CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY | JAMES PALMER CAMBRIDGESHIRE & PETERBOROUGH MAYOR

Risk Management Strategy

Cambridgeshire and Peterborough Combined Authority (CPCA)

Contents

1. Introduction

This Risk Management Strategy outlines the approach taken by the Cambridgeshire and Peterborough Combined Authority (CPCA). This guide describes the specific management activities that will be undertaken for the organisation and the individual portfolios within CPCA.

Risk management is the effective way to manage risk before it becomes an issue. It also implements processes to deal with risk escalation, de-escalation, and issue management.

The British Standard from ISO31000:2018 defines risk management as “coordinated activities to direct and control an organisation with regard to risk”. They also define a risk as “effect of uncertainty on objectives– an effect is a deviation from the expected. It can be positive, negative or both, and can address, create, or result in opportunities or threats”.

By CPCA definitions, a risk can be either a threat (i.e., uncertain event that could have a negative impact on objectives or benefits) or an opportunity (i.e., an uncertain event that could have a favourable impact on objectives or benefits).

The benefits gained from effectively managing risk include:

- Encouraged proactive management – strategic, operational, and financial.
- Increased likelihood to deliver against objectives and targets.
- Improved identification of opportunities and threats.
- Improved operational effectiveness and efficiency.
- Improved CPCA learning.
- Improved CPCA resilience.

Issues are risk events that have happened. These were not planned and require immediate management actions. Risks, when they occur, become issues or as otherwise known “become realised”.

The Risk Management Strategy implements section 6.3 of the Assurance Framework. “It is important that the level of risk taken on any project and programme is understood from an early stage alongside the associated cost implications. Project managers are required to include risk as part of funding requests”.

2. Risk Policy

CPCA recognises the need for risk management to feature in our strategic, operational planning and decision-making governances. CPCA will agree appropriate Risk Appetite and Risk Tolerances levels to be used within the organisation. CPCA is also committed to managing and minimising risk by identifying, analysing, evaluating, and treating risks that may impact the future success of the organisation. This approach has the following aims:

- All staff to develop a sound understanding of the principles of risk management.
- Issues are avoided, or if realised they have a reduced financial impact by an increased understanding of risk and quickly identifying mitigation responses.
- Risk management is embedded within the organisation and also in the decision making by providing visibility of risks.

The Government’s Orange Book (Management of Risk – Principles and Concepts) advises “effective risk management should support informed decision-making in line with this risk appetite, to ensure confidence in the response to risks, transparency over the principal risks face and how these are manged”.

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

CPCA is a complex organisation with different portfolios, these include:

- Business & Skills.
- Delivery & Strategy.
- Housing.
- Corporate Services.

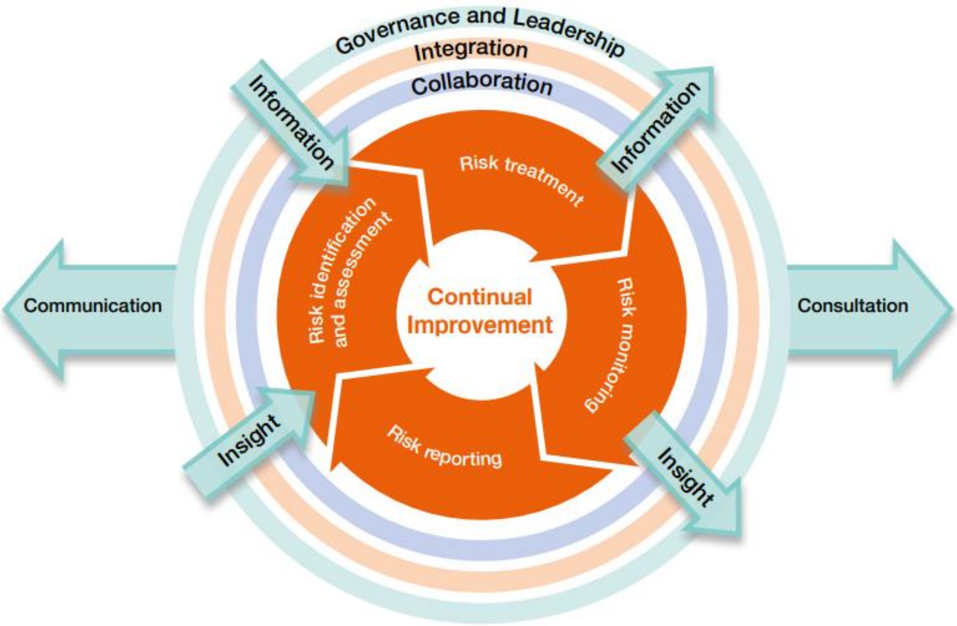
When dealing with particular projects within these portfolios, guidance is used through the Government's Orange Book, as well as Supplementary Green Book Guidance for Optimism Bias.

3. Risk Management Aims and Objectives

The aim of risk management is to ensure that CPCA has an effective process to support better decision making through good understanding of risks and the likely impact these risks may have. In general terms, "risk management" refers to the architecture (principles, framework, and process) for managing risks effectively, while "managing risk" refers to applying that architecture to individual risks.

The Orange Book advises that "Risk management frameworks support the consistent and robust identification and management of opportunities and risks within desired levels across an organisation supporting openness, challenge, innovation and excellence in the achievement of objectives".

Diagram 1: The Orange Book framework is shown below:



In order for CPCA's Risk Management Strategy to be effective, all employees at CPCA should understand risk management. The core principles of the Risk Management Strategy are:

- Integral part of all CPCA processes.
- Part of decision making.
- Explicitly addresses uncertainty.
- Based on the best available information.
- Tailored approach.
- Takes human and cultural factors into account.
- Transparent and inclusive.
- Dynamic, iterative, and responsive to change.
- Facilitates continual improvement of CPCA.

These principles will be achieved by:

- Establishing clear roles, responsibilities, and reporting lines within CPCA for risk management.
- Following the Risk Management Methodology (Appendix 1).
- Effective communication with all CPCA employees.
- Monitoring progress in implementing the strategy and reviewing the risk management arrangements on an on-going basis.

As per the Assurance Framework (paragraph 6.30), "at project level, all projects are expected to outline, in detail, any identified risks during the business case development and due diligence processes. Once in delivery, ongoing risk registers are maintained and incorporated into the monthly highlight report".

Within CPCA, we have defined risk into four groups, to effectively implement the risk management strategy. The four risk groups are:

- Project.
- Programme.
- Portfolio.
- Corporate.

4. Roles and Responsibilities

Risk Management is an essential part of governance and leadership, and fundamental to how an organisation is directed, managed, and controlled at all levels. The table below outlines the key roles within the Risk Management Strategy: -

Table 1: Roles and Responsibilities – Project Level

Role	Responsibility / Action
Corporate Risk Owner / Chief Executive	• Authorises the risk and issue management strategy and its adjustment, improvement, and enforcement. • Ownership of strategic / corporate risks and issues, ensuring mitigation actions are dealt with at the appropriate senior level. • In charge of monitoring the strategy / corporate risk register. • Define clear rules for escalation and de-escalation. • Deploys a consistent language of risk management across the corporate, portfolio, programme, and its projects.
Portfolio Director	• Ownership of portfolio-level risk and issues. • Assures portfolio adherence to the risk management principles. • Define clear rules for escalation and de-escalation. • Deploys a consistent language of risk management across the portfolio, programme, and its projects. • Escalates items across the programme boundaries to Corporate Risk Owner for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the portfolio. • Coordinates risk and issue management interfaces with programmes. • Provides support and advice on risks and issues to programmes. • Allocates risk and issues as appropriate.
Programme Risk Owner	• Ownership of programme-level risk and issues. • Assures programme adherence to the risk management principles. • Deploys a consistent language of risk management across the programme and its projects. • Escalates items across the programme boundaries to Portfolio Director for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the programme. • Coordinates risk and issue management interfaces with projects. • Provides support and advice on risks and issues to projects. • Allocates risk and issues as appropriate.
Project Risk Owner	• Ownership of project-level risk and issues. • Assures the project adherence to the risk management principles. • Deploys a consistent language of risk management across the projects.

	• Escalates items across the programme boundaries to Programme Risk Owner for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the project. • Allocates risk and issues as appropriate.

Table 2: Roles and Responsibilities – Governance Level

Role	Responsibility / Action
Combined Authority Board	• Adopt and review the Risk Management Strategy. • Receive recommendations from the Audit and Governance Committee as to the Authority's arrangements for the management of risk and on the any concerns that risks are being accepted which the Authority may find unacceptable.
Business Board	• Review and challenge mitigation and exploitations at the appropriate level (in relation to matters directly controlled or indirectly accessible by the Business Board).
Audit and Governance Committee	• Initiates assurance reviews of risk and issue management effectiveness. • The Authority's Audit and Governance Committee is responsible for overseeing the Authority's risk management strategy and corporate risk register. They will approve the Risk Strategy 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 Committee to review and scrutinise the Authority's financial affairs and to review and assess its risk management, internal control and corporate. governance arrangements.
Internal Audit	• Responsibility to undertake sufficient work to establish whether the CA has "adequate and effective" risk management, control, and governance processes. • The Chief Internal Auditor provides an annual opinion on the overall systems of internal control and their effectiveness.
Monitoring Officer	• Manages and coordinates the resolution of risks relating to operational performance and benefits achievement. • Ensures that risk management cycle includes operational risks. • Manages risks that impact on business performance and transition. • Identifies operational issues and ensures that they are managed by the programme. • Identifies opportunities from the business operations and raises them for inclusion in the programme. • Contributes to impact assessments and change control. • Monitors and reports on business performance issues that may require the attention of the programme during transition.

Section 73 Officer	• The Chief Finance Officer is appointed under Section 73 Officer of the Local Government Act 1985 to ensure that proper administration of the financial affairs of the Combined Authority and Business Board. The Section 73 Officer is responsible for providing the final sign off for funding decisions. The Section 73 Officer will provide a letter of assurance to government by 28th February each year regarding the appropriate administration of government funds under the Cambridgeshire and Peterborough Investment. • The S73 office is also required to report to, and provide assurances to, the Audit and Governance Committee in relation to the Combined Authority's risk management and assurance mapping arrangements and has overall responsibility for maintaining adequate and effective internal control arrangements.
Project Management Office (PMO)	• Manages and coordinates the information and support systems to enable efficient handling of the programmes risk and issues. • Maintains the risk register for each programme. • Maintains the issue register for each programme. • Establishes, facilitates, and maintains the risk management cycle. • Establishes, facilitates, and maintains the issue management cycle. • Maintains the configuration management system (document control). • Facilitates the change control steps.

The Assurance Framework states that "Senior Officers of the Combined Authority (Chief Executive and S73 Officer) are responsible for the identification and management of risk (paragraph 6.3).

5. Arrangements for Managing Risk

The Risk Management Methodology to be employed at CPCA is outlined in Appendix 1, with a copy of the Issue Management Strategy within Appendix 2. The project risk and opportunity templates can also be found in Appendix 3. Dealing with risk events that have become issues are documented in Issue Log Appendix 4.

6. Monitoring Arrangements

To ensure that informed decisions are made, it is essential to identify key strategic risks for the CPCA. Strategic risks will be reviewed monthly by the Combined Authority Management Team, as detailed within the Assurance Framework, and will be documented in the Corporate Risk Register.

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

The Corporate Risk Register will also be reviewed by the Audit & Governance Committee on a quarterly basis as per the Assurance Framework. The Audit & Governance Committee ensures that CPCA is spending public money correctly and have the right systems in place to manage finances appropriately and meet legal and regulatory responsibilities. The Corporate Risk Register will be taken to board for review on annual basis.

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

In carrying out audits throughout the year, Internal Audit will also:

- 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.

In order to ensure risk management is effective, CPCA will:

- Measure risk management performance against indicators, which are periodically reviewed for appropriateness.
- Periodically measure progress against, and deviation from the risk management plan.
- Periodically review whether the Risk Management Methodology, policy and plan are still appropriate given CPCA internal and external context.
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed.
- Review effectiveness of Risk Management Methodology.

All Risk and Opportunity registers will be reviewed via an internal audit every quarter. The Risk team will also randomly select Risk and Opportunity registers at periodic times to ensure procedures are followed, this is also a good point of training. The Combined Authority Management Team can ask to review any Risk and Opportunity registers at any point.

7. Training and Communication Arrangements to Support Implementation of the Strategy

Training of the Risk Management Methodology (Appendix 1) will be provided to all employees with direct responsibility for involvement in the risk management process, such as:

- Corporate Risk Owner.
- Portfolio Director.
- Programme Risk Owner.
- Project Risk Owner.
- PMO.
- Board.
- Audit and Governance Committee.
- Internal Auditor.
- Monitoring Officer.
- Section 73 Officer.

Each new starter to the organisation will also be provided training on the Risk Management Strategy and all employees will be given a yearly update training. Subsequent training will be provided after any revisions are made to the Risk Management Strategy.

Risk Owners will be given additional training to ensure risks and mitigation plans and actions are effectively identified, recorded, and managed.

8. Review of the Risk Management Strategy

This strategy will be reviewed every three years. The next update will be in April 2023.

9. Appendices:

Appendix 1: Risk Management Methodology

Appendix 2: Issue Management Strategy

Appendix 3: Risk and Opportunity Register

Appendix 4: Issue Log.

10. Version Control:

Any amendments to the Risk Management Strategy should all be logged in the box below:

Version	Date	Comments
1.0	07/11/2019	First draft of Risk Management Strategy
2.0	05/12/2019	Finalised for inclusion to Audit and Governance Committee for 16th December 2019
3.0	25/03/21	Updated following RSM Audit Management Actions

11. References

1. Association for Project Management (APM) Book of Knowledge, 2014.
2. Managing Successful Programmes (MSP) Best Practice Management, 2011.
3. Cambridgeshire & Peterborough Combined Authority (CPCA) Risk Management Strategy, 2018.
4. British Standard – Risk Management – Principles and guidelines, BS ISO 31000:2018.
5. Orange Book: Management of Risk – Principles and Concepts, 2020. Including Risk Appetite Guidance Note.
6. Supplementary Green Book Guidance, Optimism Bias, HM Treasury.
7. Cambridgeshire & Peterborough Combined Authority (CPCA) Constitution, 2021.
8. Cambridgeshire & Peterborough Combined Authority (CPCA) Assurance Framework, 2021.
9. Cambridgeshire & Peterborough Combined Authority (CPCA) Relationship between Risk and Change Control, 2021.

Appendix 1. Risk Management Methodology

1. Risk Appetite and Risk Tolerance

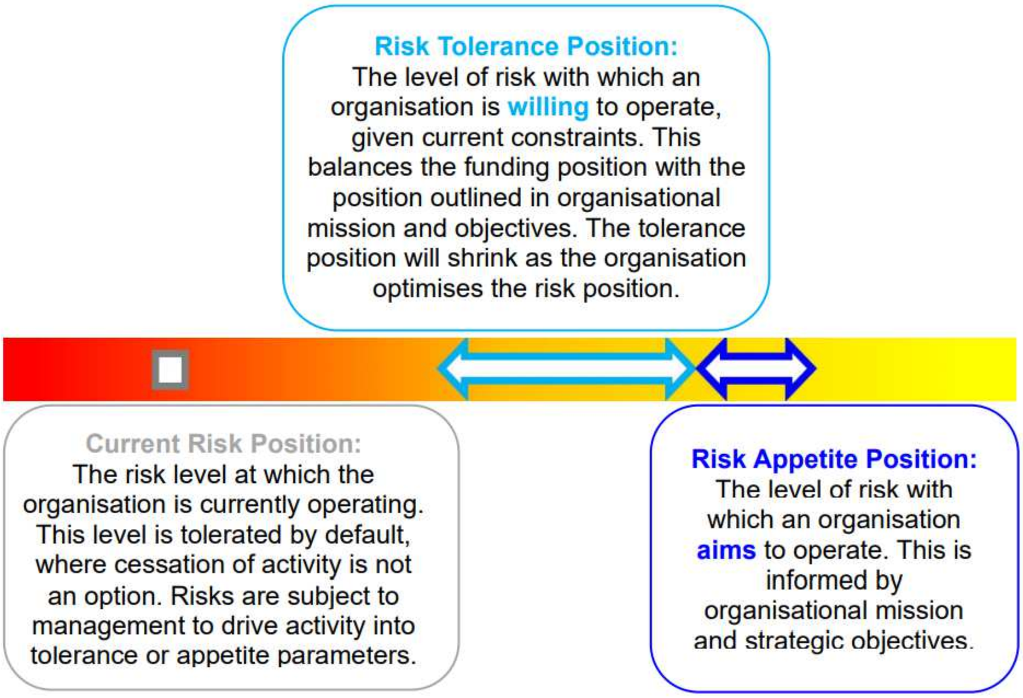
An individual risk is defined as "either a threat (i.e., uncertain event that could have a negative impact on objectives or benefits) or an opportunity (i.e., an uncertain event that could have a favourable impact on objectives or benefits)".

The amount of risk that CPCA is willing to accept is based on the Risk Appetite and Risk Tolerance. The Orange Book defines Risk Appetite and Risk Tolerance as the following:

- **Risk Appetite**: the level of risk with which an organisation **aims** to operate.
- **Risk Tolerance**: the level of risk with which an organisation is **willing** to operate.

This is demonstrated in the diagram below:

Diagram 1: Orange Book interaction between Risk Appetite and Risk Tolerance:



Risk Tolerance Position: The level of risk with which an organisation is **willing** to operate, given current constraints. This balances the funding position with the position outlined in organisational mission and objectives. The tolerance position will shrink as the organisation optimises the risk position.

Current Risk Position: The risk level at which the organisation is currently operating. This level is tolerated by default, where cessation of activity is not an option. Risks are subject to management to drive activity into tolerance or appetite parameters.

Risk Appetite Position: The level of risk with which an organisation **aims** to operate. This is informed by organisational mission and strategic objectives.

Risk appetite provides a framework which enables the CPCA to make informed management decisions. By defining risk appetite and risk tolerance, the CPCA clearly sets out both an optimal and acceptable position in the pursuit of its strategic objectives. The benefits of using this approach are:

- Supporting informed decision-making.
- Reducing uncertainty.
- Improving consistency across governance mechanisms.
- Supporting performance improvement.
- Focusing on priority areas.
- Informing spending review and resource prioritisation processes.

This is applied to all risks identified and is supported by appropriate financial risk appetite and tolerance levels. CPCA has defined Risk Appetite and Risk Tolerance as:

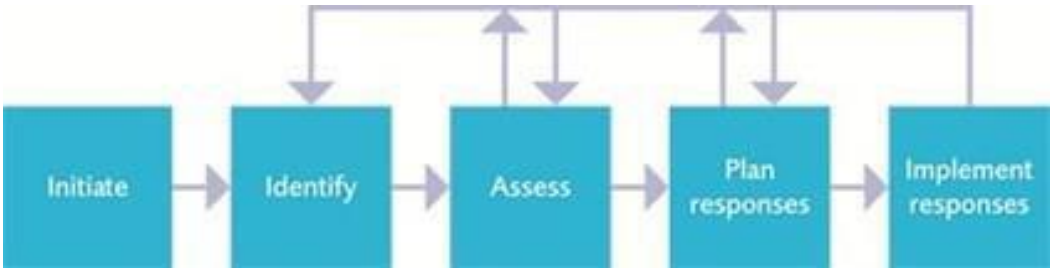
- Risk Appetite is defined as the amount and type of risk that an organisation is prepared to seek, accept, or tolerate.
- Risk Tolerance is an organisation's readiness to bear the risk or opportunity, after treatments established, in order to achieve its objectives.

These definitions and additional information relating to this is found within the CPCA Relationship between Risk and Change Control document.

2. The Risk Management Cycle

There are 5 key stages in the risk management cycle: Initiate; Identify; Assess; Plan; and Implement:

Diagram 2: Risk Management Cycle



The 5 stages of risk management are part of a cycle. Risk management is dynamic, and the identification phase needs to be carried out continuously. As the process is repeated throughout the project/programme/portfolio lifecycle, the assessment or response planning stages can lead to the identification of further risks and planning and implementing responses can trigger a need for further analysis and so on.

A key output from the initiation step is the risk management plan, which details how risk will be managed throughout the life cycle.

3. Initiate

The main output for the initiation phase is the Risk Management Framework or Risk Management Strategy.

This describes the key elements on how risk management will be implemented:

1. Scope.
2. Objectives.
3. Roles and Responsibilities.
4. Process.
5. Tools.

4. Risk Identification (what can happen and how can it happen?)

Risk identification starts with uncertain events being articulated as threats and opportunities. Uncertain events are also identified as a project, programme, portfolio, or corporate risk.

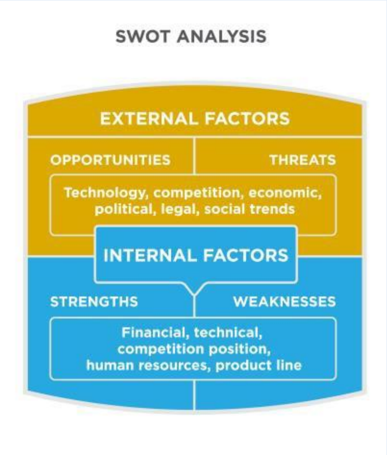
Definitions for these risk groups can be found below:

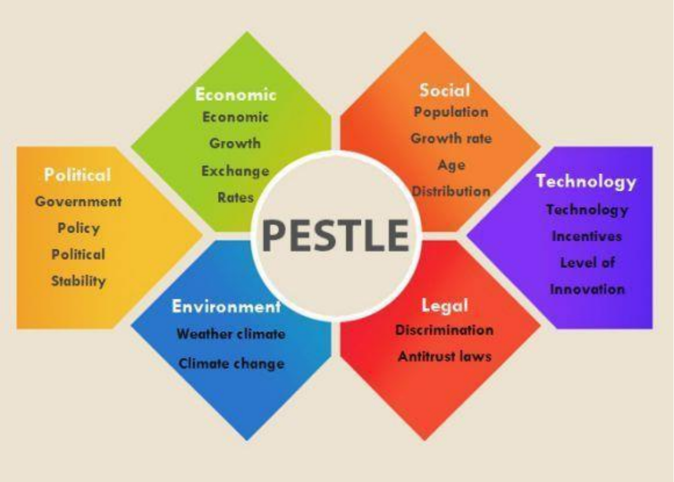
- Project – has a specific impact on a single project only.
- Programme – has common attributes across multiple projects (within an interdependent group of projects) and may affect the delivery of those associated projects.
- Portfolio – distinct directorial area, made up of a collection of individual projects and programmes that are not necessarily interdependent of each other e.g., Business & Skills, Corporate Services, Housing, Transport & Strategy.
- Corporate – refers to the liabilities and opportunities that positively or negatively impact CPCA as an organisation.

Identification techniques draw on various sources of information. Identification of risks from previous projects, programmes and portfolios involves looking at lessons learned reports and risk registers.

The aim of the risk identification process is to generate a comprehensive list of risks, with relevant and up to date information important in identifying these risks. A variety of risk identification processes may be used as exemplified in the table below.

Table 1: Risk Identification Techniques

Risk Identification Techniques	
Technique	Description
Risk Gap Analysis	Using a list of common risks as a discussion point in risk reviews.
Workshops & Brainstorming	Collection and sharing of ideas that could impact the objectives of the project / objective.
Audits and Inspections	Physical inspections of premises and activities and audits of compliance with established systems and procedures. Flowcharts and dependency analysis of the processes and operations within the organisation to identify critical components that are the key to success.
SWOT analysis	Considering a project/programme/organisation's Strengths Weaknesses Opportunities Threats (SWOT) – opportunities and threats are usually external risks, while strengths and weakness are normally internal risks.  SWOT ANALYSIS EXTERNAL FACTORS OPPORTUNITIES THREATS Technology, competition, economic, political, legal, social trends INTERNAL FACTORS STRENGTHS WEAKNESSES Financial, technical, competition position, human resources, product line

PESTLE analysis	Considering potential sources of risk arising from six possible elements: Political, Economic, Social, Technological, Legal & Environment (PESTLE)  Political Government Policy Political Stability Economic Economic Growth Exchange Rates PESTLE Social Population Growth rate Age Distribution Technology Technology Incentives Level of Innovation Environment Weather climate Climate change Legal Discrimination Antitrust laws

Risks should be identified whether or not their sources are under CPCAs direct control. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or significant opportunity.

5. Risk Assessments (Determine the likelihood and impact)

The assessment of risk can be broken down into how likely it is that a risk might become an issue, and what impact that issue would have. These are defined as likelihood and impact:

- The probability of an event occurring and when they might happen – **likelihood.**

- The potential severity of the consequences (positive and negative) should such an event occur – **impact.**

The following table below provides likelihood and impact descriptors to assist with this process:

Table 2: Likelihood vs Impact definitions

Likelihood	
1	Rare – This event may occur but only in exceptional circumstances (0-5%)
2	Unlikely – Not likely to not occur under normal circumstances (6-20%)
3	Moderate - Given time likely to occur (21-50%)
4	Likely – The event will probably occur in most circumstances (51-80%)
5	Almost Certain – This event is expected to occur soon (81-99%)

Impact	
1	Negligible – Risks may have minimal damage / gain or long-term effect
2	Marginal – Risks may have minor loss / gain but little overall effect
3	Significant – Risks may have considerable loss / gain.
4	Major – Risks may have significant loss / gain.
5	Monumental – Risks may have extensive loss / gain and long-term effect.

When discussing the impact of risks, it is important that we are not just focusing on the impact to the individual project/programme and that we also consider the impact that can affect the strategic objectives of CPCA. It should be noted that, while the likelihood assessment should not change, the impact assessment may change when risks are escalated from project to programme to portfolio to corporate risks: this reflects that a risk may be critical to a project's outcomes, but that project may not be critical to the CPCA's outcomes as a whole.

When discussing the impact (positive or negative) a risk can have on a project, programme, portfolio or corporate, it is important to remember to use the following criteria. These are:

- Cost
- Time
- Quality
- Safety
- Operational Impact
- Reputation

Once every risk has been given a score for its likelihood x Impact, it is given an overall score and corresponding RAG status (Red Amber Green Rating).

Table 3: Overall RAG Status

Overall RAG Status		Impact				
		1	2	3	4	5
Likelihood		Negligible	Marginal	Significant	Major	Monumental
5	Almost Certain	**5**	**10**	**15**	**20**	**25**
4	Likely	**4**	**8**	**12**	**16**	**20**
3	Moderate	**3**	**6**	**9**	**12**	**15**
2	Unlikely	**2**	**4**	**6**	**8**	**10**
1	Rare	**1**	**2**	**3**	**4**	**5**

Priority will be given according to the RAG Status:

- Red – Require immediate action plans.
- Amber – Require action plans and / or to be closely monitored as appropriate.
- Green – Can be "Accepted" and may not require action plans.

The RAG rating is an indicator to determine the severity of a risk and is a qualitative assessment to identify the inherent risk score (risk scored without controls). Risks are also quantitively assessed and appropriate risks are given a financial value (although this may not be appropriate for all risks and opportunities).

For example, a risk relating to an additional planning application would require a financial value whereas a risk around a consultation event potentially receiving bad publicity would not.

The risk owner is responsible for providing an approximate financial value of each risk but should consult the project team, supplier, or any other relevant person to help quantify.

The qualitative and quantitative assessment determines the Risk Tolerance.

Risk Tolerance is the measure of the degree of uncertainty that a stakeholder/organisation accepts in respect of the project/programme/portfolio risk assessment. Additional guidance on appropriate levels of Risk Tolerance can be found within the CPCA Relationship between Risk and Change Control document.

Just as risks can increase in RAG status, they can also decrease with the right mitigation or change in circumstance. A risk that was deemed as red at the beginning of the project can be moved down to green throughout the project lifecycle. The current RAG rating is called the Project/Programme/Portfolio/Corporate Risk Status.

Risks are recorded on the Risk and Opportunity Register for that project, programme, or portfolio. Templates and guidance for this is found in Appendix 3. Corporate Risks are stored on the Corporate Risk Register.

6. Mitigation and Risk Control

Having prioritised the risk, it is now necessary to determine a potential response for the higher risk events. There are two things to do here:

1. Determine what can be done to reduce the probability of the risk occurring (therefore, reducing its likelihood).
2. Determine a plan and set aside contingencies to deal with if it does become realised. (therefore, reducing its impact)

This process is called mitigation. *An example of risk events and planned responses are shown below*:

Table 4: Risk Events and Responses

Risk Event	Consequences	Mitigation action to reduce probability	Contingency actions to deal with the event if it occurs
Bad weather happens on a key date.	There may be delays in replacing the roof, thereby causing delays and potential overspend.	Do roofing work during drier months.	Erect protective sheeting above roof while work takes place. Stop work and move workers inside during bad weather.
The new server does not arrive in time.	The software testing cannot take place.	Make sure it is purchased from a reputable supplier.	Provide a delay between planned delivery and testing starting. Purchase two as a spare.
The staff do not accept the new working practices.	Poor customer service and morale.	Make sure staff are communicated with early in the process.	Have a long transition phase. Hire temporary staff while changes and alterations are made.

Risk Control is the process of acting to minimise the likelihood of the risk event occurring and/or reducing the severity of the consequences should it occur. This will be applied on risk and opportunities. There are 8 main options to consider, 4 for risk and 4 for opportunities.

Risk

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.

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, aspect that was not previously discussed that will achieve some extra benefit.
4. **Share** – Seek partners with whom can actively capitalise on the circumstances such as a Joint Venture.

After the Risk Assessment and controls are placed, the risk is RAG rated again. This is called the Residual Risk score (with controls considered).

Mitigation is based on two aspects:

- **Mitigation Plan (Current Controls)** – what CPCA currently does.

- **Mitigation Action (New Controls)** – what CPCA could do in addition.

All mitigation should be SMART:

- **Specific** – state what will be done.
- **Measurable** – provide a way to evaluate.
- **Attainable** – within scope and possible to accomplish.
- **Relevant** – to the project, programme, or portfolio.
- **Time-based** – state when the mitigation will be completed.

Care is needed when arriving at any response to risk because regardless of what action is taken, there is the potential to generate other risks.

Where appropriate, arrangements for contingency, containment, and continual management should be developed, as well as crisis and incident arrangements. This should also be communicated to support resilience and recovery if a risk becomes an issue. When a risk can no longer be mitigated and the risk becomes realised, it is then called an "Issue". This requires a different management strategy, and this can be found in Issue Management Strategy (Appendix 2).

7. Implement Risk Responses

The primary goal of the implement element is to ensure that the planned risk management (mitigation and control) actions are monitored as to their effectiveness and corrective action is taken where responses do not match expectation.

An important part of this is to understand the roles and responsibilities outlined in Table 1 of the Risk Management Strategy. This ensures that at least one individual is always clearly identified as the risk owner, and another individual is identified as the rick actioner. The key roles are:

- **Risk Owner** – Responsible for the management and control of all aspects of risk assigned to them, including managing, tracking, and reporting the implementation of the selected actions to address the threats or to maximise the opportunities.
- **Action Owner** – Responsible for the implementation of risk response actions. They support and take direction from the risk owner.

Anyone can raise a risk. Just because an employee and or stakeholder raises a risk, this does not necessarily make them the Risk Owner. A Risk Register can have many risk owners.

8. Risk Escalation from Project to Corporate

Risk Escalation is the term used when a project risk is deemed to be a programme/portfolio or even a corporate risk. The decision to escalate a project risk to a programme risk is taken by the Programme Risk Owner. A risk should be escalated from a project to a programme risk when the project risk is deemed to have an impact on the programme.

For example, if a project needs to deliver a particular output in order for another project within that programme to be completed. This also works the same for when a programme risk has impact on a portfolio. The risk will then be escalated by the Portfolio Risk Owner. Another example is that at project level, a small risk can have limited effect, but when a project risk is combined with other risks in adjacent projects, it can produce a significant impact on a programme or portfolio.

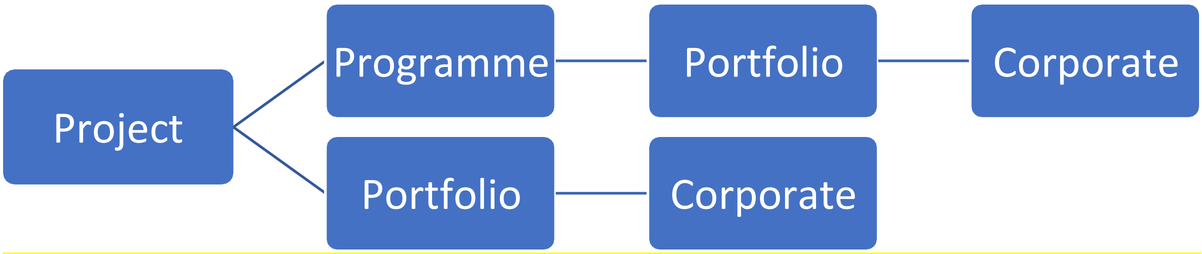
Therefore project, programme, portfolio, and corporate risks can:

- Accumulate to critical loss and or damages.
- Grow (where the sum of the risks is bigger than individual parts).
- Reduce (where the sum of the risks is smaller than individual parts).

Within the CPCA, project risks can be escalated from programme to portfolio and then to corporate risk level. As previously defined, a programme is a collection of projects which have an interdependent link, while a portfolio is a collection of individual projects and programmes not necessarily having that interdependent link. Therefore, a project risk can have significance on an individual project but also have the opportunity to affect the delivery of a portfolio.

Below is a diagram showing this Risk Escalation process.

Diagram 3: Risk Escalation Process



It is the decision of the relevant Risk Owner (as per the Roles and Responsibility table within the Risk Management Strategy) to decide to escalate the risk. A risk can be deemed to have project, programme, portfolio, and corporate significance and therefore might stay on all three risk registers with different levels of action / mitigation and different risk owners.

Just as risks can be escalated up the chain, risks can also be de-escalated when the risk no longer is significant.

It is important to remember that no matter which level the risk sits, that the risk is managed effectively and review on a regular basis to ensure the appropriate escalation and de-escalation happens.

9. Review Monitoring and Review

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 meeting such as Risk Reviews, Programme Reviews etc) or ad hoc. A combination of both ensures that risks are reviewed regularly, and the mitigation and action plan are up to date.

Risks will need to be monitored to ensure that any controls or mitigation remain operational in order to manage them during the risk management cycle. Just because a risk is deemed as "Accepted" does not mean that this risk is forgotten about.

Below are the monitoring requirements for risks with Residual RAG Scores:

Table 5: Risk Monitoring Arrangements via Residual RAG Scores

RAG Status	Monitoring Arrangements
Red – Residual risk score above 12.	- Reviewed frequently with Action Owner and Risk Owner (minimum every 2 days). - Reviewed as to whether this risk requires escalation with the appropriate Risk Owner. - Ensure the controls and mitigation are appropriate for the risk. - Reviewed at Project Board, Committee, Business Board or Combined Authority board - if appropriate.
Amber – Residual risk score between 5-11.	- Reviewed with the Action and Risk Owner (minimum weekly). - Ensure the controls and mitigation are appropriate for the risk. - Reviewed with the Risk Owner at the next escalation level.
Green – Residual risk score between 1-4.	- Reviewed with the Action and Risk Owner (minimum bi-weekly). - Ensure the controls and mitigation are appropriate. - Reviewed with the Risk Owner at the next escalation level.

*The above is subject to change. If the risk requires immediate attention, this will be reviewed by Corporate Management Team. As the risk are reviewed and updated, the RAG score is likely to reflect this change. Some risks may require more frequent evaluation.

Monitoring and review ensure 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.

Open culture tool for improvement – good mission statement.

Appendix 2: Issue Management Strategy

1. Introduction

An issue is a relevant event that has happened, was not planned, and requires management actions. The action may be to fix the problem that has caused the event to happen in the first place, or to change the boundary of the project/programme.

Issue management is the process of identifying and resolving issues. Problems with staff or suppliers, technical failures, material shortages for example all have a negative impact on your project. If the issue goes unresolved, you risk creating unnecessary conflicts, delays, or even failure to produce project objectives.

Issues and risks are not quite the same thing, however the exact nature of both is largely unknown at the start of a project. The Risk Management Methodology (Appendix 1) highlights how to identify and assess all potential risks. Issues, however, have to deal with as they happen. Issue management is therefore a planned process for dealing with an unexpected issue – whatever that issue may be – if and when one arises.

Issues can typically be classified into one of the following three types:

1. A previously identified risk that has now materialised and requires appropriate issue management action.
2. A request for change to some aspect of the programme, an operation, or a project
3. A problem affected all or part of the programme/project in some way.

2. Issue Register

Issues are recorded in the Issue Log (Appendix 4). The Issue Register is similar to the Risk Register and is a repository that focuses on all identified issues that have occurred. It includes former risks if they have materialised from previous projects / programmes / programmes to ensure a Lessons Learned approach. On the Project Risk and Opportunity Register template (Appendix 3), under column "Risk Status" it allows the risk status to be updated to "realised". Once the risk becomes realised, these are then migrated to the Issue Log (Appendix 4).

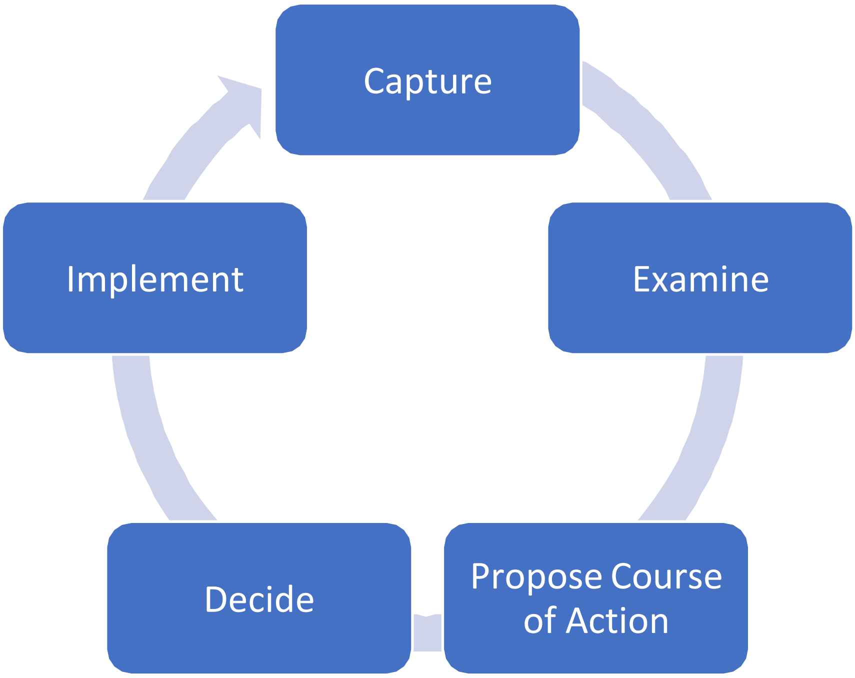
Having an Issue Register allows CPCA to:

- Have a safe and reliable method for the team to raise issues.
- Track and assign responsibility to specific people for each issue.
- Analyse and prioritize issues more easily.
- Record issue resolution for future reference and project learning.

3. Issue Management Methodology

Like the Risk Management Methodology (Appendix 1) the Issue Management Methodology is a cycle with 5 steps, shown below:

Diagram 1: Issue Management Cycle



Within these 5 steps there are two ongoing activities. These are:

1. **Monitor and Control** ensures that the decision can be achieved within the estimates of time and cost and that the impact of the overall risk profile is not greater than anticipated.
2. **Embed and Review** ensures that issue management is being appropriately and successfully handled within each programme and ultimately across the organisation. It looks at each individual step of the cycle to determine its contribution to the overall quality of issue management.

1. Capture

The first step is to undertake an initial analysis to determine the type of issue that has been raised. When capturing the issue, it should be assessed by its severity and impact on the portfolio/programme/project and also allocated to an individual or group of people for examination.

When allocating an issue, the initial decision might be to direct the issue to where it can most appropriately be managed. Some issues will be managed by the Programme, and major issues might need to be managed at Portfolio level when outside the authority of the programme. Smaller issues might need to be managed at project level.

2. Examine

The next step is to examine the issue by undertaking impact analysis. The analysis should consider the impact that the issue, and the options for its resolution, will have on:

- The portfolio/programmes performance, especially how benefits are realisation will be affected.
- The portfolio/programmes/projects business case.

- The portfolio/programme risk profile – the impact on the overall risk exposure.
- The operational performance of the organisation and existing plans.
- Suppliers contact or service level agreements.

Impact analysis must include a broader view, the portfolio, the programme, its projects, operations, and strategic objectives. As a minimum, an issue should always be assessed against the impact on the projects/programmes objects and benefits.

3. Propose Course of Action

Alternative options should be considered before proposing a course of action to take. The action chosen should maintain an acceptable balance between the advantage to be gained (benefits) and the impact on cost, time, and risk. When the concurrent change initiatives affect the same operational areas, this acceptable balance may require an assessment across these other portfolio, programme, and projects.

Some changes may be mandatory, *for example to comply with new legislation*. Therefore, the action might be to then achieve compliance with minimum impact. However, in such cases the analysis work should explore where the mandatory change opens up other opportunities to improve the portfolio/programmes/projects performance and benefits.

4. Decide

As per the Risk Management Strategy Section 4, the roles, and responsibilities in terms of Risk and Issues have been defined. A table below demonstrates these roles and responsibilities set out relating to Issue Management:

Table 1: Roles and Responsibilities

Role	Responsibility / Action
Corporate Risk Owner	• Authorises the risk and issue management strategy and its adjustment, improvement, and enforcement. • Ownership of strategic / corporate risks and issues, ensuring mitigation actions are dealt with at the appropriate senior level. • In charge of monitoring the strategy / corporate risk register. • Define clear rules for escalation and promotion. • Deploys a consistent language of risk management across the corporate, portfolio, programme, and its projects.
Portfolio Director	• Ownership of portfolio-level risk and issues. • Assures portfolio adherence to the risk management principles. • Define clear rules for escalation and promotion. • Deploys a consistent language of risk management across the portfolio, programme, and its projects. • Escalates items across the programme boundaries to Corporate Risk Owner for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the portfolio.

	• Coordinates risk and issue management interfaces with programmes. • Provides support and advice on risks and issues to programmes. • Allocates risk and issues as appropriate.
Programme Risk Owner	• Ownership of programme-level risk and issues. • Assures programme adherence to the risk management principles. • Deploys a consistent language of risk management across the programme and its projects. • Escalates items across the programme boundaries to Portfolio Director for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the programme. • Coordinates risk and issue management interfaces with projects. • Provides support and advice on risks and issues to projects. • Allocates risk and issues as appropriate.
Project Risk Owner	• Ownership of project-level risk and issues. • Assures the project adherence to the risk management principles. • Deploys a consistent language of risk management across the projects. • Escalates items across the programme boundaries to Programme Risk Owner for resolution where necessary. • Communicates the progress of the resolution of issues in a clear and timely fashion across the project. • Allocates risk and issues as appropriate.

The Programme / Project Risk Owner may be able to resolve or delegate minor issues without reference to any other role for a decision. Some issues, however, may need to be referred to the Corporate Risk Owner or Portfolio Director or the proposal may need to be referred to a specialist role (monitoring officer or Section 73) when it involves business change.

If a decision for change is made, then this change should be planned with appropriate recognition of the need for contingency, additional resources and a fall-back plan should the change cause unexpected problems.

When a decision is made there will also need to be an issue owner, issue actioner and a response action plan identified. The Issue Register should also be updated.

5. Implement

The decision and response action plan will be communicated to the appropriate stakeholder for several reasons:

- So that personnel, especially each issue actioner, are aware of changes to their work schedules and can undertake their assigned tasks to fix the problems and implement the changes.

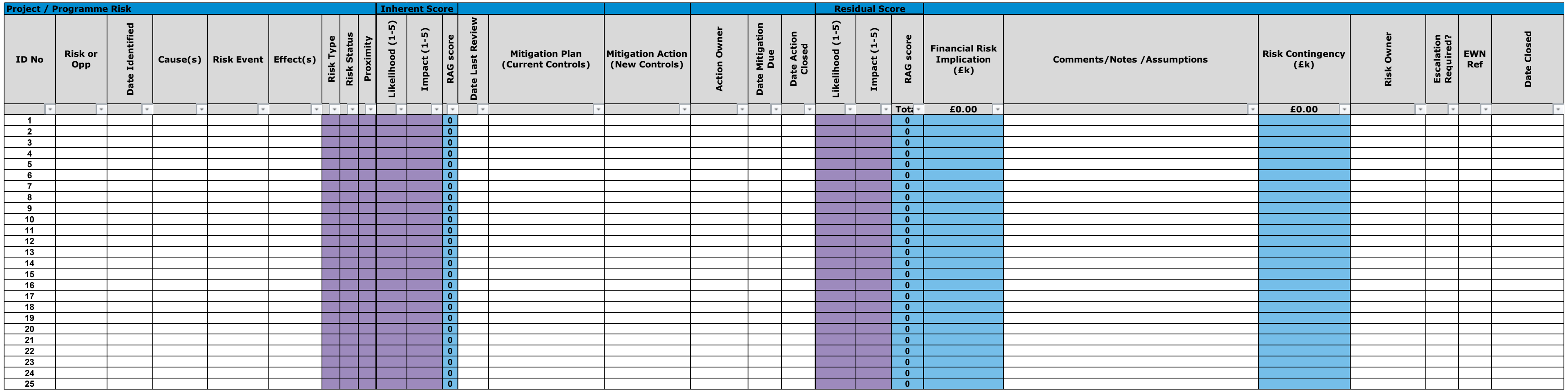
- To inform those who raised the issue and what course of action is being perused.
- To inform stakeholders who may be affected by the change (suppliers, contractors etc)
- To demonstrate effective management of the project/programme/portfolio.

The issue register is updated, and all other documents are revised whether the decision affects the content. In majority of cases the programme plan will need to be updated as well.

The change is then applied, and the impact of the change monitored, and lessons learned from its introduction. The impact of these should be used for the assessment of future changes/issue management.

As stated previously this a continual cycle and should be monitored and reviewed regularly to ensure compliance.

Appendix 3: Risk and Opportunity Register



Project / Programme Risk									Inherent Score									Residual Score									
ID No	Risk or Opp	Date Identified	Cause(s)	Risk Event	Effect(s)	Risk Type	Risk Status	Proximity	Likelihood (1-5)	Impact (1-5)	RAG score	Date Last Review	Mitigation Plan (Current Controls)	Mitigation Action (New Controls)	Action Owner	Date Mitigation Due	Date Action Closed	Likelihood (1-5)	Impact (1-5)	RAG score	Financial Risk Implication (£k)	Comments/Notes /Assumptions	Risk Contingency (£k)	Risk Owner	Escalation Required?	EWN Ref	Date Closed
																				Tot	£0.00		£0.00				
1											0									0							
2											0									0							
3											0									0							
4											0									0							
5											0									0							
6											0									0							
7											0									0							
8											0									0							
9											0									0							
10											0									0							
11											0									0							
12											0									0							
13											0									0							
14											0									0							
15											0									0							
16											0									0							
17											0									0							
18											0									0							
19											0									0							
20											0									0							
21											0									0							
22											0									0							
23											0									0							
24											0									0							
25											0									0							

Appendix 4: Issue Log

Issue Management - Project / Programme											
Issue ID	Project ID and Project Name (if applicable)	Programme Directorate (drop down)	Issue Logged	Status (drop down)	Severity (drop down)	Priority (drop down)	Dated Reported	Issue Owner	Issue Actioner	Response Action Plan	Last Updated
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											