GREATER**LONDON**AUTHORITY

Finding the right balance:

The GLA's framework for managing risk

Date of approval and issue	October 2025
Approved by	Corporate Management Team
Changes from previous version	• Added 'future' into the Risk definition. • 'Positive' principle added to Risk management principles. • Change of 'Tier 2' risks to 'Directorate' risks to align with the Portfolio Management Framework's (PMF) levels of risks • Continual Improvement section, including Appendix 2 Questions to ask – taken from HMT's Orange Book - has been added. • Appendix 3 Risk categories – taken from HMT's Orange Book - has been added. • Risk score grid, x and y axis have been swapped, so Probability is now x axis, and Impact is now y axis. • Financial figures for capital and revenue have been added into the Impact Criteria Scoring table. • An 'Issue' definition has been added. • Portfolio risk management section – taken from HMT's Orange Book - has been added. • Levels of risk section – with escalation and de-escalation routes – has been added. • Other minor and factual updates.
Review date	October 2027
Senior owner	Chief Finance Officer
Document owner	Head of Performance & Governance

Contents

Foreword

In a city as dynamic as London, uncertainty is a constant. Threats emerge and fade—some from external forces, others from within our own operations. These uncertainties are what we define as risks: risks to London, to the GLA, to our directorates, units, programmes, and projects. Their nature may be unpredictable, but their impact can be profound.

Our decisions and actions carry consequences—both intended and unintended—that extend beyond the outcomes we aim to achieve. While we cannot eliminate uncertainty, we can manage it. By applying best-practice risk management principles, we equip ourselves to anticipate, prevent, and mitigate risks effectively.

Good risk management is not about avoiding risk altogether. It's about enabling bold, confident delivery while maintaining the agility to adapt. It provides a framework that helps us strike the right balance—between innovation and caution, between cost and benefit.

This framework is built on a core principle: risk management must be owned and applied by managers at every level - and understood by all staff. It is not a function delegated to the corporate centre, but an integral part of our everyday decision-making and delivery. It is embedded in how we work—not an add-on, but a foundation.

I trust this framework will support you in navigating uncertainty with confidence, helping you to deliver for London while safeguarding what matters most.

Our approach is kept under review so, if you have ideas about how it could be improved, do contact the Performance & Governance Team.

Fay Hammond
Chief Finance Officer and GLA Risk Management Champion

Section 1: The GLA's approach to managing risk

Why a risk management framework?

Serving a major world city is fraught with uncertainty – with the possibility that things could turn out differently from our expectations, for the better or worse, in other words, with risks.

A risk is defined as:

> *an uncertain **future** event or set of events that, should it occur, will influence the achievement of our objectives*

We cannot avoid or eliminate risk entirely. Moreover, to attempt to do so would be prohibitively costly – in money, time and opportunities foregone. But we can manage risk. We can identify and understand how, where and when threats and opportunities might arise. We can influence the likelihood of a given risk arising, together with the nature and extent of the impact. And we can consider when and how much calculated risk to take given the rewards at stake. Looked at another way, risk management helps us to act proactively to make the most of our circumstances.

The benefits of sound risk management, and the outcomes sought from GLA risk management practices, are:

- a broader and deeper understanding of our operating context
- a reduced incidence and impact of threats, (i.e., negative risks)
- an enhanced ability to seize opportunities, (i.e., positive risks)
- a sharper assessment of the trade-offs between risk and reward, cost and benefit
- better informed decision making
- a corporate culture that promotes innovation, new ways of doing things, and organisational learning, and ultimately
- improved outcomes for London and Londoners.

This document helps us realise these benefits by:

- communicating the value derived from, and the importance the GLA places on, effective risk management
- setting out eleven principles to underpin the GLA's approach to risk management
- highlighting the practices and mechanisms that are at the core of the GLA's risk management framework
- being clear about what the GLA expects of its staff – our roles and responsibilities – in managing risk
- providing practical guidance, grounded in best practice, for staff to follow.

Risk management is one of a number of disciplines we use to determine strategy, implement Mayoral objectives and make the best use of our resources – while acting properly and transparently. It is therefore closely related to and interwoven with corporate governance, business planning and performance management. It also has close links with other GLA policies and guidance, including those for portfolio and project management, procurement, partnerships, information governance, data quality and business continuity.

The GLA's risk management principles

The principles below underpin the GLA's risk management framework. They are both practical and aspirational: practical because they inform and guide our approach to risk management; aspirational in that they are objectives for us to progress towards.

- **Embedded** – Risk management is an integral part of decision making; interwoven with governance, business planning and performance management disciplines; and rooted in and an influence on the GLA's culture.
- **Dynamic** – Risk management is ongoing and continuous, operating vertically and horizontally at different levels and across different areas.
- **Proactive** – Risk management is not seen as a compliance activity; rather it is actively used to look forward, to take charge of events and circumstances, and to mitigate threats and seize opportunities.
- **Proportionate** – Risk management focuses on the things that matter, adds value and helps ensure controls are commensurate with potential threats.
- **Enabling** – Risk management helps the organisation to be agile, to innovate, to take calculated risks and to learn from successes and mistakes alike.
- **Owned** – Risk management is owned and driven by everyone, but there are also clear and specific accountabilities for risk management processes, for individual risks and for their associated actions.
- **Communicated**– The importance the organisation places on risk management is effectively communicated, and different areas of the business talk to each other about shared and cross-cutting risks.
- **Understood** – There is a shared understanding of the GLA's approach to risk management, of the organisation's appetite for risk and the range and nature of risk it faces, and of strategies for minimising threats and maximising opportunities.
- **Robust** – GLA risk management practices are coherent, accord with best practice and are supported by helpful and practical guidance.
- **Evaluated** – The efficacy of the GLA's management of risk and the risk management framework are regularly reviewed, leading to improved approaches and practices.
- **Positive** – Risk management fosters a culture where taking informed and responsible risks is encouraged, supported by open dialogue, trust, and a shared commitment to learning and continuous improvement. This culture recognises risk as an opportunity for growth and innovation, not just a threat to be avoided.

Looking at risk from different perspectives

Risk is ever present. It exists within and across all those areas in which we seek to make a difference for London and Londoners. And it operates at and spans different levels. So, our risk management approach must also be holistic and cross-cutting.

This framework identifies four specific levels, or perspectives, as a focus for risk management.

Corporate risks

The GLA's most significant risks, which have the potential to impact extensively on the capability and vitality of the Authority as a whole.

A corporate risk is:

- strategic and cross-cutting, often with the potential to impact on a range of different areas or functions.
- related to, and has a significant impact on, the GLA's ability to successfully deliver Mayoral objectives and Assembly priorities.
- operates over the medium or long-term.
- has the potential to significantly enervate the organisation's capacity, for example by limiting, reducing or failing to maximise financial 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 Londoners and/or GLA staff.
- may impact significantly and broadly on the GLA's reputation.

The number of corporate risks should vary depending on the GLA's risk profile. But in normal circumstances it is helpful to think of corporate risks as the most serious risks faced by the Authority.

Corporate risks are captured on the corporate risk register, which is owned by the Corporate Management Team (CMT). The approach to corporate risks sets the context for decisions at other levels of the Authority.

The process for identifying and escalating corporate risks is as follows:

- every six months, the Performance & Governance Team meets with the Corporate Management Team to review and refresh the risk register in the round and identify any major changes required, including the addition of new risks.
- in parallel, risk leads – each risk has a lead CMT Member – co-ordinate a review of their risks, again supported by the Performance & Governance Team, involving senior members of staff.
- the Chief of Staff is also invited to provide input.
- the register is presented to the Audit Panel for its consideration.

While there is a formal, six-monthly refresh, senior managers should ensure risk management happens in real-time, with significant risks escalated up to the Corporate Management and

Mayoral Teams as and when they arise. This can also be undertaken through the corporate quarterly performance reporting.

Directorate risks

Directorate risks refer to the risks that sit below or outside the Corporate Risk Register and above programme risks and meet at least one of the following criteria:

- the risk impacts the directorate's ability to deliver its priorities and would have significant ramifications for the GLA corporately and reputationally.
- the risk is significant enough in its own right to warrant dedicated risk management arrangements.
- the risk is corporate in nature and has a decent probability of increasing to a level where it would be captured on the CRR.
- directorate risks operate over the medium to long-term.

Directorate risks will be reviewed by CMT on a six-monthly basis.

Programme risks

These are risks that relate to a specific GLA programme. They are likely to comprise a mixture of the most serious project risks (see below) and cross-cutting risks that could affect two or more of the projects within the programme. Each of the GLA's programmes must have a dedicated risk register, maintained by the programme manager. Risks should be reviewed by the programme board. A risk register template can be found on the intranet here.

Where programme risks impact on the delivery of the GLA's top priorities, they should be reflected in quarterly performance reports to the Corporate Management and Mayoral Teams.

Project risks

These risks relate to or flow from a specific project. A project risk has the potential to impact on the project's scope, outcomes, budget or timescales. Where the risk could impact on other projects or objectives, or the project is considered a high priority and the level of risk is such that it could lead to a failure to deliver project objectives, the risk should be escalated to the programme level.

All significant projects must maintain a 'project risk register', depending on the level of risk involved, or ensure the project risk is captured on a wider risk register.

Risks associated with decision making.

These are the potential risks that flow from a decision to pursue, or not to pursue, a particular course of action and which may impact on the delivery of the associated outcomes. Risk assessment at this level is likely to be at an early stage, forming the basis of future risk management at one or more of the levels above. Considering risk whenever significant decisions are made is a central plank of the GLA's approach to risk management. A template for articulating risks in decision forms can be found in the Decisions 'Top Tips' document here and should be used where there are several risks flowing from a proposal.

The different levels described above do not exist in isolation or in a strict hierarchy. Indeed, it is a fundamental principle of this framework that risk management is dynamic. Risks must be escalated from bottom to top according to the risk characteristics highlighted above, and in turn cascaded down for management action.

Furthermore, these are not the only levels at which risk operates. We all manage risk daily to achieve our personal objectives. Directors, heads of unit and team managers will want to put in place mechanisms to monitor and manage risks that cut across projects and programmes and/or operate outside programmes/projects at an operational, unit and team level.

Risk management and quarterly performance reporting.

Quarterly corporate performance reporting must capture top risks for each programme. These should not be simply those risks which are most severe, but instead risk reporting should be dynamic and bring any emerging and new risks to the fore. The Portfolio Management Framework (PMF) is mentioned in Section 2 and provides more guidance in this area.

The GLA's risk appetite

In many ways, risk appetite is the backbone to the GLA's approach to risk management. Without knowing how much and what types of risk are acceptable, we cannot expect to make sound decisions on the balance between risk and reward.

Risk appetite applies at the corporate, programme and project level. At the corporate level, it refers to the overall exposure to risk the organisation is willing to accept; and at the programme and project level to the level of risk beyond which a programme and project would not be considered viable.

When risk appetite is defined rigidly it can impede innovation and make an organisation overly cautious. It can also fail to reflect the complexity and diversity of decision making in an organisation such as the GLA. However, as general rules, the GLA:

- will not tolerate risks rated red on the risk scoring matrix where they are avoidable – other than in exceptional circumstances that should be formally documented.
- has a near zero tolerance for risks that cannot be mitigated to avoid the potential for a breach of law / formal regulation.
- has an extremely low tolerance for taking risk where there is the potential to actively cause harm to individuals or groups – all such risks should be avoided as far as possible.
- has a low tolerance for risks that might cause harm to the environment.
- is willing to operate in higher-risk environments, and take on a broader range of risks, to deliver Mayoral priorities and significant outcomes – but the GLA will seek to implement assurance mechanisms to manage and reduce consequential risks, including those to delivery.

Where a given project or programme is proposing to tolerate a high level of residual risk, the rationale must be outlined within the approving decision form.

The Corporate Management Team monitors risk exposure every six months as part of the periodic review of the corporate risk register. But the GLA also takes the view that risk appetite should be an integral part of strategic and financial planning and of decision making.

Below the corporate level, the guidance and tools that follow are designed to help managers and others consider risk appetite in a systematic way; by categorising and scoring risks. Risk

appetite should be considered at the very outset of project and programme conception – and especially within the formal decision-making process – and throughout delivery, actively guiding project and programme management.

An overview of the risk management process

Risk management is as much an art as it is a science. It relies first and foremost on good judgement. Yet by applying a recognised and methodical process, and grounding risk management in evidence-based analysis, we can increase our chances of identifying and managing risk successfully. Communication is necessary as an ongoing process to ensure risks are effectively identified and managed.

The GLA uses a four-stage process for managing risk. In summary, it involves:

- **identifying** what could happen.
- **assessing** the *probability* of a given thing happening and the extent of its potential *impact*
- **addressing** the risk by taking steps to reduce its probability or constrain its impact.
- **reviewing and reporting** on the efficacy of risk controls and mitigations.

Although the four stages are sequential, there will be times when it is necessary to return to earlier stages. As the diagram implies, the process should also be ongoing given that our risk environment is always changing.

The different stages, and techniques that can be used to support each stage, are explained in more detail in section 2 of this framework.

Putting the GLA's risk management framework into practice

Risk management cannot be effective if it is seen either as a function solely of the corporate centre or as a box ticking exercise. The GLA expects directors and managers, at team and project level, to take ownership of drive and review risk management within their respective areas using this document as a frame of reference.

Yet equally risk management will be ineffective if it is devolved entirely or if robust, rigorous and consistent practices and mechanisms are not in place.

This section highlights those practices, together with related roles and responsibilities, which form the spine of our approach to risk management. It also identifies how we will evaluate and review the success of our approach. In most cases roles and responsibilities are integrated within existing remits. But there are three roles that exist specifically to support effective risk management: a GLA risk champion, risk owners, and risk action owners.

All of us should:

- understand the GLA's approach to risk management.
- make active and effective use of risk management in our work.
- escalate risks to the project, directorate or corporate level as appropriate, via managers or, in the case of corporate risks, by liaising directly with the Performance and Governance Team
- provide feedback to the Performance and Governance team on the usefulness of the risk management framework.

The Corporate Management Team must:

- take an overview of and consider the top-level risks facing the authority, their likelihood and potential impact and the total quantum of risk faced by the authority.
- carry out horizon scanning and ensure there are early warning indicators.
- make active and ongoing use of risk management to effectively conduct the GLA's business.
- promote a culture in which risk management is used proactively, enables innovation and organisational learning, and is owned by everyone.
- help to review and monitor how much risk the GLA is willing to tolerate (the organisation's risk appetite)
- own the GLA's corporate risk register and formally review and refresh it every six months, facilitating the escalation of programme and project level risks to the corporate level.
- assign accountability for top level risks.
- cascade strategies for controlling risks.
- monitor the implementation of actions to improve risk management at the GLA, with progress formally reported to CMT at least annually.
- review and sign off major updates to the GLA's risk management framework.

The Chief Finance Officer (the GLA's risk management champion) must:

- ensure the risk management framework is aligned and embedded with the GLA's approach to and disciplines for sound corporate governance and strong internal control.

- review and sign off updates to the GLA's risk management framework.
- champion the importance of effective risk management across the Authority.

Executive and Assistant Directors must:

- work with their directorate management team to scan the horizon, put in place early warning mechanisms, and to take an overview of risk within their directorate.
- use information about risks to inform decisions (via the Decisions process), develop strategy and implement policy.
- champion and embed proactive, enabling and robust risk management practices within their directorate, in line with the risk management framework.
- review and monitor risk appetite for their directorate.
- lead strategies to address corporate risks within their directorate.
- ensure risk registers are held for all GLA programmes.
- assign responsibility for managing and controlling specific risks.
- serve as the primary link between risks emerging at the directorate level and the corporate risk register, cascading risks up and action down, including ensuring risks identified at the unit level through the quarterly performance reporting process are suitably reflected in and aligned to the corporate risk register.
- ensure top risks are reflected in quarterly corporate performance reports.
- monitor the implementation and efficacy of risk management within their directorate.
- annually, and in consultation with their departmental management team, provide assurance that risk management within their directorate is robust and in line with this Risk Management Framework.

Programme and project managers must:

- embed risk management, in line with the GLA's risk management framework, within the programme/project lifecycle to support project definition, approval, change control, decision making and delivery.
- agree risk appetite with the programme/project sponsor and the overall approach for managing and escalating risk.
- maintain a project/programme risk register (at least a mini risk-register for projects and a full risk register for programmes) and an overview of total risk exposure
- align risks with programme/project objectives and outcomes.
- assign clear accountabilities for risk, including risk owners and risk action owners.
- put in place early warning mechanisms.
- communicate clearly risks to stakeholders and ensure risk is comprehensively covered in project initiation documentation and monitoring reports.

- escalate risks to directors and senior managers where appropriate, and if the overall risk exposure or a specific risk is particularly serious, to the corporate risk register.
- seek out expertise to help effectively identify and control risks and
- maintain records of historic and current risk registers, forming an effective audit trail.

Other managers must:

- manage operational risk and the risks associated with policy implementation in accordance with the GLA's risk management framework.
- escalate serious risks to the directorate and corporate levels as appropriate, as well as advising when operational risk may impact on project delivery.
- use the GLA's competency framework and personal development plans to enhance risk management skills.
- identify training needs.
- take account of risk management issues when setting staff performance targets.

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.
- escalate risks to the directorate or corporate level as and when necessary.

Risk action owners must:

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

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.
- make recommendations for improving risk management practices.

The Audit Panel's remit includes:

- reviewing the outcome of audits, highlighted risks and officer responses
- reviewing the GLA's risk management framework documentation on a periodic basis

- reviewing and challenging the GLA's corporate risk register every six months.

The Performance & Governance team's remit is to:

- own the GLA's risk management framework documentation.
- ensure there is clear and robust guidance for managing risk.
- keep abreast of best practice and draw on Internal Audit recommendations to review and coordinate improvements to the risk management framework.
- communicate and promote the GLA's risk management framework through regular updates to staff via blogs and Internal Comms publications, including through the induction process and corporate governance e-learning.
- maintain a risk management intranet page.
- be available to provide support to those undertaking risk management.
- maintain and administer the corporate risk register and support CMT in ensuring it is comprehensive and accurate.
- report to CMT at least annually on progress in implementing any risk management actions.
- coordinate six-monthly reports to the Audit Panel on the corporate risk register.
- promote, integrate and reinforce risk management within other disciplines, in particular portfolio management, governance and decision making (via Mayoral, Director and Assistant Director Decision Forms)
- update associated risk documents on a regular basis, such as the list of fraud risks (as detailed in the Anti-Fraud & Corruption Policy and Response Plan), and biannual risk timetable.
- ensure there are clear and robust links between risk management and corporate performance reporting processes.

Continual improvement

Risk management shall be continually improved through learning and experience. Through this end, we commit to the following principles:

1. The GLA will continually monitor and adapt the risk management framework to address external and internal changes. The GLA will also continually improve the suitability, adequacy and effectiveness of the risk management framework. This will be supported by the consideration of lessons based on experience and review of the risk management framework and the performance outcomes achieved. Appendix 2 contains questions that will assist in assessing the efficient and effective operation of the risk management framework. These are taken from HMT Orange Book.

2. All strategies, policies, programmes and projects should be subject to comprehensive but proportionate evaluation, where practicable to do so. Learning from experience helps to avoid repeating the same mistakes and helps spread improved practices to benefit current and future work, outputs and outcomes. At the commencement, those involved and key stakeholders should identify and apply relevant lessons from previous experience when planning interventions and the design and implementation of services and activities. Lessons should be continually captured, evaluated and action should be taken to manage delivery risk and facilitate continual improvement of the outputs and outcomes.

3. As relevant gaps or improvement opportunities are identified, the GLA will develop plans and tasks and assign them to those accountable for implementation.

Section 2: A guide to managing risk

The guidance that follows is not intended to be a rigid instruction manual for managing risk. Different situations demand different approaches. But it does offer a process that can be adapted to different circumstances, together with tools and techniques that will help you at the different stages the risk management cycle. A risk register template is at Appendix A.

The risk management process is linear in the sense that each stage builds on the stages that preceded it. But, as the word cycle indicates, it is also ongoing. So, the different stages will need to be revisited at different times.

It is important to remember that risk management should not be conducted in isolation. Involving different people increases the range of perspectives and leads to a deeper understanding of the operating environment, risks and how best to control them. It is also vital to draw on the expertise available to you within the GLA and the procurement and legal functions provided by Transport for London.

Furthermore, risks are often 'shared'. That is, they flow from the work of and have the potential to impact on two or more organisations. In these instances, the process below should be undertaken collaboratively. In such circumstances, it is especially important that risk and action ownership is clear. It may on occasion be difficult to agree a shared view of or approach to risk. In such instances, the GLA should maintain its own risk register detailing how it ranks and is responding to the risks in question.

Stage 1: Identify

The first stage of the risk management process is, naturally enough, about understanding and identifying. There are three things to understand and identify at the outset of a given project, work-stream or when implementing risk management afresh. The first is the context within which the activity is taking place; the second is the level of risk appetite; and the third is the risks themselves – i.e. the uncertain threats and opportunities.

You should seek to:

- clarify the scope and objectives of the activity/project/work and the outcomes that are being sought.
- use tools such as horizon scanning and SWOT[1] and PESTLE[2] analysis to help understand the wider operating context, often organised by taxonomies or categories of risk (see Appendix 3)
- identify and understand constraints, assumptions and interdependences.
- produce an integrated and holistic view of risks.

[1] Considering Strengths, Weaknesses, Opportunities and Threats.

[2] Considering the context from Political, Economic, Social, Technological, Legal and Environmental perspectives.

- consider the flow of cause and effect and any unintended consequences that might arise from pursuing the outcomes[2]
- use common and generic areas of risk as a stepping off point for identifying specific risks.
- align risks to objectives so that at the next stage it is easier to establish their potential impact.
- involve a range of people with different perspectives and areas of expertise.
- establish a risk register and begin to record the risks.
- describe risks clearly and plainly, setting out the cause, the 'risk event' and the potential impacts.

This stage of the process is not just about identifying risks. You should also identify:

- the risk appetite for the project or work area – i.e. the total quantum of potential risk that is tolerable given the benefits and/or opportunities at stake.
- a risk owner for each risk
- tolerances to trigger reporting or escalation of risk to the programme board and director.

Some common types and sources of risk are set out below. The list is neither prescriptive nor exhaustive.

Areas of risk	
• Changes in government policy, legislation or regulation • Legislative breaches • Financial/funding threats and opportunities • Other limits on resources • Changes in the economic climate • Uncertainty arising from transformational change • Social or demographic flux • Technological change and failure • Environmental issues • Reputational impacts • Governance and internal control arrangements • Information governance	• Stakeholder and partner capacity and attitudes • Threats to the health and safety of employees and citizens • Business continuity and resilience issues arising from incidents such as fire, flood, terrorism and damage to buildings and/or plant • Organisational or service capacity and capability • Unintended consequences and externalities • Perverse incentives • Difficulties arising from working across organisational boundaries • Staff morale • Procurement • Shifting priorities • Changes in demand or citizen expectations

By the end of this stage, you should have:

- a partially populated risk register containing a long list of clearly articulated threats and opportunities with an owner for each.
- risk descriptions including cause, event, effect.
- an agreed risk appetite for the area of work that is clearly documented, including within relevant project documentation (such as the project initiation document)
- clear thresholds for escalating risks to those with ultimate accountability for the work
- an understanding of when and how to escalate risks to the directorate and corporate levels.

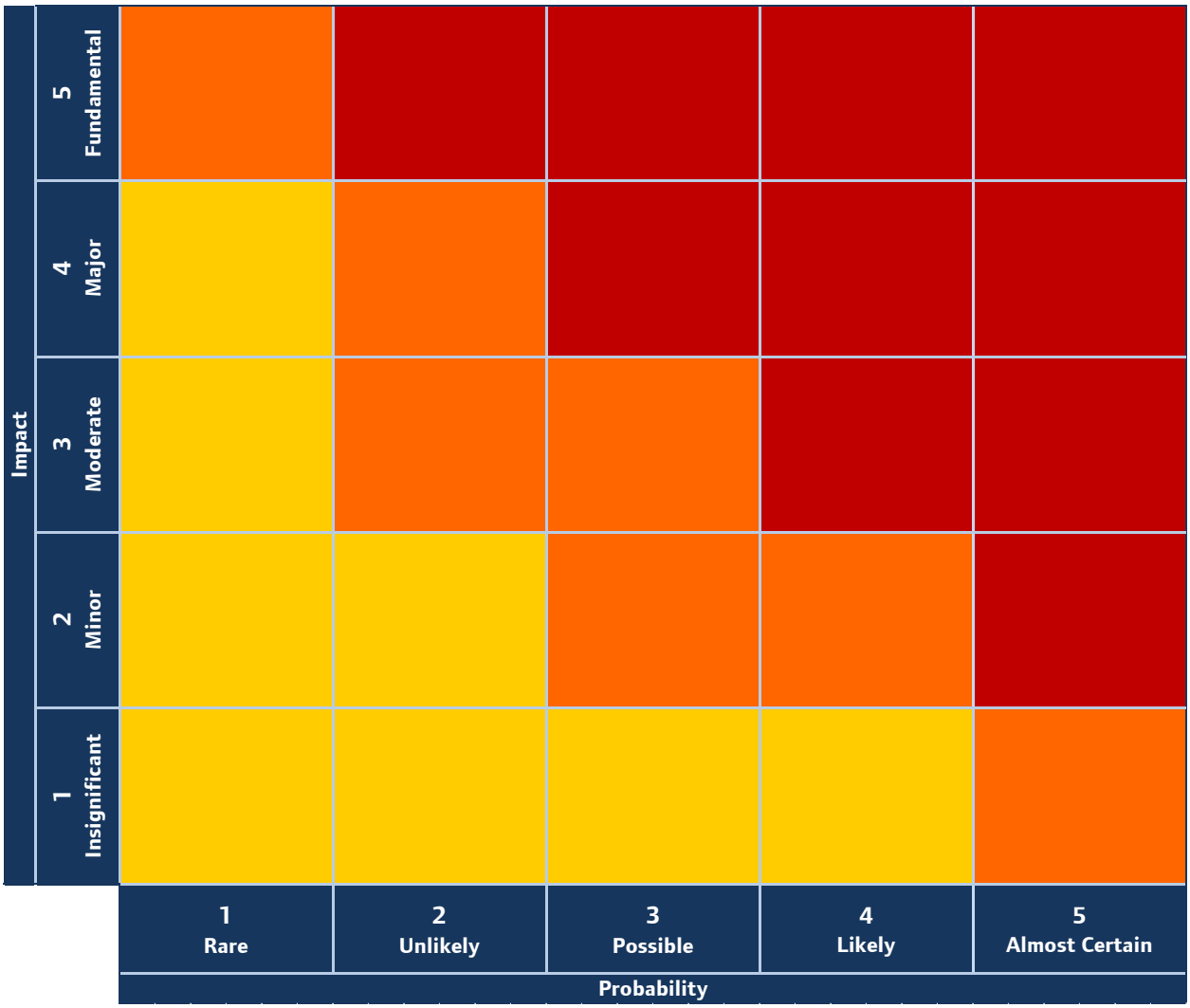
Stage 2: Assess

It is not enough to simply have a sense of the risks that might impact on a given area or activity. The risks need to be understood and prioritised. This involves assessing risks against two main dimensions:

- **probability**: the likelihood of a particular threat or opportunity occurring.
- **impact**: the estimated effect on one or more objectives of a particular threat or opportunity occurring.

There is also likely to be merit in undertaking a proximity assessment to estimate when a risk might occur.

Risks are assessed using a probability/impact grid. By plotting a risk against the two different dimensions we can derive a score and associated traffic light, and therefore understand the seriousness of individual risks and compare different risks. At this stage you are assessing the **inherent risk**; that is the probability and potential impact before any actions are taken to make the risk less likely to arise and/or to mitigate its impact if it does. You should draw on and develop the information gathered at stage 1.



The risk score is arrived at by multiplying the probability rating and the impact rating. Using the grid above, the possible scores therefore range from 1 to 25. The scores should be derived with reference to the following descriptors.

Probability scoring criteria		
Score	**Level**	**Descriptors** (lifetime of project or five-year period)
1	Rare	0 to 20 per cent chance of materialising
2	Unlikely	21 per cent to 40 per cent chance
3	Possible	41 per cent to 60 per cent chance
4	Likely	61 per cent to 80 per cent chance
5	Almost Certain	81 per cent to 100 per cent chance

Impact scoring criteria									
Score	**Level**	**Financial Impact**	**Health and Safety**	**Environment**	**Reputation**	**Legal/ Regulatory**	**Capacity**	**Schedule**	**Outputs and Targets**
1	Insignificant	Containable within budget (£1m capital, £250k revenue)	No significant injury	Temporary damage or degradation	Temporary loss of standing among partners/ stakeholders	Improvement/ prohibition notice	Short-term disruption or impairment to a non-critical work area / service	A delay of less than 10 per cent	Key target missed by up to 10% Lower priority output not delivered to the expected standard
2	Minor	Containable within overall budget (£2m capita,l £1m revenue)	Minor injury	Temporary and localised damage or degradation	Temporary loss of standing among partners/ stakeholders Minor local adverse media coverage or complaints	Improvement/ prohibition notice	Short-term disruption or impairment to a few non-critical work area / service	A delay greater than 10 per cent of original timescale	Key target missed by up to 20% Lower priority output not delivered
3	Moderate	Containable within overall budget but might require resources to be reprioritised (£20m capital, £2m revenue)	Moderate injury	Medium or long-term localised damage or degradation	Medium-term damage to reputation among partners Major local or minor London-wide adverse media coverage	Prosecution with fine	Short-term disruption or impairment to several non-critical work areas / services or to one critical work area / service	More than 25 per cent increase on original timescale or such that the work/project will fail to meet core objectives as a result of the delay	Key target missed by up to 30% Several lower priority outputs not delivered to expected standard Or Mayoral commitment not achieved
4	Major	Not containable within existing budget (£100m capital, £10m revenue)	Fatality or several major injuries	Long-term or permanent localised damage or degradation; or widespread short-term damage	Long-term damage to reputation among partners Significant London-wide, or national, adverse media coverage	Director charged Major compensation claims	Medium-term disruption or impairment to several non-critical work areas / services or to one critical work area / service	More than 50 per cent increase on original timescale or such that the work/project will be unable to achieve its primary purpose	Key target missed by up to 40% Numerous lower priority outputs not delivered Or significant underachievement against a key Mayoral commitment
5	Fundamental	Cannot be resourced, including within existing contingencies (£250m capital, £50m revenue or threatens the financial viability of the organisation as a going concern)	Several fatalities or numerous major injuries	Long-term or permanent widespread damage	Permanent damage to reputation among partners/ stakeholders, which constrains future action Significant adverse national media coverage	Director convicted Major compensation claims exceeding available cover Central government action	A fundamental impact on the GLA's ability to achieve its objectives or to meet the needs of its service users	More than 75 per cent increase on original timescale or such that the work/project will be unable to achieve its primary purpose	Key target missed by > 50% Numerous lower priority outputs not delivered Or significant underachievement against a key Mayoral commitment

The impact criteria above are neither exhaustive nor entirely prescriptive. Below the level of corporate risk, they are intended as a guide. You should always use the 5x5 scoring system – and apply it consistently – but at the same time you must take context into account. What is crucial is that risks are scored within the context they are reported. A risk may be 'red' in the context of a given project but escalated to the corporate risk register it may only be 'amber'.

You may wish to document your own descriptors at the start of the project.

By the end of this stage, you should have:

- a risk register that has been updated to include scores for the probability of each threat and opportunity materialising, the potential impact and the overall risk (remember, these are the **inherent** risk scores, i.e. before the impact of controls has been taken into account)
- an overview of the aggregate amount of risk exposure, for example by putting a financial value on risk impacts or creating a heat map (this involves plotting all the risks onto a probability/impact grid to understand how they are distributed)
- a clearer sense of whether a given activity or proposal has a favourable balance between risk and reward, i.e. whether to accept the risks given the benefits that may be accrued and/or the outcomes that are planned to be delivered.
- a hierarchy of risks, and an understanding of the urgency associated with individual risks, so that effort and resources can be directed effectively.
- a better understanding of which risks might need to be escalated to senior managers and the corporate level.
- an understanding of the correlation between risks.

Stage 3: Address

Prevention is better than cure. That is the crux of this stage of the process, and indeed risk management in general.

Putting in place effective controls to address risks relies on good judgement and thorough analysis, which can be aided by drawing on the advice of experts. That is because there is an obvious trade-off between the time and cost of putting in place risk controls and the benefit derived from reducing the probability and impact of a given risk. There is no value in investing in controls if there is not a commensurate benefit. And the most extensive control measures may not offer the best balance between cost and benefit.

The best response is the one which has the biggest impact on the level of risk exposure for the lowest cost. That means putting in place controls that are proportionate, economical, efficient, effective, timely, straight forward and practical.

The key steps at this stage are to:

- determine which risks need to be controlled.
- identify and implement control mechanisms that strike the optimum balance between cost and benefit.

- using the probability/impact grid, assess and record the **residual**[3] probability, impact and overall scores for each risk, taking into account the likely efficacy of control mechanisms.

- implementing the controls – to not do so would be to waste much of the time and effort expended up to this point.

The main methods for controlling risks are known as the 'four Ts'. You may wish to use a combination of these for a given risk.

Treat

Either the probability or the impact of the risk can be 'treated', as described below.

- Acting to reduce the risk probability by putting in place preventative controls is the most common response to risk. Examples include strengthening governance arrangements, putting in place new or more rigorous management practices, or enhancing quality controls.

- Acting to reduce the potential impact of a risk is about having a 'Plan B'. This should be your chosen response when you cannot economically lower the probability of the risk to a tolerable level.

- Putting in place measures to detect when undesirable outcomes have occurred. This approach is appropriate only when it is possible to accept the loss or damage incurred up to the point of identification. Examples include financial reconciliation, monitoring and post implementation reviews.

Treatment is likely to be more effective when both the probability and the potential impact are acted upon.

Transfer

Part or all the risk may be transferred to another party, normally at a cost. This can be done through partnership agreements and commissioning where others are better placed to manage the risk. Purchasing insurance will transfer the financial impact of a risk. Be careful to avoid transferring control of the risk without also transferring the potential negative impacts, for example reputational damage – particularly when that party has a lower capacity and capability for managing the risk than the GLA itself.

Terminate

In other words, eliminating the risk by not pursuing the activity in question. This could be done by changing the scope of the programme/project or the delivery mechanism. However, and unless done early on, this can be costly or difficult to achieve. It is likely there were good reasons for deciding on the original scope or delivery mechanism. And often it will not be a viable option, given political or regulatory considerations.

[3] While the residual risk rating is forward looking, in that it looks at the position once control measures are in place, you need to consider and be realistic about the likelihood of the controls being successfully implemented, in sufficient time and having the intended mitigating effect. If their success is uncertain, you need to reflect that in the rating.

Tolerate

This means accepting the risk without putting any controls in place, i.e. taking a calculated chance. This may be an appropriate response when:

- there is nothing that can be practically done to limit the risk.
- implementing control measures would shift the balance between costs and benefits from favourable to unfavourable.
- control of the risk is properly the responsibility of another party, for example central government.
- the risk is of low probability and negligible impact.

By the end of this stage, you should have:

- a residual probability and impact score for each risk
- a completed (but not static) risk register
- where risks are particularly complicated or involved, a risk response plan.
- escalated risks as appropriate to directorate and corporate levels
- a good sense of the total quantum of risk (and an updated heat map, if you created one) associated with the activity.
- where relevant, a sound basis for deciding whether overall benefits and rewards outweigh the potential threats and associated controls.

Stage 4: Reviewing and reporting

New risks will continue to emerge, existing risks will change in nature, and the perceived efficacy of controls will also change based on experience and evolving circumstances.

It is essential, therefore, that risk is reviewed and reported on a periodic basis, but also flexibly when there are significant changes in circumstances or key decisions to take. Risk review, like risk identification and assessment, should be a collaborative exercise drawing on input from risk and risk action owners and from others involved in the project or work area.

Risk review and reporting should be integrated with other monitoring and reporting mechanisms, to help identify linkages and ensure there is a comprehensive picture of progress and prospects.

Early warning mechanisms should also be monitored, and there may be merit in returning to some of those techniques deployed at stage 1, such as horizon scanning.

By the end of this stage, you should have:

- refreshed your environmental analysis, if there have been changes in the operating context.
- added and removed risks from the risk register.

- assured yourself that controls are in place or that good progress is being made to implement them.
- reviewed the efficacy and impact of controls and considered different approaches where necessary.
- refreshed risk assessments, both inherent and residual
- considered and where relevant amended the risk hierarchy.
- reassessed the overall level of risk, and in some cases risk appetite, associated with the activity.
- decided whether to escalate any risks to the directorate or corporate level.

Note that historic risk registers and associated reports should be retained for three years (rather than only the most recent being kept) to aid review of the efficacy of risk mitigation, facilitate project evaluation and serve as an audit trail. This requirement is also documented in the GLA's Records Retention and Disposals Schedule, on page 33, found here: GLA Records Retention Disposal Schedule table.pdf

Issues

In risk management an 'Issue' is no longer a future risk, but a risk that has materialised and is now causing measurable disruption or affecting operations, governance, or strategic outcomes.

More detail for issue management is found in the portfolio risk management section below.

Portfolio risk management

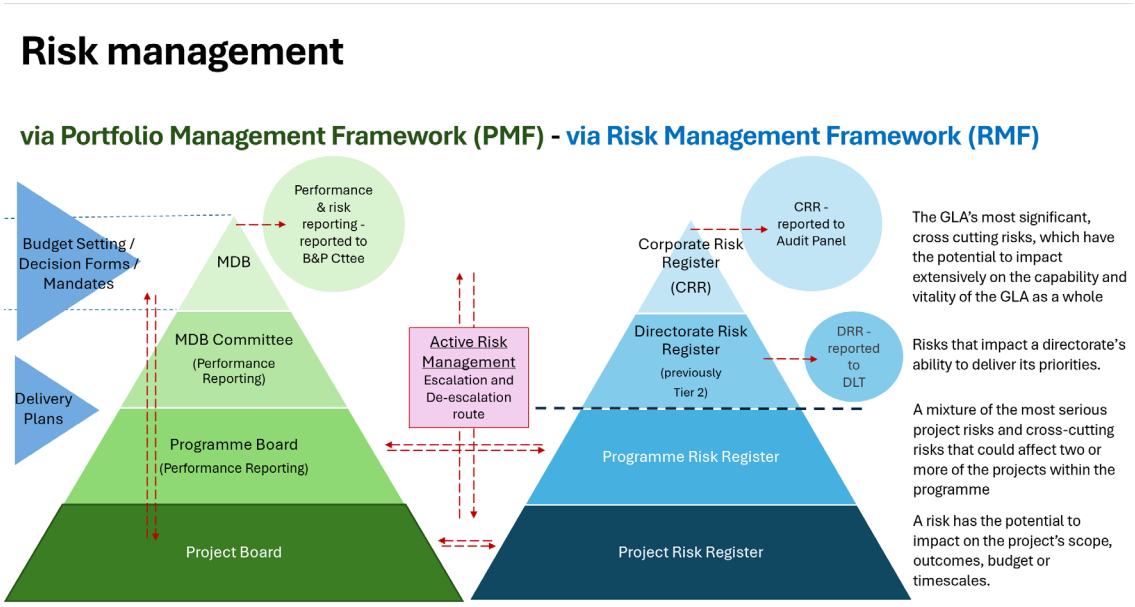
Taking well-considered risks in pursuit of opportunity is as relevant at portfolio level as at any other level in an organisation. Using information on riskiness and risk management effectiveness at this level can help ensure that options are well developed and considered and that decisions are taken with due regard to the probability of success.

More guidance that can be used at portfolio level to direct decision making at the point spending/ investment and prioritisation choices are made and reviewed, is provided in the Portfolio Management Framework (PMF) that can be found here: **ADD LINK**

The portfolio risk management good practices detailed in the PMF have been gathered from HM Treasury's Orange Book and are intended to be particularly beneficial in times of heightened uncertainty and/or rapid change where decisions need to be made quickly and often with incomplete information.

Levels of risk

The diagram below illustrates the levels of risk, and the escalation and de-escalation routes for 'active risk management'. GLA's risk reporting is presented and scrutinised by Assembly Members at the Budget & Performance Committee and the Audit Panel.



Appendix 1: Risk register template

Note that an Excel format risk register is available via the risk intranet page. This includes a format that allows more detailed information to be captured.

Risk #	Risk description and impact	Inherent risk assessment			Control measures/Actions	Action owner	Deadline/Completed	Residual risk assessment			Risk owner
		Prob.	Impact	Overall				Prob.	Impact	Overall	
1	[Cause, 'risk event', potential impacts]	**[1-5]**	**[1-5]**	**[1-25]**				**[1-5]**	**[1-5]**	**[1--25]**	
2											
3											
4											
5											
6											
7											
8											
9											

Example risk

1	**Poor KPIs** Poor definitions, inadequate systems or shaky rationales mean that the GLA's suite of KPIs does not provide insight into the performance of the Authority in key areas. In turn, this will impair the GLA's ability to take remedial action, achieve its goals and celebrate success.	**3**	**3**	**9**	Consultation with Mayoral Advisors and senior officers on the scope of the KPIs.	Michelle W	Completed 21/12/25	**1**	**2**	**2**	Fay H
					Named performance and data managers for each indicator.	Michelle W	In progress. To complete by 25/1/26				
					Lead process to ensure systems are established, including data quality checks.	Michelle W	Begin 28/1. To complete by 1/3/26				
					Put in place process to monitor KPI scope and data quality on an ongoing basis.	Michelle W	To be in place by 1/4/26				

Appendix 2: Questions to ask for continual improvement (From HMT Orange Book)

Governance and Leadership

1 How is the desired risk culture defined, communicated, and promoted? How is this periodically assessed?

2 How has the nature and extent of the principal risks that the GLA is willing to take in achieving its objectives been determined and used to inform decision making? Is this risk appetite tailored and proportionate to the GLA?

3 How are the MDB and other governance forums supported to consider the management of risks, and how is this integrated with discussion on other matters?

4 How effective are risk information and insights in supporting decision-making, in terms of the focus and quality of information, its source, its format and its frequency?

5 How are authority, responsibility and accountability for risk management and internal control defined, coordinated and documented throughout the GLA?

6 How is the designated individual responsible for leading the overall approach to risk management positioned and supported to allow them to exercise their objectivity and influence effective decision-making?

7 How are the necessary skills, knowledge and experience of the GLA's risk practitioners assessed and supported?

8 How has the necessary commitment to risk management been demonstrated?

Integration

9 How are risks considered when setting and changing strategy and priorities?

10 How are risks transparently assessed within the appraisal of options for policies, programmes and projects or other significant commitments?

11 How are emerging risks identified and considered?

12 How are risks to the public assessed and reflected within policy development and implementation?

13 How are central government's National Risk Register risks, which are particularly pertinent to the GLA, recognised in risk assessments and discussions?

Collaboration and Best Information

14 How is an aggregated view of the risk profile informed across the GLA, GLA companies and the directorates supporting the delivery of services?

15 How are the views of external stakeholders gathered and included within risk considerations?

16 How does communication and consultation assist stakeholders to understand the risks faced and the GLA's response?

17 How is function and professional expertise used to inform strategies, plans, programmes, projects and policies?

18 How do expert functions and professions inform the identification, assessment and management of risks and the design and implementation of controls?

19 How are functional standards communicated and their adherence monitored across the GLA?

Risk Management Processes

20 How are risk taxonomies or categories used to facilitate the identification of risks within the overall risk profile?

21 How are risk criteria set to support consistent interpretation and application in assessing the level of risk?

And how effective are these in supporting the understanding and consideration of the probability and impact of risks?

22 How are interdependencies between risks or combinations of events ('domino' risks) identified and assessed?

23 How dynamic is the assessment of risks and the consideration of mitigating actions to reflect new or changing risks or operational efficiencies?

24 How are exposures to each principal risk assessed against the nature and extent of risks that the GLA is willing to take in achieving its objectives – its risk appetite – to inform options for the selection and development of internal controls?

25 How are contingency arrangements for high impact risks designed and tested to support continuity, incident and crisis management and resilience?

26 How are new and changing principal risks highlighted and escalated clearly, easily and more rapidly when required?

27 How comprehensive, informative and coordinated are assurance activities in helping achieve objectives and in supporting the effective management of risks?

Continual Improvement

28 How are policies, programmes and projects evaluated to inform learning from experience? How are lessons systematically learned from past events?

29 How is risk management maturity periodically assessed to identify areas for improvement? Is the view consistent across differing parts or levels of the GLA?

30 How are improvement opportunities identified, prioritised, implemented and monitored?

Appendix 3: Risk categories (from HMT Orange Book)

Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

Operations risks – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

Legal risks – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

Property risks – Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.

People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the GLA and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver objectives and outcomes and intended benefits to time, cost and quality.

Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.