Agenda Item 1.7 - Appendix 1

CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

CAMBRIDGE & PETERBOROUGH COMBINED AUTHORITY

CORPORATE RISK MANAGEMENT STRATEGY

CONTENTS

1. INTRODUCTION -What is Risk Management?

2. RISK POLICY - The Authority's Approach to Risk Management

3. RISK MANAGEMENT AIMS AND OBJECTIVES

4. ROLES AND RESPONSIBILITIES

5. ARRANGEMENTS FOR MANAGING RISKS

6. MONITORING ARRANGEMENTS

7. TRAINING & COMMUNICATION ARRANGEMENTS TO SUPPORT IMPLEMENTATION OF THE STRATEGY

8. REVIEW OF RISK MANAGEMENT STRATEGY

Appendix 1: Risk Management Methodology

Appendix 2: Corporate and Project Risk Registers

CAMBRIDGE AND PETERBOROUGH COMBINED AUTHORITY RISK MANAGEMENT STRATEGY

1. INTRODUCTION

What is Risk Management?

1.1 Risk can be defined as uncertainty of outcome. Risk is ever present and a certain amount of risk-taking is inevitable if the CPCA is to achieve its objectives. Risk management implies adopting a planned and systematic approach to the identification, evaluation and control of the risks facing the Authority and is a means of minimising the costs and disruption caused by undesired events.

1.2 Risk management covers the whole spectrum of risks and not just those associated with finance, health and safety and insurance. It also includes risks associated with public image (reputation), the environment, technology, contracts/partnerships, projects etc.

1.3 The Authority also has a statutory responsibility to have in place arrangements for managing risks, as stated in the Accounts & Audit Regulations 2015:- *"A relevant body must ensure that it has a sound system of internal control which: (a) facilitates the effective exercise of its functions and the achievement of its aims and objectives; (b) ensures that the financial and operational management of the authority is effective; and (c) includes effective arrangements for the management of risk."*

1.4 The benefits gained from effectively managing risk include:

Improved strategic management

- Greater ability to deliver against objectives and targets;
- Improved decision making

Improved operational management

- Reduction in managerial time spent dealing with the consequences of a risk event; having occurred;
- Improved service delivery

Improved financial management

- Better informed financial decision-making;
- Greater financial control;
- Minimising waste and poor value for money;
- Reduction in costly claims against the Authority

Improved customer service

- Minimal service disruption to customers and a positive external image as a result

2. RISK POLICY

2.1 The Authority's Approach to Risk Management

The Authority recognises the need for risk management to feature as a consideration in our strategic and operational planning and decision making. The Authority is committed to managing and minimising risk by identifying, analysing, evaluating and treating risks that may impact the future success of the organisation. The approach is designed to ensuring that risk management is fit for purpose by applying the following:

- All staff obtain a sound understanding of the principles of risk management.
- Avoid surprises and reduce financial impact by generating an increased understanding of risk and quickly identifying mitigation response plans.
- Embed risk management as part of decision making by providing visibility of risks.
- Have plans in place on how to respond to an emergency or crisis, to carry on with business and recover from a disaster.

The approach is based on: thinking logically; identifying key risks and what to do about each risk; deciding who is responsible for the risk; recording the risks and changes in risk exposure; and monitoring the risks and learning from events.

3. RISK MANAGEMENT AIMS AND OBJECTIVES

3.1 The aim of risk management is to ensure that the Authority has an effective process to support better decision making through good understanding of risks and their likely impact.

3.2 The objectives of the Authority's risk management strategy are to:-

- Raise awareness of the need for risk management;
- Minimise loss, disruption, damage and injury and reduce the cost of risk, thereby maximising resources;
- Inform policy and decision making by identifying risks and their likely impact.

3.3 These objectives will be achieved by:-

- Establishing clear roles, responsibilities and reporting lines within the Authority for risk management;

- Effective communication with, and the active involvement of, Service Managersand Directors;
- Monitoring progress in delivering the strategy and reviewing the risk management arrangements on an on-going basis.

4. ROLES AND RESPONSIBILITIES

4.1 The table below outlines the key roles within the risk management strategy: -

Table 1: Roles and Responsibilities

Chief Executive and Board	➢ To approve the Risk Management Policy and Strategy (including the Authority's risk appetite) ➢ To approve the Corporate Risk Register ➢ To monitor progress in the management of Strategic Risk ➢ Understand the most significant risks ➢ Manage the organisation in a crisis
Audit & Governance Committee	➢ To ensure that the Authority has an effective risk management process in place ➢ To monitor progress on the management of Strategic Risks
Head of Risk and Compliance	➢ To develop and review the risk management strategy and process in accordance with best practice ➢ Build awareness culture ➢ To provide advice and support to Management Team and Service Managers on the identification, analysis and prioritisation of risks ➢ To report on the identification and progress of strategic risks to the Audit & Governance Committee ➢ To provide risk management training as

	required to officers and Members ➢ Identify and report changes in the risk exposure to the organisation. ➢ Develop the risk management policy and keep it updated. ➢ Co-ordinate the risk control activities. ➢ Develop specialist contingency and recovery plans ➢ Support investigations of incidents and near misses ➢ Provide assurance on the management of risk
Management Team	➢ To determine the Authority's risk appetite ➢ To identify strategic risks ➢ To determine actions to manage strategic risks ➢ To monitor progress in managing strategic risks ➢ Ensure implementation of risk improvement recommendations ➢ Build awareness of risks within functions ➢ Evaluation of reports from employees on identified risks ➢ Identify and report on risk changes.
Service Managers	➢ To support the Management Team in the identification and management of Strategic Risks ➢ To manage operational risks effectively in their particular service areas ➢ To monitor and review risks at appropriate intervals

Employees	➢ To identify risks ➢ To implement actions as instructed ➢ Report inefficient, unnecessary or unworkable controls ➢ Report loss events and near miss incidents ➢ Co-operate with others in the investigation of risk incidents ➢ Ensure that visitors and contractors comply with procedures
Monitoring Officer	➢ To ensure that the Authority has an effective risk management framework
Internal Audit	➢ Provide advice and guidance on the management of risk relating to the design, implementation and operation of systems of internal control.

5. ARRANGEMENTS FOR MANAGING RISKS

5.1 The risk management methodology to be employed at the Authority is outlined in Appendix 1.

6. MONITORING ARRANGEMENTS

6.1 To ensure that informed decisions are made, it is essential to identify key strategic risks. Strategic risks will be identified at Management Team level as part of the Corporate Planning process and will be documented in the Corporate Risk Register which will be maintained by the Risk & Compliance Manager on behalf of the Monitoring Officer and the Management Team.

6.2 Progress in managing strategic risks will be monitored and reported on to ensure that intended actions are delivered and risks managed.

6.3 The Corporate Risk Register will form the basis of half yearly risk management reports to Board and the Audit & Governance Committee.

6.4 Internal Audit will carry out a periodic review of the Authority's risk management arrangements to provide independent assurance as to their effectiveness.

6.5 Internal Audit will also during the course of audits throughout the year:

- Identify and report weaknesses in the controls established by management to manage/monitor risks;
- Provide advice on the design/operation of the controls established by management to manage/monitor risk.

6.6 The Chief Internal Auditor will review the strategic risk register on an annual basis and incorporate strategic risk areas into the Internal Audit planning process as appropriate.

6.7 Service Managers should maintain a record of key operational risks within their service area relating to service change, projects and significant procurement. Progress in managing these risks should be monitored on a regular basis.

7. TRAINING & COMMUNICATION ARRANGEMENTS TO SUPPORT IMPLEMENTATION OF THE STRATEGY

7.1 Training in the risk management methodology will be provided to those officers with direct responsibility for / involvement in the risk management process.

7.2 Training in the risk management methodology will be provided to:

- Board
- the Audit & Governance Committee;
- Management Team;
- Service Managers; and
- Other employees as appropriate.

8. REVIEW OF RISK MANAGEMENT STRATEGY

8.1 This strategy will be reviewed every three years.

APPENDICES:

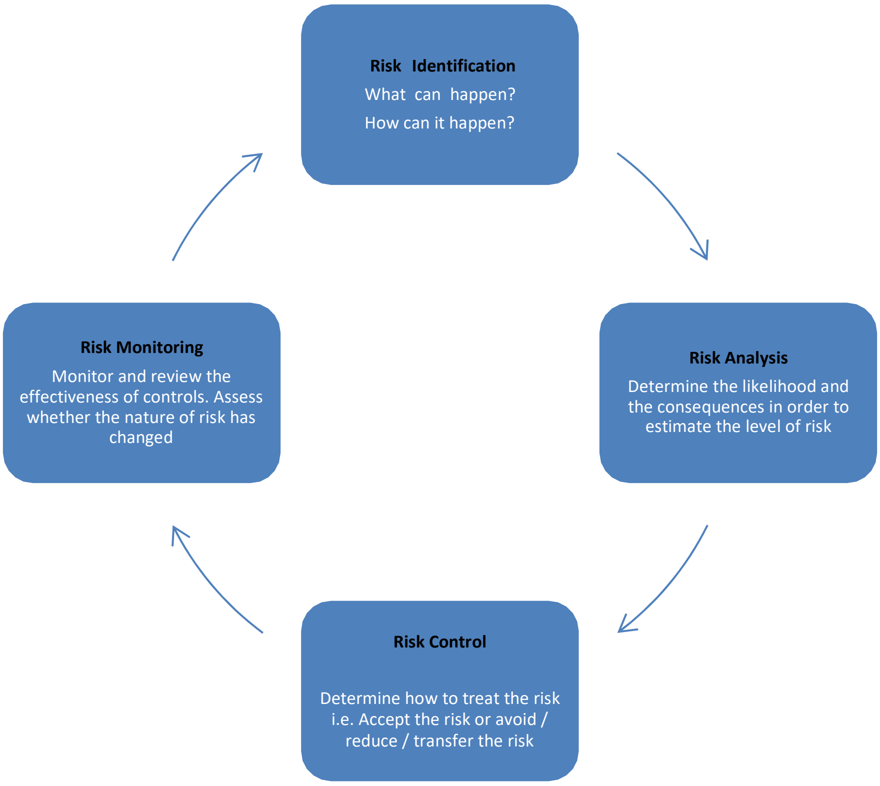
Appendix 1: Risk Management Methodology

Appendix 2: Corporate Risk Register and Project Risk Registers

APPENDIX 1: RISK MANAGEMENT METHODOLOGY

1. The Risk Management Cycle

There are 4 key stages in the risk management cycle, as illustrated in the diagram below:-



The 4 stages of risk management are part of a cycle. Risk management is dynamic and so the identification phase needs to be carried out continuously.

2. Risk Identification

2.1 Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. **Table 3** below lists the main techniques being used and a brief description of each of these techniques. When completing risk assessments for General Data Protection Regulation (GDPR) purposes consideration should be given to whether a Data Protection Risk Assessment (DPIA) is needed

Table 3 Risk Assessment Techniques

Risk Assessment Techniques	
Technique	Description
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks.
Workshops and brainstorming	Collection and sharing of ideas at workshops to discuss the events that could impact the objectives, core processes or key dependencies.
Inspections and Audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures.
Flowcharts and dependency analysis	Analysis of the processes and operations within the organisation to identify critical components that are the key to success.

The aim of the risk identification process is to generate a comprehensive list of risks be faced. Relevant and up to date information is important to identifying these risks and equally important is ensuring that our people with the appropriate knowledge are involved in our identification process. A variety of Risk Identification processes may be used as exemplified in the table below.

Table 4: Risk Identification Techniques

Risk Identification Techniques	
Technique	Description
Risk gap analysis	A list of common risks and uses these as a discussion point in risk reviews to facilitate risk thinking and identification
Workshops & brainstorming	Collection and sharing of ideas that could impact the objectives of the project/objective.
Audits and Inspections	Physical inspection of premises and audits of compliance with established systems and procedures
SWOT analysis	Strengths weaknesses opportunities Threats (SWOT)
PESTLE analysis	Political, Economic, Social, Technological, Legal & Environment

3. Risk Analysis and Scoring

3.1 Risk analysis involves completing a full investigation of the risk to develop an understanding of the likelihood and impact on the organisation. This analysis forms part of the risk evaluation process and helps to understand how the risks should be treated.

3.2 At this part of this risk analysis, risks are classified using the classification table below and recorded on the risk register which is stored in SharePoint. Once risks have been identified they need to be assessed. This process requires risk owners to assess the level of risk by considering:-

- The probability of an event occurring - “likelihood”; and
- The potential severity of the consequences should such an event occur – “impact”.

3.3 Not all factors are equally important and higher scores should be given to those risks considered to impact most on the achievement of objectives. The impact scores have therefore been weighted to reflect that more significance should be given to those risks with a medium or high impact than those with a medium or high likelihood.

3.4 The following table provides **Likelihood** and **Impact** descriptors to assist with this process:-

LIKELIHOOD

Score	Description	Indicative Guidelines
4	**Very Likely**	▪ There is a high exposure to the risk ▪ Event expected to occur ▪ Has occurred and will continue to do so without action being taken ▪ Indication of imminent occurrence ▪ There are external influences which are likely to make our controls ineffective
3	**Probable**	▪ There is a moderate exposure to risk ▪ Reasonable to expect event to occur ▪ Has occurred in the past ▪ Is likely to occur in the Authority’s planning cycle ▪ There are external influences which may

		reduce effectiveness of controls
2	**Possible**	▪ There is low exposure to risk ▪ Little likelihood of the event occurring ▪ There is a potential for external influences which may reduce the effectiveness of controls
1	**Unlikely**	▪ Extremely remote ▪ Not expected to occur but may do so in exceptional circumstances ▪ There are few or no external influences which may reduce effectiveness of controls
IMPACT		
Score	**Description**	**Indicative Guidelines**
5	**Major/ Serious Consequences**	The consequence is so bad that urgent action must be taken to improve the situation or prevent it worsening. External support from the Government or other agencies is likely to be needed: • Major loss, delay or interruption to services • One off event which would de-stabilise the Authority • Financial loss, additional costs or loss of assets which would need an Authority decision as the scale of the loss would be outside the Authority's budget & policy framework • The risk will cause the objective not to be reached, causing damage to the organisation's reputation. • Will attract medium to long-term attention of legislative or regulatory bodies • Major complaints • Significant adverse media interest • Death or life-threatening injury

3	**Moderate/Disruptive**	The consequence is sufficiently serious to require attention by Management Team and / or the Board: • Significant loss, delay or interruption to services • Medium term impact on operational efficiency or performance • Financial loss, additional costs or loss of assets that is within the Authority's budget and policy framework but needs a Statutory Officer decision, Management Team decision, or to be drawn to the attention of the Board. • The risk will cause some elements of the objective to be delayed or not achieved, causing potential damage to the organisation's reputation. • May attract medium to short term attention of legislative or regulatory bodies • Significant complaints • Serious accident / injury (but not life threatening)
1	**Minor/Non Disruptive**	The consequences can be dealt with as part of the normal day-to-day business by the Service Manager and the Director: • Minor loss, delay or interruption to services • Short term impact on operational efficiency or performance • Negligible financial loss • The risk will not substantively impede the achievement of the objective, causing minimal damage to the organisation's reputation • No or minimal external interest • Isolated complaints • Minor accident / injury

3.5 Both gross and residual scores should be identified to effectively review and monitor the effectiveness of the controls in place.

- **Gross Score**-The level of risk faced before internal controls/mitigating actions have been applied / implemented.
- **Residual Score**-The level of risk faced after any internal controls/mitigating actions have been applied/considered.

3.6 Internal controls are the Authority's policies, procedures and processes or any additional controls or mitigating actions taken to deal with a risk. Judgement must be made by the risk owner/facilitator as to the numerical reduction to the gross risk score to produce the residual risk score. The residual scores are then plotted onto the risk matrix, see below, which will determine the risk priority.

RISK		**IMPACT**		
LIKELIHOOD		**Minor/Non-Disruptive(1)**	**Moderate/Disruptive (3)**	**Major/Serious Consequences(5)**
	Very Likely (4)	**4**	**12**	**20**
	Probable (3)	**3**	**9**	**15**
	Possible (2)	**2**	**6**	**10**
	Unlikely (1)	**1**	**3**	**5**

4. Risk Control

4.1 Having identified and analysed the risks, it is necessary to decide what to do and who will do it. Priority will be given to the High (red) risks which will require immediate action plans.

4.2 Medium (Amber) risks will require actions plans and / or to be closely monitored as appropriate.

4.3 Low-scoring (Green) risks can be “accepted” and will not require actions plans. However, these risks will need to be monitored to ensure that controls remain operational to manage them and that such risks do not run out of control and become Medium (Amber) or High (Red) risks.

4.4 Where it is not deemed appropriate to accept the risk, the risk will need to be controlled. Risk control is the process of taking action to minimise the likelihood of the risk event occurring and/or reducing the severity of the consequences should it occur. There are 3 main options for controlling risk; avoidance, reduction and risk transfer.

4.5 **Risk avoidance** involves the Authority opting not to undertake a current or proposed activity because it is considered to be too risky.

4.6 **Risk reduction** is dependent on implementing actions which will minimise the likelihood of an event occurring or limit the severity of the consequences should it occur.

4.7 **Risk transfer** involves transferring liability for the consequences of an event to another body. This may be done in two ways: -

- Cost, delivery or legal liability may be transferred to an alternative provider under contractual/partnership arrangements for service delivery; however, it should be remembered that some responsibility may be retained for ensuring that the risk is managed e.g. Health & Safety.
- The costs associated with a damaging event may be reduced by transferring some or all of the financial risk to external insurance companies however; it should be remembered that many risks are uninsurable.

5. Risk Treatment

5.1 Risk treatment is the activity of selecting and implementing appropriate control measures to modify the risk. The Authority’s system of risk treatment provides the development of efficient and effective internal controls. Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures.

5.2 The cost effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits achieved.

5.3 Controls are defined as actions that are taken to reduce the likelihood and/or magnitude of a risk. Controls can be preventive, corrective, directive or detective as set out in the table below.

Table 1: Types of Control

Types of Control	
Control Type	Description
Preventive	Designed to limit the risk from occurring
Corrective	Designed to limit the scope for loss
Directive	Type of control based on giving instruction
Detective	Designed to identify a risk that has occurred to minimise the loss

6. Risk Response

6.1 The risk management responses used can be a mix of five main actions; transfer, tolerate, treat, terminate or take the opportunity.

- **Transfer**; for some risks, the best response may be to transfer them. This might be achieved by conventional insurance or by supporting a third party to take the risk in another way.
- **Tolerate**; the ability for us to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. This course of action will commonly be used for large external risks.
- **Treat;** by far the greater number of our risks will belong to this category. The purpose of treating a risk is to reduce the chance of the risk occurring and is not necessarily to obviate the risk, but to contain it to an acceptable level.
- **Terminate** the risk by doing things differently thus removing the risk where it is feasible to do so.

7. Risk Mitigation and Management

7.1 The mitigating actions are the key to successful risk management. These focus on the risk and are actions which make it less likely that the risk will occur, or which will reduce its impact, probability or both. They are designed to be as Specific Measurable Achievable Realistic, and Time bound (SMART) as possible. Any mitigating actions which stay the same over a long period are reviewed as they may not be effective, although they might still be necessary.

7.2 Most risks can be managed – either by minimising the likelihood of the risk occurring and / or reducing the severity of the consequences should the risk occur. Relatively few risks have to be avoided or transferred. Managers must judge which courses of control action are the most appropriate to address each of the risks they have identified, taking advice from the Risk & Compliance Manager and other support services where appropriate.

7.4 The cost/benefit of each control act is assessed. The benefits will not always be solely financial. Managers need to use their own professional knowledge and experience to judge whether the financial cost of risk control is justified in terms of non-financial benefit to the Authority. On occasions, managers may conclude that the cost of the control action may outweigh the benefits which will accrue to the Authority as a result of the action being taken. In such instances, all or an element of the risk is retained. However, no statute should be breached when making this decision.

7.5 For each risk actions should be identified, the officer responsible and timescales. Responsibility for drawing up the action plans lies with the Management Team (for strategic risks) and with service managers for service / operational risks

8. Risk Monitoring

8.1 To complete the risk management cycle, there must be monitoring and review of:-

- The implementation of the agreed risk control action plan;
- The effectiveness of the action in controlling the risk; and
- How the risk has changed over time.

Monitoring and review ensures that we continually learn 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 event
- Detecting changes in the external and internal context
- Identifying emerging risks

9. Risk assurance

Successful management of risk depends on four important risk based outputs which have been identified as follows:

Mandatory as required by laws, customers/clients and standards

- Assurance for our Management Team and other stakeholders
- Decision making based on the best information available

Effective and efficient core processes through our organisation.

10. Communication and Consultation

Communication and consultation with external and internal stakeholders takes place during all stages of risk management. In addition, as part of the communication process, the reporting of risks to management and the Board is most important. The reporting pattern is shown in the diagram below.

Figure 1 Risk Reporting Structure

11. Adding value

Risk management provides extra value to the Authority. In particular it is important to emphasize that employees will

- only take risks where there are likely to be benefits from doing so; and
- focus on risks where benefits could be enhanced, or the likelihood of success could be improved, or the likelihood of negative impact reduced.

It is important to ensure that risk management is having an impact – and change it if it is not doing so. It is also necessary to be proportionate paying more attention may be appropriate for larger interventions.

12. Revision History

A record should be maintained of all revisions to the Corporate Risk Strategy as shown below.

Version	Date	Summary	Name

Appendix 2: Corporate Risk Register and Project Risk Registers

Format of Risk Registers

Risk registers are commonly prepared either as tables in Word format or in Excel spreadsheet format. The Word format generally includes more narrative descriptions and response actions to provide a one-stop approach to the document whereas the Excel format often provides a tabular listing with reference to other documentation outlining further details of the issues.

Project Risk Register Templates

Risk management register templates are readily adaptable to include the corporate risk strategy risks and the project risks in the respective portfolios. There are clear advantages of using this approach principally because of the interactive facility, common approach and accessibility through Share point.

The complete **Corporate Risk Register** and the **project risks** identified in the Transportation and **Housing portfolios** are shown in Appendix 2 and have been transferred to the risk issue template can be viewed through the following link:

https://cambridgeshirepeterborough.sharepoint.com/:x:/s/CPCATeamSite/ERL7V3hIjeJNn6zjBg9wMR4BpYQhx34-30Ls0mfYGMtxzQ?e=0FdOg3