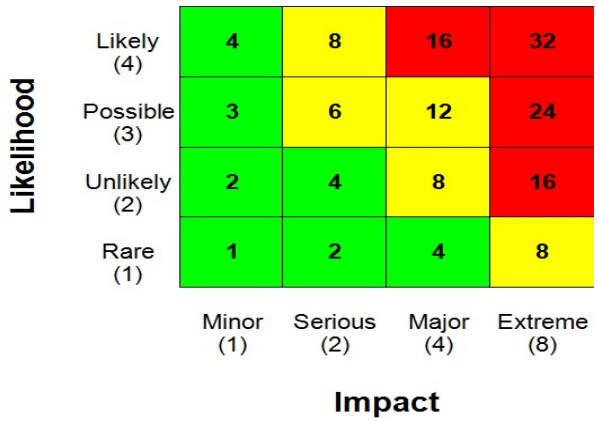


Fig 3 – The City Corporation's risk matrix (see appendix 3)
The red, amber and green (RAG) ratings have the following meanings:

- Red - Urgent action required to reduce rating.
- Amber - Action required to maintain or reduce rating.
- Green - Action required to maintain rating

Tools

The key tool to use is the City Corporation's risk matrix (see appendix 3).

The key outputs from this stage include a list of risks with a scored level of risk added to the risk register, and a consequent understanding of their relative priority for further action.

Step 4: Address Risks

Without this step, risk management would be no more than a bureaucratic process. Addressing risk involves taking practical steps to manage and control it.

Not all risks need to be dealt with in the same way. The common risk responses are outlined below should help in considering the range of management responses available when responding to risks.

Importantly, when agreeing actions to control risk, consideration is required on whether the actions themselves introduce new risks (i.e. consequential risks).

Management responses

When managing risks, the actions that are put in place should help to effectively reduce the risk to a manageable level.

There are four approaches that can be taken when deciding on how to manage risks:

Accept: An informed decision to accept the likelihood and consequence of a particular risk, ~~e.g.~~e.g., the ability to do anything about some risk may be limited, or the cost of taking any action may be disproportionate to the potential benefit, or in terms of the City Corporation risk appetite the risk may be manageable.	**Transfer:** Shifting the responsibility or burden for the loss to another party, e.g. through insurance. Note this should be used with caution -- it is often impossible to transfer a risk entirely. This is particularly true where a service is outsourced. The operational and financial risks may lay with the contractor. In the event of poor service there may be a reputational impact on the City Corporation.

Avoid:	Reduce:
An informed decision not to become involved in a risk situation. For example -the City Corporation may not be out to avoid risks associated with its statutory functions.	A selective application of management action, by applying internal control to reduce either the likelihood or the impact, or both, designed to contain risk to accept levels, e.g. mitigation action, contingency planning.

In most cases, the chosen option will be Reduce.

Identifying actions – Reduce option response

All risks identified and assessed need to be reviewed to determine what actions need to be put in place to mitigate them (either to prevent them occurring or lessen the effect).

There could be several actions identified for each risk – usually no more than 4 or 5- which will help reduce the risk. Actions should be written as a SMART statement for inclusion in the risk register. For example: "Prepare a detailed communication plan for approval by the project manager by (insert date)."

For each action there needs to be an action owner, that is someone responsible for one or more actions needed to mitigate the risk and to report on progress, usually to the risk owner.

Effective risk management is taking well thought through risks and balancing them against the benefits and costs.

Tools
The tool to be used in this process is the above table which shows the options for treating a risk and describing action using the SMART (Specific, Measurable, Achievable. Realistic and Time bound) statement.

The key outputs from this stage are that a completed risk register will have been produced showing the related actions to each risk with an identified risk owner. The register may also show where risks are complex and may require additional actions. As a result, there will be an overall appreciation of the total risk exposure of the planned business activity.

Step 5: Monitor, Review and Report

The primary purpose of this stage is to ensure that the planned actions are implemented, monitored for effectiveness and corrective action is taken where responses do not match expectations. ~~They must also be reported to the appropriate management level or Grand Committee, where appropriate.~~

Both risks and the effectiveness of their related actions can and do change. It's important to ensure that they are regularly reviewed and amended to meet the changing risk environment. New risks and actions may be required to address new threats identified at this stage.

At the same time as reviewing the risks it can be helpful to check the corporate and departmental performance indicators as they can act as an early warning of a risk increasing or decreasing.

Tools
The key tool will be the completed risk register together with the report format used for reporting risk information to senior management and where appropriate ~~Grand~~Grand/Service Committees. For more information about the Pentana Risk system for recording and reporting risks please contact the Corporate Risk Management on ext 1297.

The key outputs from this stage are that risks, and related actions have been thoroughly reviewed and amended as appropriate. This may result in some existing risks and actions being removed or new risks/actions being added. It also provides a~~A~~ssurance that the actions, currently being undertaken, are effective and making good progress in line to the target completion date.

In addition, the risk register has been reported in a timely manner to the appropriate levels of management and where appropriate to the relevant ~~Grand~~Grand/Service Committee. There is guidance for Chief Officers for reporting their corporate and departmental level risks to their appropriate ~~Grand~~Grand/Service Committee.

References:

This revised guide draws upon the City Corporation's Risk Management Strategy 2014 as well as best practice and various internal and external publications including CoL financial regulations, the ISO Risk Management:2018, HM Orange Book (2004 and 2019/2020) and HM (OGC) Management of Risk 2010 and other public sector risk management guides.

Appendix 1

Glossary

Acceptance - an informed decision to accept the likelihood and impact of a risk, e.g. the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit, or in terms of the City Corporation risk appetite, the risk may be manageable,

Action owner – An action owner is the individual assigned for the implementation of the measures to mitigate the risk. They support and take direction from the risk owner. Action owners are responsible for:

- reviewing and implementing controls assigned to them and updating progress on the risk register.
- regularly reporting on progress to the risk owner via, for example, team meetings and/or one to one meeting or as required

Avoidance - an informed decision not to become involved in a risk situation. (Note:The City Corporation may not be able to avoid risks associated with its statutory functions).

Business risk - Failure to achieve business objectives/benefits

Contingency plan(ning) - The process of identifying and planning appropriate responses to be taken when, and if, a risk occurs.

Exposure - The susceptibility to loss.

Frequency - A measure of likelihood expressed as the number of occurrences of an event in each time.

Impact - Effect or consequence of a risk, should it occur e.g. time, cost, quality, reputation, financial loss, reputation etc

Incident - An event or circumstance which could have or did lead to unintended and/or unnecessary harm to a person, and/or a complaint, loss or damage.

Issue - A relevant event has happened, was not planned and requires management action. It could be a problem, query, concern, change request or risk has occurred.

Likelihood - A qualitative description of a probability or frequency of the risk event occurring.

Loss - A negative outcome.

Mitigating action - Any controls or measures that seek to reduce the likelihood or impact of a risk event to an acceptable level.

Opportunity - An uncertain event that could have a favourable impact on the objectives or benefits

Planned (business) activity - a term to describe an activity (e.g. activities in a business plan) to which the risk management process is being applied.

Programme - A set of projects and activities that are co-ordinated and managed as a unit such that they achieve outcomes and realise benefits.

Project risks - Those which are concerned with delivering defined outputs to an appropriate level of quality within agreed time, cost and scope constraints.

Reduction - A selective application of management action, by applying internal control to reduce either the likelihood or the impact, or both, designed to contain risk to acceptable levels, e.g. mitigation action, contingency planning.

Risk - The effect of uncertainty on objectives

Risk analysis - A systematic use of available information to determine how often specified events may occur and the magnitude of the impact.

Risk appetite - an organisation's unique attitude towards risk taking that in turn dictates the amount of risk that it considers acceptable in pursuit of ots objectives.

Risk assessment - The identification of risk, the measurement of risk, and the process of communicating about risks.

Risk categories - Risks can be identified by category ~~e.g.~~e.g., technological risks

Risk cause: a description of the sources of the risk ~~i.e.~~i.e., the event or situation gives risk to the risk.

Risk effect: a description of the impact that the risk would have on the organisational activity should the risk materialise.

Risk event: A description of the area of uncertainty in terms of the threat or opportunity ~~(i.e. what activates the threat).~~

Risk identification - The process, by which events, which could affect the organisation's objectives, are identified, described and recorded.

Risk management – Concerned with the "coordinated activities to direct and control and organization with regard to risk".

Risk management framework - Sets the context within which risks are managed in terms of how they will be identified, assessed, controlled and reported.

Risk matrix - A model that visually displays the relationship between the likelihood and impact of specific risks. Visually it is a 4x4 box that plots likelihood and impact. (see appendix 3)

Risk owner - is a role or an individual that is responsible for the management and control of all aspects of that risk, including the implementation of the measures taken to mitigate it.

Risk prioritisation - The process that allows risks to be ranked into a logical order by establishing how significant they are in terms of likelihood and impact.

Risk register - A record of all identified risks relating to corporate, departmental, service, programme or project objectives.

Risk treatment - Selection and implementation of appropriate options for dealing with risk.

RMIS - Risk management Information System. A web-based system that can record risks and action and produce reports (within the City Corporation – Pentana Risk~~Performance~~).

SMART – An action must be specific, measurable, achievable, realistic and time bound.

Stakeholder - An individual, group or organisation that can affect, be affected by, or perceives itself to be affected, by a planned business activity.

Target risk – The risk score that the organisation wishes to reduce the risk to (i.e. target risk score) after the completion of all related actions and achieved by a certain date.

Threat – An uncertain event that could have a negative impact on objectives or benefits.

Transfer - Shifting the responsibility or burden for the loss to another party, e.g., through insurance. Note this should be used with caution - it is often impossible to transfer a risk entirely. For example, if the risk to the City Corporation's reputation, notwithstanding that a contractor is obliged to compensate the organisation financially for poor performance, the risk cannot be considered as well managed

Uncertainty - A condition where the outcome can only be estimated.

Appendix 2

Characteristics of a corporate risks

The Chief Officer Risk Management Group will assess potential new risks, using the following characteristics of a corporate risk, before determining whether to recommend to Summit Group that a risk should be added to the corporate risk register.

A corporate risk is likely to have one or more of the following characteristics:

- strategic and cross-cutting, with the potential to impact on a range of different areas or statutory functions.
- related to the organisation's ability to successfully deliver one or more high priority corporate objectives/outcomes (there needs to be a significant link to the outcome at risk).
- affects the outcomes sought from one of the organisation's major programmes.
- operates over the medium or long-term; (note –occasionally short-term risks may be added where there is demonstrable business case)[6]
- has the potential to seriously impact upon the organisation's capacity, for example by limiting, reducing or failing to maximise financial, physical assets or human resources.
- linked to the organisation's ability to successfully deliver transformational change and major initiatives, while continuing with business as usual.
- concerned with the wellbeing of the residents, businesses, the public and staff.
- may impact significantly and broadly on the organisation's reputation.
- The speed of the impact(s) if the risk occurred on the organisation.

Characteristics approved by Summit Group 19 December 2019

[6] Guide to short, medium and long term time frames: Short term <1 year; Medium term 1-5 years and long term > 5 years

City of London Corporation Risk Matrix (Black and white version)

Note: A risk score is calculated by assessing the risk in terms of likelihood and impact. By using the likelihood and impact criteria below (top left (A) and bottom left (B) respectively) it is possible to calculate a risk score. For example a risk assessed as Unlikely (2) and with an impact of Serious (2) can be plotted on the risk scoring grid, top right (C) to give an overall risk score of a green (4). Using the risk score definitions bottom right (D) below, a green risk is one that just requires actions to maintain that rating.

(A) Likelihood criteria

	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)
Criteria	Less than 10%	10 – 40%	40 – 75%	More than 75%

(C) Risk scoring grid

Likelihood	X	Impact: Minor (1)	Impact: Serious (2)	Impact: Major (4)	Impact: Extreme (8)
	Likely (4)	**4 Green**	**8 Amber**	**16 Red**	**32 Red**
	Possible (3)	**3 Green**	**6 Amber**	**12 Amber**	**24 Red**
	Unlikely (2)	**2 Green**	**4 Green**	**8 Amber**	**16 Red**
	Rare (1)	**1 Green**	**2 Green**	**4 Green**	**8 Amber**

(B) Impact criteria

Impact title	Definitions
Minor (1)	**Service delivery/performance**: Minor impact on service, typically up to one day. **Financial:** financial loss up to 5% of budget. **Reputation**: Isolated service user/stakeholder complaints contained within business unit/division. **Legal/statutory**: Litigation claim or find less than £5000. **Safety/health**: Minor incident including injury to one or more individuals. **Objectives**: Failure to achieve team plan objectives.
Serious (2)	**Service delivery/performance**: Service disruption 2 to 5 days. **Financial:** Financial loss up to 10% of budget. **Reputation:** Adverse local media coverage/multiple service user/stakeholder complaints. **Legal/statutory**: Litigation claimable fine between £5000 and £50,000. **Safety/health**: Significant injury or illness causing short-term disability to one or more persons. **Objectives:** Failure to achieve one or more service plan objectives.
Major (4)	**Service delivery/performance**: Service disruption > 1 - 4 weeks. **Financial:** Financial loss up to 20% of budget. **Reputation**: Adverse national media coverage 1 to 3 days. **Legal/statutory**: Litigation claimable fine between £50,000 and £500,000. **Safety/health**: Major injury or illness/disease causing long-term disability to one or more people **objectives:** Failure to achieve a strategic plan objective.
Extreme (8)	**Service delivery/performance**: Service disruption > 4 weeks. **Financial**: Financial loss up to 35% of budget. **Reputation**: National publicity more than three days. Possible resignation leading member or chief officer. **Legal/statutory**: Multiple civil or criminal suits. Litigation claim or find in excess of £500,000. **Safety/health**: Fatality or life-threatening illness/disease (e.g. mesothelioma) to one or more persons. **Objectives:** Failure to achieve a major corporate objective.

(D) Risk score definitions

RED	Urgent action required to reduce rating
AMBER	Action required to maintain or reduce rating
GREEN	Action required to maintain rating

Contact the Corporate Risk Manager for further information. Ext 1297

Version date: January 2020