Agenda Item 12	Appendix
Risk Management Framework	A

CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

Risk Management Framework

September 2023

Version History

Revision Number	Revision Date	Nature of Revision	Created by
V1	January 2020	Approved at Audit & Governance in November 2019 and Combined Authority Board January 2020	Programme Office
V2	September 2023	Refresh of Risk Management Framework following RSM Audit and structured around new HMT Orange Book guidance	Programme Office
	Next review September 2025 at Audit & Governance		

Contents

1 Introduction

The Combined Authority Risk Management Framework has been based upon the principles of the HMT Orange Book (2020).

The Orange Book states that, in successful organisations, risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. Therefore, if we are serious about meeting our objectives successfully, improving service delivery and achieving value for money, risk management must be an essential and integral part of planning and decision-making.

The Department for Levelling Up Housing & Communities (DLUHC) published its English Devolution Accountability Framework (EDAF) in March 2023. This provides guidance on how Mayoral Combined Authorities should be accountable to local scrutiny, the public and the UK government. Our Risk Management Framework supports our compliance with the standards in the EDAF.

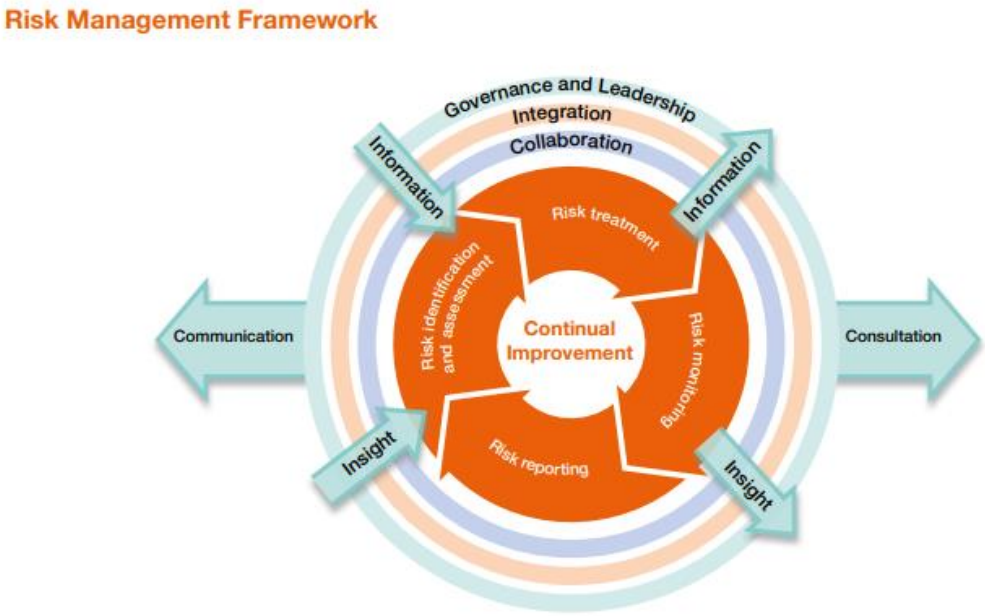
This Framework sits within a broader Single Assurance Framework (SAF). The SAF sets out the processes, approach and criteria that demonstrate to government the robust assurance, appraisal and value for money considerations that are used to develop and deliver projects and programmes to a high standard, maximising the opportunity to realise benefits whilst ensuring effective stewardship of public funds. The Risk Management Framework is a key tool in successfully delivering the SAF. It ensures that appropriate pipeline and project oversight is provided by both officers and politicians and provides risk data on project development and delivery to drive performance review considerations.

2 Approach

Figure 1 is an illustration of the Orange Book Risk Management Framework and how the Combined Authority Risk Management Framework has been designed around these Orange Book principles.

These principles of risk management support the consistent and robust identification and management of risk within desired levels across the organisation, supporting openness, challenge, innovation, and excellence in the achievement of objectives.

Figure 1



The Orange Book 5 principles are **governance, integration, collaboration, processes,** and **continual improvement.**

The objective of this framework is to adapt these principles to the Combined Authority's ways of working, ensuring compliance with our Single Assurance Framework.

The outcomes and benefits gained from the implementation of this framework include:

- Strengthened governance and leadership: with clear lines of reporting and clarity of levels of delegation and escalation.
- Improved knowledge of risk: as an organisation and improved risk culture.
- Efficient risk reporting: where risks will be reported to the relevant people ensuring resources are in the right place.
- Effective risk reporting: where risk management processes are used correctly at all levels to ensure good management of risks
- Better cooperation and collaboration: with partners, identification, and management of risk.
- Improved culture of continual improvement and learning.

This Risk Management Framework is underpinned by the Authority's Risk Management Procedure. The Risk Management Procedure outlines the tools, techniques, and mechanisms for managing risk in line with this strategy.

3 Governance

3.1 Desired risk culture

Our five values **(CIVIL)** are central to our culture, driving everything we do. Our employees embody these values to help us all work toward a common purpose.

A positive risk culture starts from the top and filters down. Senior members of teams, forums or boards must encourage staff to be open, honest/transparent and must listen and communicate effectively. If a risk does arise, there must be a no blame culture, otherwise it may stop people raising other risks in the future. A risk identified is positive, a risk ignored is negative.

Our five values are central to our culture, driving everything we do. Our employees embody these values to help us all work toward a common purpose. Excellent risk management demonstrates our values by:

- listening when a risk is raised and communicating the impact of risks in an open and transparent manner (demonstrating our value '**Collaborative**').
- positively challenging why we do things the way we do based on data and evidence (demonstrating our value '**Innovation**').
- ensuring that seeking inclusive, good growth for an equitable, resilient, healthier, and connected region is at the heart of our risk management (demonstrating our value '**Vision**').
- ensuring risks are identified and not ignored when they do not fit with where an officer wants the project, programme, or Authority to be - putting the obligations of public service above their own personal interests (demonstrating our value '**Integrity**').
- encouraging members of the team, forum or board to be honest about the risk and its potential impact (demonstrating our value '**Leadership**').

Risk reports are provided to the Audit & Governance Committee (A&G) which are published and discussed publicly. These are available on our website.

3.2 Roles & Responsibilities

The Chief Executive, working closely with the Executive Director of Resources & Performance, is accountable for ensuring that Corporate Risk Management is being completed to the appropriate standard in line with this framework. This includes ensuring risks are captured and updated and that mitigating actions have been completed. The Corporate Management Team review the risks on the register monthly. Similarly, the Executive Directors and Heads of Service are accountable for the service level risk registers within their remit, and Project Managers for the project level risk registers.

The Authority's Programme Management Office (PMO) manage and coordinate these reviews, as well as collating information to support effective decision making and developing

the associated risk reports. The PMO support A&G and other governance forums to consider the management of risks, and how the risks are integrated with discussion on other matters.

The PMO are responsible for ensuring that the Corporate Risk Register is maintained, updated and that risks are regularly reviewed with the Executive Director of Resources & Performance, CMT, A&G and the risk owners. The PMO also meets with service teams to review the service/programme level risk registers.

The A&G Committee is responsible for overseeing the Authority's Risk Management Framework and Procedures and the Corporate Risk Register, to ensure that risk management is being done to the appropriate standard and in line with this framework.

The full roles & responsibilities are set out in Appendix 1.

3.3 Corporate Risk Appetite

The Authority has an approved risk appetite statement that provides the parameters for the management and decision making of the risks being faced by the organisation. Different categories of risk have been defined, each of which has an appetite aligned to it. The associated risk appetite level aids in informing the target risk score for each risk within the corporate risk register.

3.3.1 Risk Appetite Level Definitions

Risk appetite level	Risk appetite level description
Averse	We shall seek to reduce the residual risk as far as practically and reasonably possible within the constraints of resources available.
Minimal	We shall accept a low degree of residual risk. Benefit will not be the driver.
Cautious	We are willing to accept some degree of residual risk where we have identified scope to achieve significant benefit and / or realise an opportunity.
Open	We are willing to consider a range of options where we are able to demonstrate a balance between a high level of residual risk and a high likelihood of successful / beneficial outcomes.
Hungry	We are eager to be innovative and choose a range of options based on maximising opportunities and beneficial outcomes even if those activities carry a very high level of residual risk.

3.3.2 Risk Appetite Statement

Finance

Ensuring continued financial viability is a key factor for the Combined Authority to ensure that it is suitably positioned to deliver its day-to-day activities and future plans. We will keep in check its key internal financial controls and financial arrangements to ensure they remain in the Combined Authority's best interests.

The Combined Authority has set a **Cautious** risk appetite to financial risk, however, is willing to be **Open** and accept a higher level of residual risk where there is an opportunity to generate significant returns, benefit or outcomes in line with its Strategies.

People

The Combined Authority's risk appetite for People related risks (including but not limited to capability, experience, and skills) has been set as **Open**. We will continue to provide and review creative opportunities to develop the workforce to build the capability and skills needed to deliver our strategic objectives.

However, we are mindful that we must remain **Cautious** to people risk that may impact upon our ability to succession plan, or negatively affect the wellbeing or stability of the workforce.

Service Design & Delivery

For the Combined Authority to achieve its strategic objectives, we need to be **Open** to designing and delivering services differently and to innovate. However, we need to ensure that this does not negatively affect the stability or quality of our activities, for example through drawing resources away from day-to-day activities that are important to us or that are relied upon by our communities and stakeholders.

The Combined Authority has set an **Open** risk appetite and is willing to consider a range of options for service delivery where we are able to demonstrate a balance between a higher level of residual risk and a high likelihood of successful / beneficial outcomes.

Compliance & Regulation

The Combined Authority faces an array of compliance and regulatory requirements. The Board and Corporate Management Team do not view regulation as a tick box exercise but instead understand that good regulation can provide benefits to the outcomes that the Authority is seeking. We will use compliance with regulation as a positive measure of quality and governance and therefore will develop this as part of our organisation's culture.

As such we have set a **Cautious** risk appetite and are willing to accept some degree of residual risk where we have identified scope to achieve significant benefit. However, when complying with Health and Safety legislation, we have set an **Averse** risk appetite, and will seek to reduce the residual risk as far as practically and reasonably possible within the constraints of resources available.

Culture & Confidence

The Combined Authority's risk appetite for risks related to culture and confidence has been set to **Cautious.** Our culture is important to us and will continue to evolve as it is a fundamental element of the improvement plan. We must therefore be willing to accept some degree of residual risk where we have identified scope to achieve significant benefit and / or realise an opportunity, however this will need to be undertaken in a considered manner.

Data & Management Information

The Combined Authority relies heavily upon data and management information to make decisions in an informed manner, however it is understood and appreciated that not all data will always be available when a decision is required to be made.

We have therefore agreed a **Cautious** risk appetite with regards to the access, quality and analysis of data within the Combined Authority so that we are in the best informed position possible whilst accepting some degree of residual risk may exist where we have identified scope to achieve significant benefit and / or realise an opportunity.

Partnerships

The Combined Authority works collaboratively with a number of strategic partners and seeks to use its influence and relationships to harness the benefits that these can bring.

The Combined Authority has set a **Cautious** risk appetite for partnerships and is willing to accept some degree of residual risk where we have identified scope to achieve significant benefit and / or realise an opportunity. However, if there is potential for the brand or values of our organisation to be negatively impacted then a **Minimal** appetite will be adopted where a low degree of residual risk will be acceptable, and benefit will not be the driver.

Programmes & Projects

Programmes and projects underpin the Combined Authority's strategic objectives and therefore it is important that an **Open** risk appetite is taken towards considering new bids, particularly given the desire to design and deliver services in a more innovative manner. We are therefore willing to consider a range of options where we are able to demonstrate a balance between a high level of residual risk and a high likelihood of successful / beneficial outcomes.

We will however adopt a **Cautious** appetite to contract management risks to ensure that the programmes and projects deliver the desired outcomes and benefits, and that the reputation of the Combined Authority is not negatively impacted as a result.

3.3.3 How Risk Appetite will be used

FIGURE 2

Risk Theme	Appetite Level	Maximum Risk Score
Finance	Cautious	13
People	Open	17
Service Design & Delivery	Open	17
Compliance & Regulation	Cautious	13
Culture & Confidence	Cautious	13
Data & Management Information	Cautious	13
Partnerships	Cautious	13
Programmes & Projects	Open	17

Figure 2 shows the maximum risk score for each risk theme based on our appetite level. This means, as an example, if the Combined Authority were to have a financial risk above 13 it would be escalated and a deep dive into that risk would take place with the Corporate Management Team, as well as Audit & Governance Committee. This would be to ensure the correct mitigating actions are in place, including if we would be willing to tolerate the risk. **Risks are therefore escalated based on exceeding the maximum risk score.**

Within the Risk Report taken to Corporate Management Team and Audit & Governance Quarterly, there will be a graphic showing the risks that fall above risk appetite.

The frequency of review is determined by the category of risk. As figure 2 illustrates there are 5 categories from A to E, for example A is a risk between 20-25. The frequency of review will be built into the 4risk software, meaning that automatic notifications will be linked to the category that the risk currently sits within. This is expected to be the following:

Category A (20+): Reviewed every month

Category B (15-20): Reviewed quarterly

Category C (11-14) and D (7-10): Reviewed every 6 months

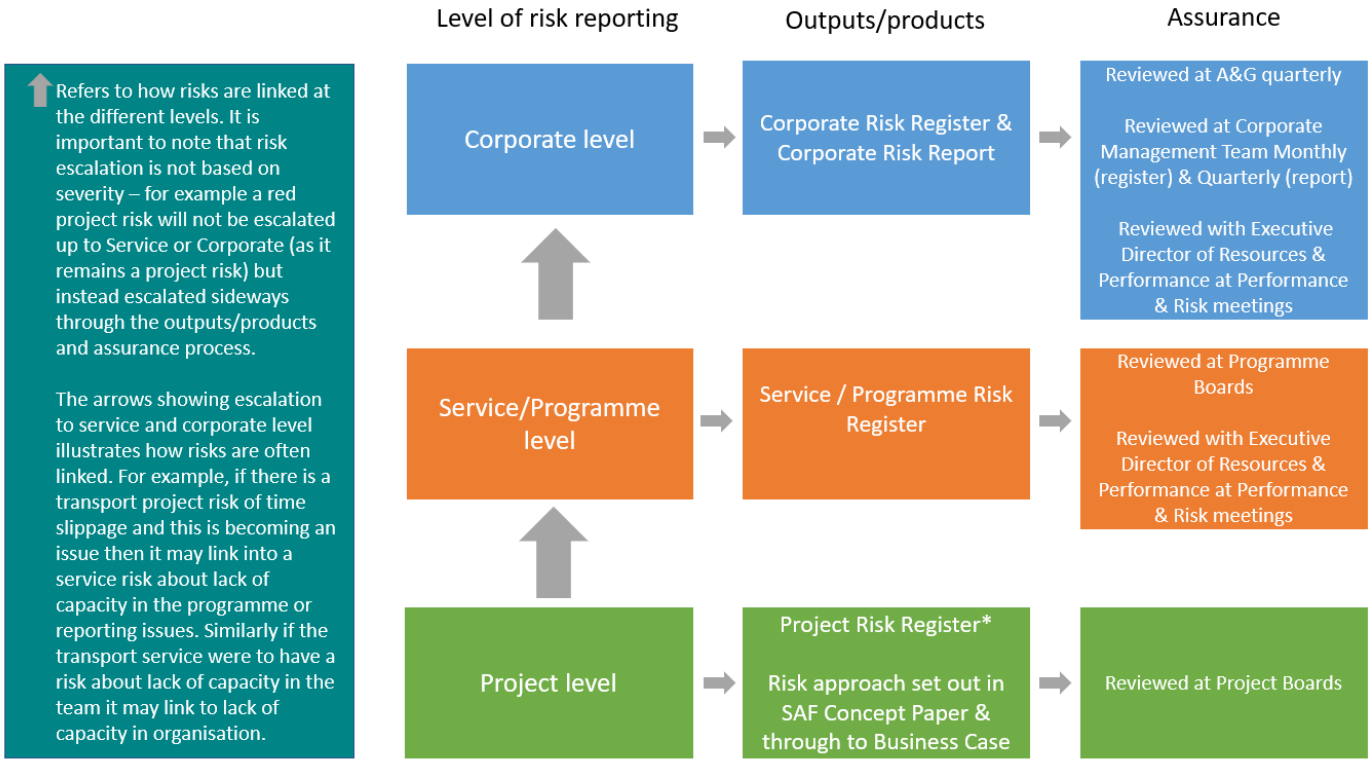
Category E (1-6): Reviewed every 9 months

4 Integration

4.1 Risk Structure in the Combined Authority

Corporate and service risk registers will be managed and reported within the 4risk platform. The level of reporting, outputs/products produced, and the level of assurance is illustrated in Figure 3.

FIGURE 3



* Projects require a risk register if the project is in delivery. This is completed as part of highlight reporting. If a project is at concept or business case stage then only a simplified highlight report is required, and this does not include a risk register. Nevertheless, at initiation stage all projects identify the key risks, and this continues through business case stage.

4.2 Corporate level risk management - roles and outputs

Corporate level risk refers to the uncertainties and opportunities that may positively or negatively impact the Authority or have an impact upon the achievement of its objectives.

As figure 3 illustrates, at a corporate level there is a Corporate Risk Register which is owned by the Chief Executive Officer, supported by the Executive Director for Resources & Performance and the PMO. This is to be held on the 4Risk platform.

This risk register is reviewed monthly by the PMO and the Executive Director of Resources & Performance and taken to Corporate Management Team meetings monthly. The Programme Office also have regular meetings with each Risk Owner.

In those meetings the risks that are above risk appetite are identified as well as high category risks (see 3.3.3 for more information). These forums can decide to close a risk and also decide that a risk which is above risk appetite is within tolerance; but in that case an explanation would be required which would feed into the Risk Report.

A Risk Report is reviewed quarterly at Corporate Management Team and taken quarterly to the Audit & Governance Committee.

As Figure 3 illustrates, service risks can often be linked to corporate risks. The Heads of Service and Executive Directors are responsible for identifying any service risks that link in to risks that impact the organisation, including threats and opportunities that our organisation faces.

4.3 Service / Programme level risk management - roles and outputs

The Combined Authority has 4 Directorates. Multiple services fall within these Directorates, an example being Transport or Skills. Each of these Services must have a risk register which will be held on 4risk. This is with the exception of services that only deliver corporate projects such as HR, PMO, Democratic Services etc.

The Authority also delivers programmes, in which multiple interrelated or dependent projects are delivered.

Understanding the risks is fundamental to the success of the service/programme. A risk unidentified or unmanaged could cause it to fail to meet its goal.

It is the responsibility of Executive Directors and Heads of Service to identify risks that may affect the service in their remit. Or if it is a programme the Programme Manager may identify common risks across the projects. It is also their responsibility to maintain this register and update the 4risk platform accordingly.

The registers are reviewed as part of the Performance & Risk meetings.

Performance & Risk meetings are between the Executive Director for Resources & Performance and the PMO team. Executive Directors, Heads of Service or Programme and Project Managers (including Sponsors) may be called into these meetings by exception to discuss risk/s.

As Figure 3 illustrates, project risks are often linked to service/programme risks. The Head of Service / Programme Manager must ensure they are close enough to the projects to be able to identify common causes of project risks which may form a service/programme risk.

To support effective decision-making risks will be managed by exception – in other words risks will only be escalated when necessary, and risk roles will be clear to ensure efficient resources are in the correct places.

A risk that is high or above appetite, should be escalated to the relevant assurance board such as programme board for a deep dive to ensure the mitigating actions are sufficient.

4.4 Project level risk management - roles and outputs

All projects are expected to show, in detail, any risks identified during the business case development and due diligence processes. Once in delivery, ongoing risk registers are maintained and incorporated into the monthly highlight report.

A risk approach (including roles & responsibilities) is developed through the Single Assurance Framework concept and initiation stage and continues into business case stage. The governance structure and roles within the project is set out, and this ensures that decision makers have focused information and that its source, format, and frequency has been agreed.

Project level risk registers are not currently held on 4risk and instead form part of highlight reporting.

To support effective decision-making risks will be managed by exception – in other words risks will only be escalated when necessary, and risk roles will be clear to ensure efficient resources are in the correct places.

A risk that is high or above appetite, should be escalated to the relevant assurance board such as project board for a deep dive and ensure the mitigating actions are sufficient.

See the Combined Authority 'Risk Management Procedure' which offers more information on the Authority's project/programme risk tools, reporting and budgets.

Who is responsible and accountable for risk depends on the governance of the project and the risk approach. Table 1 offers guidance to project managers when developing these roles and responsibilities by summarising who is responsible for risk based on the role of the Combined Authority in the project.

Table 1

Combined Authority role in projects	Who is accountable and responsible?	Further information on the role of the	How is it reported?

		Combined Authority	
Deliverer: Projects which the Combined Authority deliver directly through a supplier/contractor.	**Accountable:** The person in CPCA accountable for the project (SRO, Programme Manager etc.) **Responsible:** Project Manager (who in this case would be a Combined Authority employee) **Informed/consulted:** Programme Office, Project Board and Supplier/contractor	The Combined Authority will be responsible and accountable for the management of risk, in consultation with the supplier if they have been appointed – this is unless the supplier has agreed to take on the reporting and management of risk.	Highlight reports to the Programme Office once in delivery. Project Boards may decide to review monthly or ad hoc
Funding partner: Commissions work / subsidiary companies: *Projects which we deliver through a partner or delivery company and the responsibility for delivery has been delegated to another organisation/body.* **Or** **Grant or loan delivery:** *Delivery of grant or loan payments directly to another organisation or government body – through winning some form of bidding process.*	**Accountable:** Combined Authority Responsible Officer (Project Sponsor or equivalent) **Responsible:** Project Manager (in this case the person would be external to the Authority) **Informed/consulted:** Programme Office, Project Board, relevant body within the deliverer organisation and consultant/supplier	The Combined Authority Responsible Officer works with the project manager and delivery team to: a) approve the risk approach b) review risks by exception: the project manager will escalate the key risks where necessary c) mitigation of strategic risks: keeping an eye on the project to ensure it remains a strategic fit for the Authority.	Highlight reports to the Programme Office once in delivery. Project Boards may decide to review monthly or ad hoc

5 Collaboration & Best Information

5.1 Reporting

Risk reporting will be conducted as laid out in table 2.

At a project level a monthly highlight report cycle has been created and embedded across the organisation. Highlight reports also contain risk registers for each project in delivery, where project managers track and monitor key risks (and assign a named individual of appropriate seniority against each).

Using information from these monthly highlight reports, the data is pulled into a dashboard that is live on the Authority's website for transparency. This includes details on the RAG status of projects. One aspect of the RAG rating guidance is an assessment of level of risk; therefore the level of project risk impacts the RAG rating.

Performance data is also shared with a range of stakeholders and Boards/Committees. Table 2 sets out where performance data will be taken and what information each Board and Committee will receive.

Table 2

Meeting	What performance data will be received	Frequency
Combined Authority Board	Corporate Performance Report	Quarterly
A&G	Risk report	Quarterly
Performance & Risk meeting	Corporate Risk Register	Monthly
Corporate Management Team	Corporate Performance Report Corporate Risk Register	Quarterly Monthly

5.2 Partnership working and stakeholder risk engagement

All reports are available through the minutes / papers of the Audit & Governance Committee. Associated papers will be published on the CPCA Website through this link.

Partners and stakeholders will be continuously consulted on risks that affect the public, region, and organisation. The formal consultations take place in the following forums:

- Consultation with A&G Committee who review the Authority's Corporate Risk Register quarterly and suggest additional risk considerations.
- The Board receives an annual A&G report that includes risk. Board members can identify strategic risks and ask for these to be added to the Corporate Risk Register.
- Consultation with partners in programme boards, and sharing of risk across partners
- Consultation with partners at project boards

- Public consultations where the public are made aware of the risks and benefits of various options

6 Processes

The Combined Authority's Risk Processes are set out in the Risk Management Procedure **(link to be added shortly)** including information on the risk management cycle, how to manage risk, controls, treatments and assurance.

7 Continuous Improvement

7.1 Lessons Learned

Lessons will be captured through our lessons software (Microsoft PowerApps) which captures all lessons in the Authority, and these will be shared with partners to enable a community of learning. A Partner Working Group has been established so that all of the Authority's local partners can share ideas and lessons around assurance, performance and risk. The Authority also shares lessons with other Mayoral Combined Authorities via the 'M10' network.

7.2 Monitoring & Review of the Strategy

The Corporate Management Team will regularly review the Risk Management Framework to ensure that it continues to meet the needs of the Authority and is further refined and continually improved over time.

Risk Registers will be monitored regarding their standard of information and how often they are reviewed to ensure that specific risks are being actively reviewed and managed.

The Audit & Governance Committee will review the Risk Management Framework every 2 years to ensure that the Framework is fit for purpose and working effectively.

The Framework will be subject to regular review by Internal Audit as per audit schedules.

7.3 Training

All staff will be required to undertake risk management training appropriate to their role. The training will be delivered via workshops, online seminars and one to one support as appropriate. Those identified with increased responsibility for risk and reporting may be required to attend additional specific risk training.

A training schedule will be held by the PMO to ensure a regular training is made available.

8 Appendix 1: Roles & Responsibilities

Role	Responsibility / Action
Chief Executive supported by Executive Director for Resources and Performance	• Ownership of strategic / corporate risks and issues, ensuring mitigation actions are dealt with at the appropriate senior level. • Accountable for the monitoring and reviews of the corporate risk register. • Define clear rules for escalation and promotion.
Executive Directors and Heads of Service	• Ownership of service/programme level risk and issues. • Assures adherence to the risk management principles • Define clear rules for escalation and promotion. • Escalates items across the service / programme boundaries to Corporate Risk Register for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the service / programme. • Provides support and advice on risks • Allocates risk and issues as appropriate.
Risk owners (at all levels)	• Ownership of the risk, responsible for its management. • Assuring adherence to the risk management principles. • Escalates items where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion. • Provides support and advice on risks.

Role	Responsibility / Action
Combined Authority Board	• Adopt and review the Risk Management Framework. • Receive recommendations from the Audit & Governance Committee as to the Authority's arrangements for the management of risk and on any concerns that risks are being accepted which the Authority may find unacceptable. • Identify and propose new strategic risks • Review annual report from A&G

Audit &Governance Committee	• Initiates assurance reviews • Overseeing the Authority's Risk Management Framework and Corporate Risk Register. • Review the Risk Framework on an annual basis. • Monitor the Authority's risk and performance management arrangements including reviewing the risk register, progress with mitigating actions and assurances. • The 2009 Act requires the Audit & Governance Committee to review and scrutinise the Authority's financial affairs and to review and assess its risk management, internal control, and corporate governance arrangements.
Project Management Office (PMO)	• Manages and coordinates the information and support systems to enable efficient handling of the risk . • Maintains the risk register for the corporate risk register • Reviews the Service Level Registers. • Establishes, facilitates, and maintains the risk management cycle.