Agenda Item 12	**Appendix**
Risk Management Framework	**B**

CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

Risk Management Procedure

September 2023

Version History

Revision Number	Revision Date	Nature of Revision	Checked by	Reviewed by	Approved by
1	September 2023	Procedural document developed to supplement the refresh of Risk Management Strategy document following RSM Audit and structured around new HMT Orange Book guidance			
	Next review September 2024				

Contents

1. Scope

This risk management procedure outlines the Combined Authority's approach to managing risk and outlines the tools and techniques involved in ensuring that this takes place effectively and in a consistent manner.

1. Identify, capture and assess risk
2. Identify and implement suitable risk treatment (controls) to help reduce the likelihood of risks happening
3. Monitor how well the risk is being managed and any improvements needed
4. Understand the effectiveness of the control environment
5. Report risk using the relevant reporting system and escalation processes

2. Introduction

What is Risk?

To identify and record risk it is imperative to understand what a 'risk' is and what's involved in the process of risk management for the Authority.

Risk can be defined as anything that poses a threat to the achievement of Authority's objectives, programmes or service delivery to residents, businesses, and communities. It can come from inside or outside the organisation; may involve financial loss or gain; physical damage to people or property; customer dissatisfaction; unfavourable publicity; failure of equipment; fraud, etc. Failure to take advantage of opportunities may also have risks, e.g., not bidding for external funding, etc.

Risk definition

- Effect of uncertainty on objectives.
- May be positive, negative or a deviation from the expected.
- Risk is often described by an event, a change in circumstances or a consequence.

What is Risk Management?

Risk management is the range of activities that an organisation intentionally undertakes to understand and reduce the effects of risk in a manner consistent with the virtues of economy, efficiency, and effectiveness. Put simply when things go wrong then the cost of rectification brings about an unexpected draw on resources i.e., waste, this distracts us from delivering services and achieving our objectives and in the worst case can de-rail the Authority completely. It is also about making the most of opportunities that present themselves and knowing that the Authority can respond appropriately when it is in its interests to do so to help it achieve its objectives.

There is no such thing as a risk-free environment, but many risks can be avoided, reduced, or eliminated through good risk management – something managers do every day as part of their normal work.

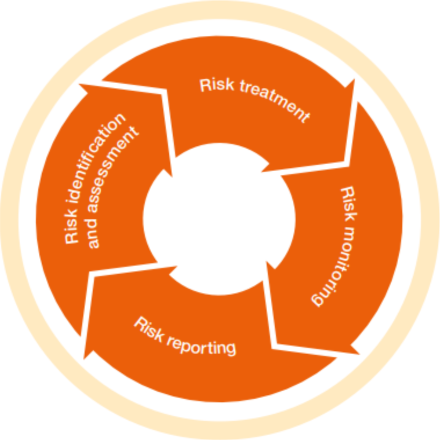
Risk Management definition

The process to help organisations understand, evaluate, and take proportionate action on all their risks with a view to increase the probability of success and reduce the likelihood of failure

3. The Risk Management Cycle

3.1 Risk management cycle

This illustrates the Orange Book procedure for managing risks. Combined Authority project, programme and corporate officers will be expected to follow this same process, which is to identify risks, assess the risk (and adding the risk treatment), monitoring and reporting the risk.



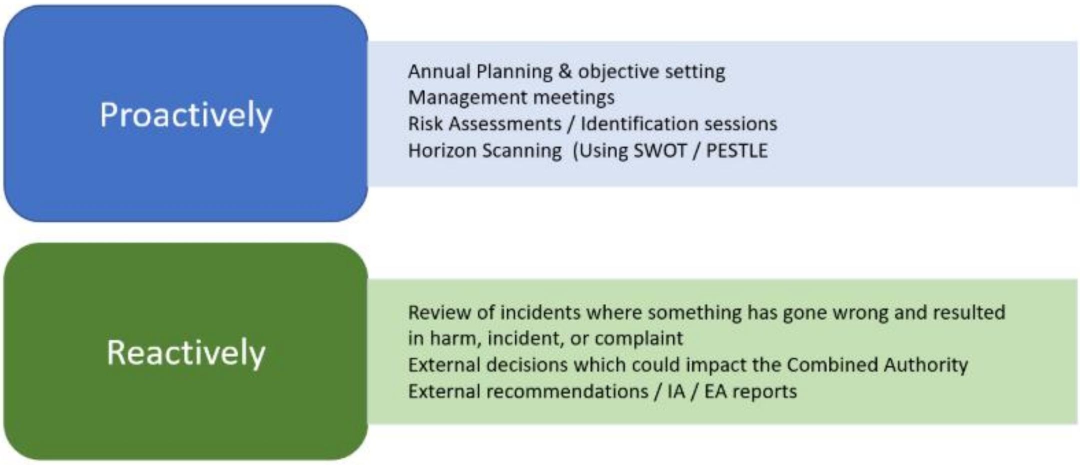
3.2 How risks are identified and considered

Risks will often be identified through reviewing lessons learned from previous projects/programmes and looking ahead through horizon scanning and using tools such as PESTLE analysis. A corporate level horizon scanning exercise will take place formally every 6 months to ensure there are no new risks facing the organisation, however it is anticipated that as risk is on the agenda for the Corporate Management Team on a regular basis that opportunities will arise for risks be identified as and when they are perceived to pose a threat.

At a project and programme level risk scanning must take place as part of reviews of the risk register. Best practice for project, programme or corporate teams is a workshop to identify new risks at a set time throughout delivery. Risks must be reviewed monthly within the project, programme and corporate registers to ensure that they remain updated given a shifting internal and external environment, and new risks identified.

The Authority’s risk appetite is outlined in the ‘Risk Management Strategy’, if the Authority’s risk appetite changes, then this will be communicated to all staff who must reassess the risks in light of those changes. For example, if the Authority’s appetite to one category of risk reduces then the management of all risks at a project, programme and corporate level will likely change, and it may lead to a trigger to escalate as risks now fall above the accepted tolerance.

Regardless of at what level a risk is captured, risks are typically identified through two avenues, either proactively, or reactively. The diagram below demonstrates examples of the different channels through which risks may be identified.



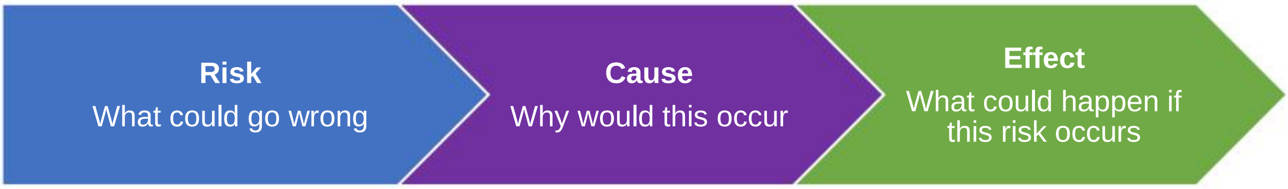
Proactively

Annual Planning & objective setting
Management meetings
Risk Assessments / Identification sessions
Horizon Scanning (Using SWOT / PESTLE

Reactively

Review of incidents where something has gone wrong and resulted in harm, incident, or complaint
External decisions which could impact the Combined Authority
External recommendations / IA / EA reports

Once a risk is identified, the risk must be assessed to determine how significant it is and how likely it is to happen. To do this the risk owner must consider why the risk would happen as this is what influences the likelihood. Then the effect the risk would have must be considered, which will tell us how big the potential impact could be.



Risk
What could go wrong

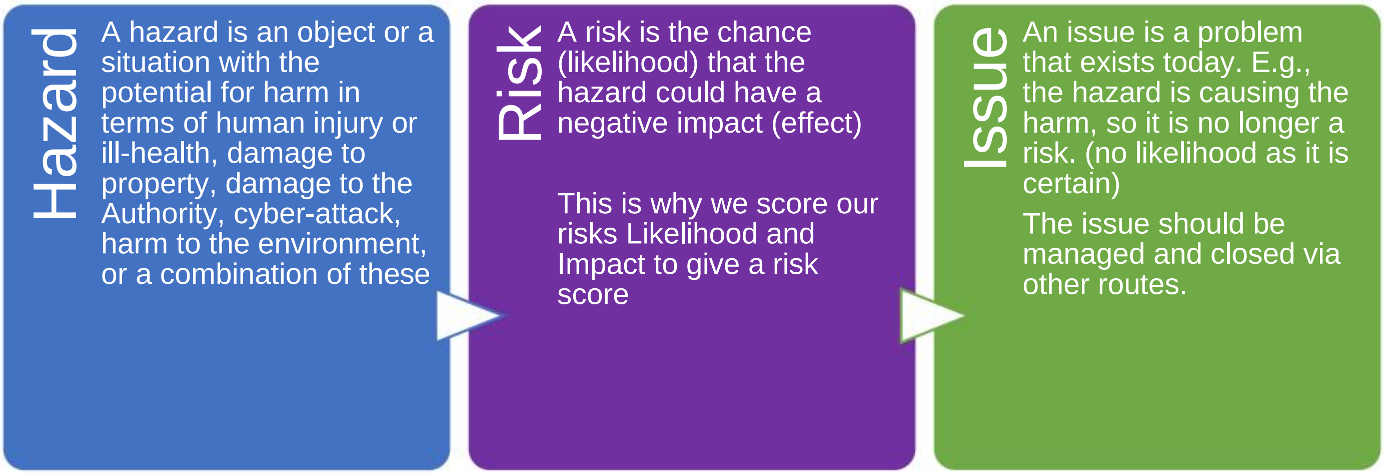
Cause
Why would this occur

Effect
What could happen if this risk occurs

Risk Assessment generally begins with understanding the objective (what the Authority is trying to maintain or achieve) and then an identification of hazards that may prohibit or delay achieving that objective.

The cause and impact of these hazards coming into effect are what is being assessed.

The differences between hazard, risk and an issue are explained below:



Hazard

A hazard is an object or a situation with the potential for harm in terms of human injury or ill-health, damage to property, damage to the Authority, cyber-attack, harm to the environment, or a combination of these

Risk

A risk is the chance (likelihood) that the hazard could have a negative impact (effect)

This is why we score our risks Likelihood and Impact to give a risk score

Issue

An issue is a problem that exists today. E.g., the hazard is causing the harm, so it is no longer a risk. (no likelihood as it is certain)

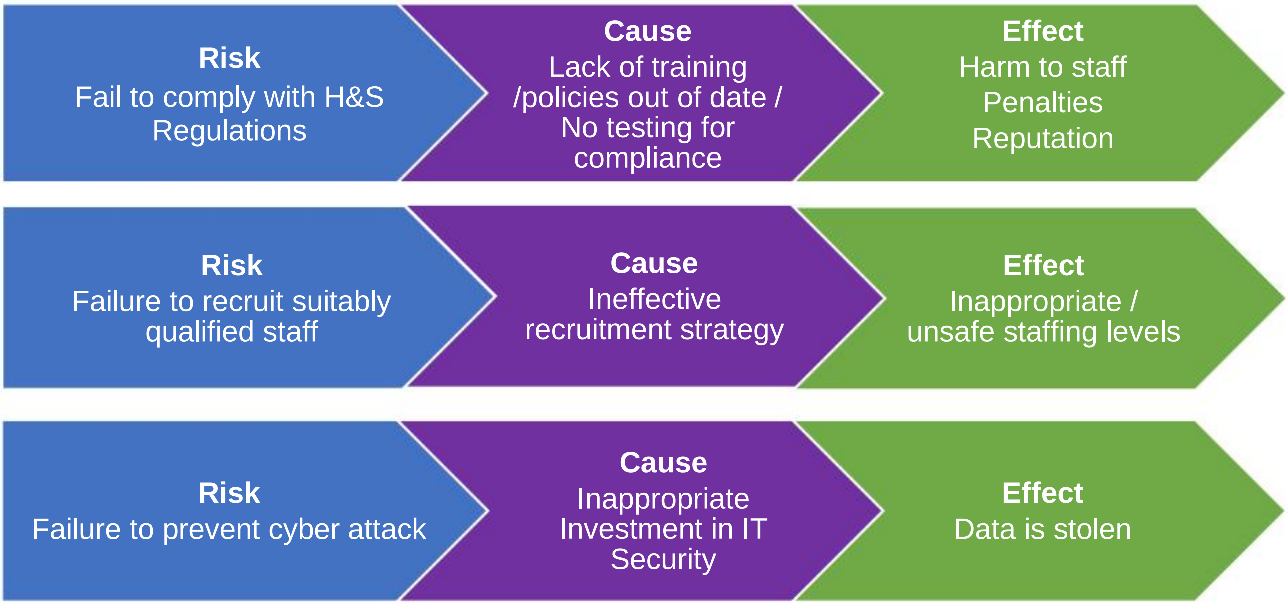
The issue should be managed and closed via other routes.

3.3 Recording Risks

Once a risk is identified, owners must record it so that management can continue to monitor and ensure that the Authority is managing the risk. A risk owner is the accountable person best placed to manage the risk. As risks escalate, they may change ownership to reflect seniority and responsibility.

All risks must be recorded in the appropriate risk register on the 4risk platform (the risk management system used by the Authority to document, manage, and monitor risk). The risk management system allows the Authority to create “Risk Registers” which are the central point for recording and monitoring the lifecycle of risk assessments. It is here that risk owners must maintain risk records and manage improvement actions.

As explained earlier risks are to be described using cause and effect to support the risk description so that, at a glance, management can understand what could cause the risk and how the Authority could be impacted if it was to happen. Simplified examples are:



Risk
Fail to comply with H&S Regulations

Cause
Lack of training /policies out of date / No testing for compliance

Effect
Harm to staff
Penalties
Reputation

Risk
Failure to recruit suitably qualified staff

Cause
Ineffective recruitment strategy

Effect
Inappropriate / unsafe staffing levels

Risk
Failure to prevent cyber attack

Cause
Inappropriate Investment in IT Security

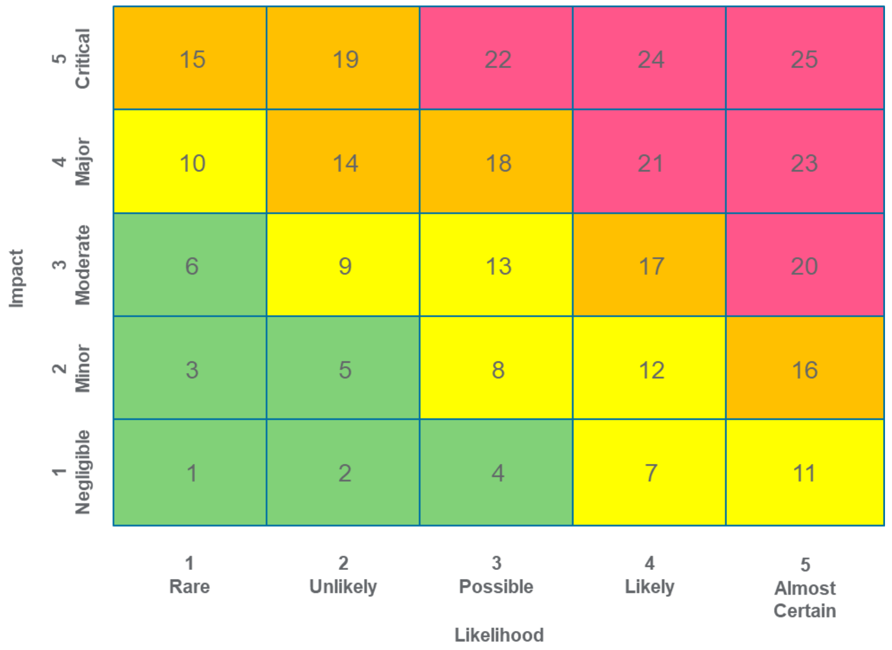
Effect
Data is stolen

3.4 Risk Assessment

The Authority uses a 5 by 5 risk grading matrix which helps assess, using scores of 1-5, the likelihood and impact (see below) of each risk.

- Each risk must be given a **‘inherent’** (before controls) score based on there being nothing in place to help manage the risk. The risk owner must then rate the risk with its **‘residual’** (after controls) score. i.e. where the risk owner believes it sits today based on how the risk is currently being managed to prevent the risk from happening.

- Finally, the risk must also be given a **'target'** score to demonstrate where the risk owner would like the risk to be once all controls are in place and actions are complete, this will be driven by the agreed risk appetite for the category of risk in question.



Impact	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
5 Critical	15	19	22	24	25
4 Major	10	14	18	21	23
3 Moderate	6	9	13	17	20
2 Minor	3	5	8	12	16
1 Negligible	1	2	4	7	11

Likelihood

3.5 Controls and Risk Treatment

Understanding the control environment for each risk is a fundamental consideration as part of the Authority's risk management framework.

Each risk must have a set of key 'current' controls identified, which must be aligned to the causes for the risk. Controls are defined as the day-to-day management activities within the Authority that will manage the risk and reduce the likelihood of the risk materialising. These must be succinctly documented within the risk register, and if deemed effective, demonstrate a reduction in risk between the inherent and residual scores.

Where it is deemed, that further action is required to better manage a risk and improve the control environment, an action must be identified, with an owner identified and an implementation date. This information must be recorded within the risk register for monitoring purposes.

For example, if the residual risk score is perceived to be higher than the target risk score, then it is expected that one or more actions would be identified.

It is possible that the residual and target scores are the same, if this is the case then it may be that no further action is required as the risk is deemed to be in-line or within the Authority's risk appetite for that type of risk.

The Authority has adopted risk treatment concepts to help risk owners ascertain how to treat a risk based upon its residual risk score and risk appetite.

Threat

1. **Accept** – Here we accept the risk and take no proactive action other than putting monitoring processes in place to make sure that the potential for damage does not change. Once the risk is accepted it is generally necessary to provide for some form of contingency to provide funds / time to accommodate the risk should it happen (despite its lower likelihood / impact)
2. **Avoid** – The only real way to avoid a risk is to change the project scope or approach – what we do or the way we do it.
3. **Transfer** – We seek to move the risk from our risk register onto someone else's risk register. We seek to transfer the potential for harm to another. Usually through an insurance policy or a contract.
4. **Reduce** – either the likelihood or impact.

When considering opportunity risk and a thorough risk assessment has been undertaken, the following treatment should be followed:

Opportunity

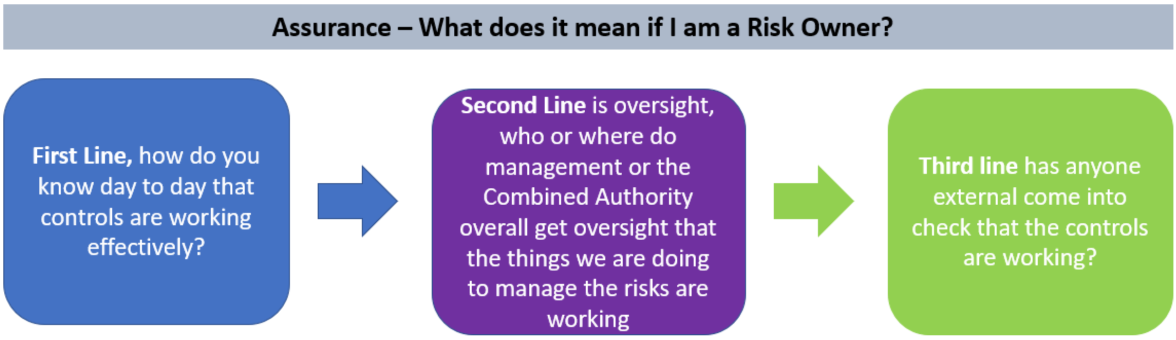
1. **Reject** – Choose not to take the advantage of the opportunity, possibly because it is worth too little or requires too much work to capitalise on.
2. **Enhance** – Take proactive steps to try and enhance the probability of the opportunity being able to be exploited.
3. **Exploit** – This involves changing the scope of the project /programme to encompass some
4. **Share** – Seek partners with whom can actively capitalise on the circumstances such as a Joint Venture.

Care is needed when arriving at any response to risk because regardless of what action is taken, it has the potential to generate other risks. When a risk can no longer be mitigated and the risk becomes realised, it is then called an "Issue".

3.6 Assurance

All corporate risks must have, where available, assurances documented to demonstrate the effectiveness of the controls. The assurance of controls is fundamental in ensuring the controls are regularly monitored and reviewed. It is important however that the approach remains proportionate and balanced to the risk exposure being faced.

Assurance refers to an opinion on the effectiveness of the controls being relied upon to manage a risk. Assurance can be either negative or positive in this instance and is gathered at 3 different 'lines'. These are explained further in the diagram below.



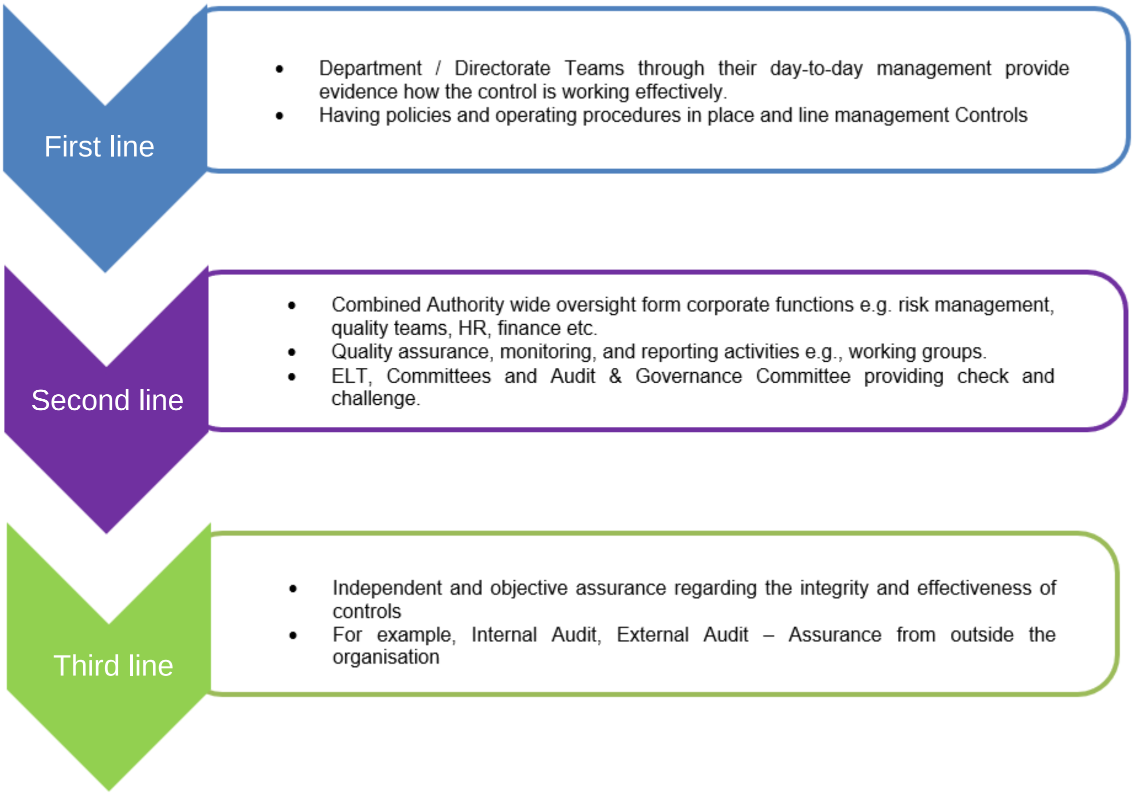
Assurance – What does it mean if I am a Risk Owner?

First Line, how do you know day to day that controls are working effectively?

Second Line is oversight, who or where do management or the Combined Authority overall get oversight that the things we are doing to manage the risks are working

Third line has anyone external come into check that the controls are working?

Examples of assurances at each of the ‘three lines’ are shown in the diagram below. It is expected that as a **minimum,** a first line of assurance should be available for each control identified and recorded within the risk register.



First line

- Department / Directorate Teams through their day-to-day management provide evidence how the control is working effectively.
- Having policies and operating procedures in place and line management Controls

Second line

- Combined Authority wide oversight form corporate functions e.g. risk management, quality teams, HR, finance etc.
- Quality assurance, monitoring, and reporting activities e.g., working groups.
- ELT, Committees and Audit & Governance Committee providing check and challenge.

Third line

- Independent and objective assurance regarding the integrity and effectiveness of controls
- For example, Internal Audit, External Audit – Assurance from outside the organisation

3.7 Monitoring and reporting of risk

Risk is managed as a cycle as it is a continual process. It should involve regular checking or surveillance, and this will be done periodically (via meetings such as Risk Reviews, Programme Reviews etc or on an ad hoc basis). A combination of both ensures that risks are reviewed regularly, and the mitigation and action plan are up to date.

Monitoring and review ensure that the Authority continually learns from experience. The objectives of our monitoring and review process are as follows:

- Ensuring the controls are effective in both design and operation.
- Obtaining further information to improve risk assessment.
- Analysing and learning lessons from previous events.
- Detecting changes in the external and internal context.
- Identifying emerging risks.

Risk will be monitored and reported in line with the following frequencies:

Corporate Risk Register:

The Corporate Risk Register will be reviewed on a monthly basis by the Executive Director of Resources & Performance and CMT and subsequently by the Audit & Governance Committee quarterly.

Service / Programme Risk:

These risk registers must be reviewed regularly and monitored bi-monthly at Performance & Risk meetings.

4. Lessons learned (learning from risk)

Organisational learning from risks that have materialised is crucial to ensure continuous improvement and risk awareness. Should a risk materialise, a review should be undertaken to understand why the risk came to fruition. This review should seek to ascertain the key causes of the risk and any control failures.

The approach to the review should be proportionate to the level of risk that materialises and the impact that it had upon the Authority, programme or project.

Any key findings should be communicated to stakeholders and logged accordingly. If improvements are required for the control environment or safeguards need to be put in place to reduce the likelihood of the risk or similar risks occurring in the future, then these should be tracked through to implementation.

5. Appendix 1 – Risk Scoring Impact Descriptors

Impact:	Safety	Reputation	Media Attitude	Legal	Financial Loss	Strategic	Political	Planning or environmental
5. Critical	Potential to cause one or a number of fatalities. H&S breech causing serious fine, investigation, legal fees and possible stop notice	Stakeholders / Third parties suffer major loss or cost	Governmental or comparable political repercussions. Loss of confidence by public.	Action brought against Combined Authority.	Over £5m	Project will no longer align with the Combined Authority strategic objectives.	Impact on relationships with political partners/stakeholders or government leading to possible funding, legal or reputational impacts. Or Loss of confidence from CPCA Board in ability to deliver project successfully.	Unlikely to receive planning permission or will cause environmental harm.

4. Major	Serious risk or injury possibly leading to loss of life. H&S investigation resulting in investigation and loss of revenue.	Significant disruption and or Cost to Stakeholders / third parties	Story in multiple media outlets and/or national TV main news over more than one day		Between £4m and £5m	Project will need changes to align with Combined Authority strategic objectives.	May not be supported if taken to Board. Lack of political unanimity for scope and objectives	
3. Moderate	High risk of injury, possibly serious. H&S standards insufficient / poor training	A number of Stakeholders are aware and impacted by problems.	Critical article in Press or TV. Public criticism.		Between £3m and £4m	Project aligns with majority of strategic objectives but change is required to fit with one specific objective.	More than one political stakeholder/partner does not support	
2. Minor	Small risk of minor injury. H&S policy not regularly reviewed.	Some external Stakeholders aware of the problem, but impact on is minimal.	Negative general article of which Combined Authority is mentioned		Between £1m and £3m	Minor impact on strategic objectives	One political stakeholder/partner does not support	
1. Insignificant	No risk of injury. H&S compliant	External Stakeholders not impacted or aware of problem	No adverse media or trade press reporting.	No threat of legal action	Between £0 and £1m	Project continue to align to objectives	No threat of political issues	Permissions likely to be received and no environmental harm

6. Appendix 2 – Risk Scoring Likelihood Descriptors

Likelihood:	Description:
5. Almost certain	• A history of it happening across the organisation • The event is expected to occur • 80% - 100% probability
4. Likely	• Has happened across the organisation in the recent past • The event will probably occur in most circumstances • 60% -80% probability
3. Possible	• Happened across the organisation in the past • The event should occur at some time • 40% - 60% probability
2. Unlikely	• May have happened across the organisation in the past • The event could occur at some time • 20% - 40% probability
1. Rare	• History of it happening across the organisation • The event may occur only in exceptional circumstances • < 20% probability