Appendix 1

Sheffield City Region MAYORAL COMBINED AUTHORITY

Risk Management

Contents **Page**

Foreword

Sheffield City Region Mayoral Combined Authority (MCA) is responsible for the strategic economic development decision making for the Sheffield City Region (SCR). The MCA works closely with the private sector led Local Enterprise Partnership (LEP) to ensure local business representatives are actively involved in decision making processes.

The MCA Executive Team provides impartial advice to the MCA and LEP encompassing the development of policy, strategy, programme commissioning and assurance at a regional level in order to meet the objective of growing the City Region economy.

The MCA is committed to delivering its strategic objectives, whilst having a keen the awareness of threats that may impact its planned outcomes, and a clear focus on the management of these risks.

This document sets out the MCA's approach to risk management and aims to explain the purpose of risk management. It also communicates why and how risk management is implemented by the MCA Executive team (on behalf of the MCA) encompassing the work of the MCA, the LEP and the Mayor.

It provides assurance to those accountable that appropriate and robust arrangements are in place to manage risk. It guides those undertaking risk management activities through the application of the principles of risk management and provides a defined process to ensure that any particular piece of activity has the best chance of achieving its objectives.

It should be read in conjunction with the Corporate Plan and the Assurance Framework.

What is Risk Management

What do we mean by ‘risk’?

Risk is defined as ‘an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by the combination of the probability of a perceived threat or opportunity occurring and the scale of its impact on objectives’.

Why should we manage risk?

Risk management is vital to the successful delivery of the work of the MCA, the Mayor and LEP and is likely to improve performance against objectives in the following ways:

- There should be fewer sudden shocks and unwelcome surprises
- We should be able to use our resources more efficiently
- It allows us to be more innovative
- It increases the likelihood of objectives being achieved
- It provides for more focus on doing the right things properly
- It reduces time spent ‘firefighting’

The importance and value of risk management is also supported by the fact that evidence of effective risk management is required by the **Accounts and Audit Regulations 2015,** and an assessment of the robustness of risk management arrangements influences the value for money (vfm) conclusion awarded through the external audit process. In addition, the **HM Treasury Orange Book** places an obligation on public bodies with responsibility for public funds to ‘actively seek to recognise risks and direct responses’ and, principle F of **CIPFA’s Delivering Good Governance in Local Government (2016)**, outlines risk management as an important and integral part of performance management and crucial to the achievement of outcomes.

What is our approach to managing risk?

The MCA has adopted the ‘Management of Risk’ (MoR®) principles of risk management which are aligned to the international standard for risk management ISO31000:2009.

The principles are that risk management:

- Aligns with objectives
- Fits the context
- Engages relevant stakeholders
- Provides clear guidance
- Informs decision making
- Facilitates continual improvement
- Creates a supportive culture
- Achieves measurable value

The objective of risk management is to provide a methodical application of these principles, a defined process to the task of identifying and assessing risks, and to planning and implementing risk responses which, in turn provide a disciplined environment for proactive decision making.

A common vocabulary for risk management has been adopted. This ensures all participants speak the same language and there is no ambiguity. A glossary of the terms can be found at annex A.

How we use risk management across the organisation

Whilst the principles, approach to, and process of risk management will be broadly the same, they may be applied differently depending on the organisational perspective they are being considered from. For example, you may be concerned with risks affecting the day to day management of the organisation, or a specific project or programme of work, or with the strategic objectives of the organisation as a whole. The table below describes these perspectives, how risks at these perspectives might be identified and provides examples.

Table 1

Perspective	Identification	Examples
Strategic - Strategic risks are those concerned with ensuring the overall success of the organisations' objectives. The materialisation of a strategic risk will be apparent externally and may affect the reputation of the organisation.	Strategic threats and opportunities will generally be identified as a by-product of the corporate or business planning cycle (*see below) and through the escalation of risks from programme, project or operational activities.	Examples inc reputation management/stakeholder perception of key policies or operational activities, political factors, pandemics, damage to key resources or core assets (fire, flood etc) financial viability etc
Programme - Programme risks are those concerned with opportunities and threats to programmes of activities that create transformational change and deliver measurable benefits.	These risks will be identified, during the start-up of the programme, through the escalation of risk from projects/schemes within a programme, by the aggregated effect of project/scheme risks on the programme or by operational units affected by the programme.	Examples inc changes in funding criteria or stakeholder priorities
Project/Scheme - Project risks are those concerned with the delivery of defined outputs within an agreed scope, quality, time and cost.	Where a scheme is funded by an investment programme, the opportunities and threats will be identified within Business Case documentation and assessed during the project assurance and appraisal process and monitored and updated throughout the delivery of the scheme. For a project that is not part of a programme (e.g. an internal piece of work or activity) risks will be identified during project initiation as well as during the delivery of the project.	Examples inc availability of resources, clarity of outcomes, change management, quality of the project infrastructure and governance, timing/slippage
Operational - Operational risks are those concerned with maintaining a level of business service that support ongoing business-as-usual activities delivered by functional teams.	Operational risks will be identified through the escalation of risk from functional teams (IT, facilities management) by service-enabling suppliers and service-receiving 'customers' and the de-escalation of strategic risks.	Examples include - strength of operational controls, quality of infrastructure, skills and resource, business continuity, legal or contractual obligations etc

Roles and responsibilities related to risk management

Risk Management sits within all areas of organisational activity. However, the MCA, supported by the MCA Executive Team Management Board, has overall accountability for risk management. The Deputy Chief Executive, who leads on continual improvement and organisational development, has specific responsibility for overseeing the effective implementation of risk management practice.

The table below sets out the different roles and responsibilities relating to risk management across the organisation.

Table 2

Role	Responsibilities
MCA	Provides strategic direction and determines overall risk appetite. Overall accountability for risk management and sets risk management policy. Ensures an appropriate risk management framework is in place. Debates and considers risk as a framework for strategic direction and decision making. **De-escalates** risks, where the threat level has decreased and falls within the agreed tolerance threshold, to Statutory Officer/Management Board.
Audit and Standards Committee	Provides assurance to the MCA on the effectiveness of the risk management framework. Reviews group risk profile (the types of risks faced and the exposure to them). Reviews the Strategic Risk Register. Has oversight of the risk management arrangements of South Yorkshire Passenger Transport Executive (SYPTE) through joint membership.
LEP Board	Debates and considers risk in the economy as a framework for strategic direction and decision making.

Thematic Boards	Identify and recommend mitigations for any programme risks relevant to the thematic area. **Escalates** risks exceeding agreed tolerances to MCA where appropriate. **De-escalates** risks, where the threat level has decreased and falls within the agreed tolerance threshold, the PPU.
Statutory Officers and Management Board	Owns and manages strategic risks. Ensures appropriate focus and resources are applied to risk management. Ensures that key strategies include appropriate risk focus. Fosters a supportive environment to promote an 'open' culture which encourages risk reporting. Encourages business-wide application of risk management. Has oversight of the Strategic Risk profile of subsidiary bodies (PTE) through representation on PTE Executive Board. **Escalates** risks exceeding agreed tolerances to MCA. **De-escalates** risks, where the threat level has decreased and falls within the agreed tolerance threshold, to either PPU/functional teams or relevant project board or collaboration team as appropriate
Programme and Performance Unit (PPU)	Implements risk management processes to ensure scheme and programme risks, are monitored, mitigated and escalated appropriately. Prepares monitoring reports for review by the Management Board and Thematic Boards. **Escalates** risks exceeding agreed tolerances to Thematic Boards. **De-escalates** risks, where the threat level has decreased and falls within the agreed tolerance threshold, to scheme promoters.
Functional Teams (e.g. IT, Facilities Management etc)	Implements risk management processes to maintain a level of business service to internal and external ‘customers’ and to support ongoing business-as-usual activities. Maintains risk registers for the management of high-risk functional areas. Reports on and escalates significant risks to the Management Board as appropriate. **Escalates** risks exceeding agreed tolerances to Statutory Officers/Management Board.
Project Boards/Collaboration Teams	Led by the Senior Risk Owner, implements risk management processes to ensure project risks, are monitored, mitigated and escalated appropriately. **Escalates** risks exceeding agreed tolerances to Statutory Officers/Management Board.
Governance and Compliance Team	Provides oversight across all risk management activities within the organisation. Reviews and updates risk management documentation to ensure they remain fit for purpose. Ensures a consistent approach to risk management reporting and escalation that fully meets the organisational needs and demonstrates best practice.
Risk Champions	Provides support and guidance on risk management processes.
All Employees	Comply with the risk management policy. Apply risk management processes within their own area of work. Consults appropriately to include risk management implications in any proposals requiring decision.

The Process of Managing Risk

Where do I start and what do I need to do?

Understanding the appetite for taking risks in order to achieve objectives

Fundamentally risk management is about giving any activity, from the delivery of a Corporate Plan to a project to role out a new system, the best chance of achieving its objectives. To do this, firstly you need to understand the 'risk appetite' - how much risk you are willing to take in order to achieve the objectives, how much risk you can actually bear (risk capacity) and where the tipping point (risk threshold) is.

In an organisation such as the MCA, whose activity is driven by multiple strategies and priorities, including those of the LEP and the Mayor, it is impossible to define a single risk appetite i.e. the amount of risk the organisation is prepared to accept, tolerate or be exposed to at any one time, that would suit every circumstance. Whilst there may be a general notion that the organisation overall is against taking too much risk or, is perhaps happy to gamble with the hope of bigger returns, risk appetite, should be considered on a case by case basis.

To determine the risk appetite for a particular activity a 'risk appetite and acceptance model' (fig.1) is in place. Defining the risk appetite helps decision makers have a better awareness of the level of risk being taken to achieve objectives and informs a consistent approach to risk-based decision-making at all levels.

Fig.1

	Risk Level					
	0 = Avoid We are averse to risk and want to avoid any uncertainty in this impact area	1 = Minimal We would prefer an ultra-safe option and accept the reward would be very limited	2 = Cautious We would prefer a safe option that may only have limited reward	3 = Open We are willing to consider all options for an acceptable level of reward (and vfm)	4 = Seek We are eager to be innovative and choose options that potentially offer higher rewards despite inherent risk	5 = Mature We are confident with high levels of risk because controls, forward scanning and responsiveness systems are robust
	Appetite – None	Appetite – Low	Appetite – Moderate	Appetite – High	Appetite - Significant	Appetite - Significant
Impact Area						
Financial						
Political/Economic						
Reputational						

At this point in the process it may be useful to begin to develop a 'risk management strategy' for the activity so you can document the agreed risk appetite. A risk management strategy describes the specific risk management activities that will be undertaken and will be specific to the activity concerned but, will also reflect the organisational approach to risk management. Guidance on determining whether a risk management strategy would be of use and a template to assist in its development forms part of the risk management tool kit.

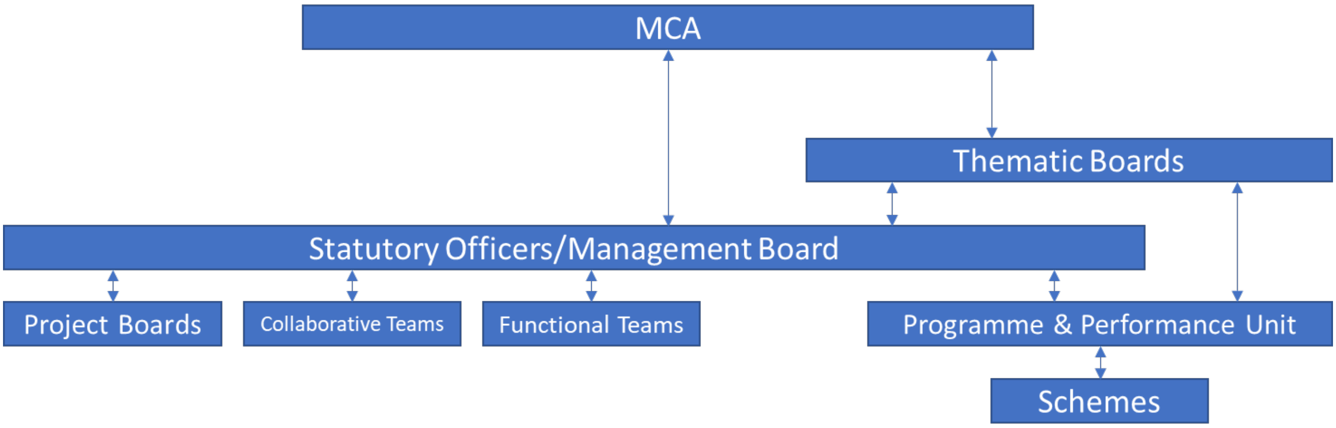
When is a risk, 'too risky'?

Understanding the risk appetite (the amount of risk you are willing and able to bear) helps understand at what point the risk becomes too much i.e. the tolerance threshold. If this threshold is reached the risk should be escalated. If the amount of risk decreases below the threshold then it can be de-escalated too.

Where do I escalate risks that can no longer be tolerated?

Escalation routes are set out in table 2 and summarised in the diagram below.

Fig 2.



Identifying and Mitigating Risks

Working out what the risks are and what to do about them

The Risk Management Process

There are four steps to the risk management process that form a logical sequence that can be repeated as often as necessary as new information becomes available.

These are:

- **Identifying** the risks
- **Assessing** the risks
- **Planning** the responses and mitigations
- **Implementing** the mitigations and monitoring their effectiveness

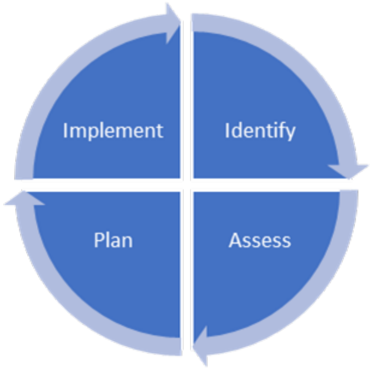


Fig 3.

Simply put, this process helps us understand what it is we are trying to achieve, what might happen that could affect it (negatively or positively), how likely those things are, the impact they may have and how we can reduce or increase the chance of them happening (depending on their effect).

Step 1 "Identifying"

First you will need to be clear about the background or context of the planned activity, including its objectives and scope, you will then need to identify the risks to the objectives of the activity with the aim of maximizing the opportunities and minimizing the threats.

Background information can be taken from such things as regulatory frameworks and contractual obligations as well as any other documentation specific to the activity. These documents also support the identification of risks along with any necessary stakeholder analysis and the review of lessons learnt documents from other similar activities.

Recording - At the end of this step a risk register should be in place. The risks recorded in the register need to be described in a way so they can be understood easily. The preferred format for risk descriptions is to create a 'string' that separates the **cause** from a **risk event** and its **effect**.

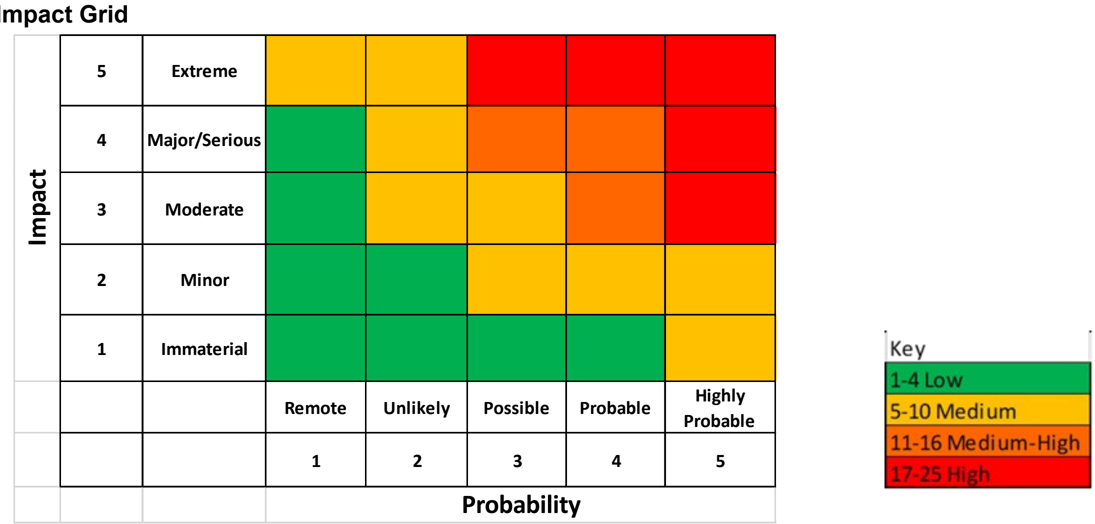
Example

Risk cause (or trigger) This describes the source of the risk i.e. the event or situation that triggers the risk.	**Risk event** This describes the area of uncertainty i.e. what *might* happen.	**Risk effect** This describes the impact on the organisation or particular activity should the risk materialise.
Example Flooding	**Example** leads to a delay in progress of a scheme (slippage)	**Example** resulting in schemes outcomes not being realised in agreed timescales as well as overall programme slippage

Step 2 "Assessing"

In this step you will need to prioritise individual risks to understand which are most important and most urgent, and to understand the total effect of the risks on the organisation or activity when aggregated together (the risk exposure). To do this a probability impact assessment, using the probability impact 'grid' needs to be undertaken and the results recorded in the risk register along with an estimation of *when* the risk might occur.

Fig.4 Probability Impact Grid



To support the assessment of the *level* of impact a risk may have, the table below describes the different types of impact at different levels. It could be that a risk has a different level of impact in each area (or no impact at all), if this is the case an informed judgement should be made on the overall impact the risk may have.

Table 3: Levels of Impact

	Type of Impact			
	Financial	**Reputational**	**Political**	**Economic**
5 – Extreme	Loss that could destabilise the financial health of the MCA Executive and / or destabilise a programme of activity this is most likely a multi-year issue or take multiple years to resolve	Circumstance leading to sustained adverse publicity from a national perspective resulting in a serious impact in government, investor and stakeholder confidence with a material loss to the MCA / LEP	Political discord with the potential to result in the breakup of the MCA OR Failure in local leadership that could result in government intervention, OR High profile legal proceedings,	Shock to the economy resulting in extreme business and / or job losses and that would require additional resources (staff and financial) to mitigate beyond the capacity of the MCA / LEP and will take the economy generations to recover
4 – Major/Serious	Loss that could be detrimental to the financial health of the MCA Executive and / or detrimental to delivering a programme of activity most probably a single year issue	Circumstance leading to adverse publicity nationally resulting in a serious impact on government, investor and stakeholder confidence and a potential material loss to the MCA / LEP	Political discord which significantly affects the business / decision making processes of the MCA OR Government enquiry into operational inadequacies / Concerns or complaints raised in Parliament OR Legal proceedings	Shock to the economy resulting in significant business and / or job losses and that would require additional resources (staff and financial) to mitigate over a sustained period and which will take multiple years to recover
3 – Moderate	Loss that is significant which cannot be contained within budget but that would require a new budget to be developed and approved	Circumstance leading to short term adverse local / regional publicity with moderate impact on government, investor and stakeholder confidence. Resulting in significant embarrassment.	Failure of political processes or to reach consensus that affects the business, services or operation of the MCA and results in a breach of requirements of the constitution and / or legislative requirements	Shock to the economy resulting in business and / or job losses and that would require additional resources (staff and financial) to mitigate over multiple years
2 – Minor	Minor loss that can be contained within budget but would result in some planned spend being	Internal issue, minimal external reputational damage and no loss of stakeholder confidence	Failure of political processes or to reach a consensus that delays the business of the MCA and/or leads to	Shock to business and / or job resulting in losses and that may require additional resources (staff and

	cancelled or delayed		minor non-compliance with the constitution	financial) to support existing activity to mitigate within a short time frame
1 - Immaterial	Minor loss that can be contained within budget with no detrimental impact on other planned activity	Isolated, internal issue, reputational damage contained within the MCA / LEP	Failure of political consensus that can be managed through the constitutional processes of the MCA	Shock to businesses and / or jobs that can be mitigated and supported within existing programmes

At the end of this step the risk register should be updated to include the assessment of the probability, impact and urgency of each risk. A summary risk profile or ‘heat map’ can also be developed, if required, to help illustrate the total risk exposure to the organisation or activity in a graphical way.

Step 3 “Planning”

In this step you will need to plan specific management responses or ‘mitigations’ to identified risks in order to remove or reduce threats and maximize opportunities.

At the end of this step the Risk Register should be updated to include the risk owner, risk actionee/action owner, risk mitigation and actions.

Step 4 “Implementing”

The aim of the ‘implement’ step is to ensure that planned risk management actions are implemented, monitored as to their effectiveness, and appropriate action taken where responses do not meet expectations or have not been implemented effectively.

At the end of this step risk responses or ‘mitigations’ will be implemented (or be in the process of being implemented) and, where appropriate, other documents and information that will enable effective monitoring and review of the risk management activities taking place will be produced as appropriate.

Applying this process at different organisational perspectives

This four step process can be followed for all risk management activity, at each different risk perspective throughout the lifespan of a particular activity however, for risks concerned with the strategic perspective there is no end point therefore the identification, review and refresh of strategic risks takes place annually as part of the development or review of the Corporate Plan and annual business planning activity. Strategic risks and the progress of the actions to manage or mitigate them are monitored by the Management Board quarterly with any significant changes in the risk profile being reported to the Audit and Standards Committee. Should any significant new risks emerge during the year e.g. pandemic, mayoral or general election, or a localized incident impacting on the delivery of organisational objectives such as flooding, additional risk management activity will take place. The MCA receive a yearly report on the risk profile (the types of risks faced by the organisation and the level of exposure to them)

Similarly, at an operational level where risks that threaten the support of ongoing business activity e.g. IT services will be ongoing and therefore subject to regular review and refresh. The monitoring of risk across the organisation is set out in the next section on reporting.

Reporting

How does the organisation know what risks are being taken and why?

Regular reporting demonstrates that risks are being tracked on a regular basis and allows the organisation to respond to situations as they arise and to avoid issues before they happen.

The table below provides an overview of the risk reporting to different groups within the organisation.

Table 4: Regular Risk Reporting

MCA	Will receive a yearly report on the risk profile (the types of risks faced by the organisation and the level of exposure to them) aligned to the Business Plan and Corporate Plan Review. Will receive information relating to the risk of proposed activities as part of the decision-making process.
Audit and Standards Committee	Will receive the strategic risk register quarterly. Will receive a yearly report on the risk profile (the types of risks faced by the organisation and the level of exposure to them) in the context of the Business Plan and Corporate Plan.
LEP	Will receive a yearly report on the risk profile (the types of risks faced by the organisation and the level of exposure to them) as part of the annual implementation plan. Will receive information relating to the risk of proposed activities as part of the decision-making process.
Thematic Boards	Will receive a programme dashboard relevant to the thematic area at each meeting. Will receive information relating to the risk of proposed activities as part of the decision-making process.
Statutory Officers and Management Board	Risk Management will be considered on a monthly basis. Risks will be managed by exception, horizon scanning activity will be undertaken and potential changes that may affect overall risk exposure will be identified. Will receive information relating to the risk of proposed activities as part of the decision-making process.
Project Boards/Collaboration Teams	Will receive the project risk register at each formal meeting, risk will be managed by exception.

Supporting, developing and assuring risk management

The Governance Team, along with a number of Risk Champions, who are certified practitioners of the 'Management of Risk (MoR®)' provide guidance and support with the application of risk management.

The following templates are available to support the application of risk management processes:

- Risk Management Strategy template
- Standard Risk Register template
- Strategic Risk Management Action Plan template

The annual budgeting and business planning cycle identifies any budget and additional resource required to support risk management activity in the forthcoming year.

A number of activities have been identified to improve risk management practice:

- Development of an induction module on risk management for new starters
- Staff development module on risk management
- Dedicated area on the intranet where tools and guidance will be available
- Inclusion of risk management on meeting agendas
- Regular updates on key risks through internal communication (staff briefings etc)
- Embedding the risk management process into organisational activity (piloting with Collaboration Teams) and decision making

This policy and process are subject to annual review. Following the review, the risk improvement plan above will be refreshed in order to further strengthen risk management practice.

Risk Management will be included in the internal audit plan annually to ensure an independent, objective view on the effectiveness of the application of risk management.

Glossary (alphabetical)

NB – not all of these terms appear in this document but may be referenced in other documentation/templates that support risk management process activity.

Accept
A risk response that mean that the organisations takes the chance that the risk will occur, with full impact on objectives if it does.

Activity
This could be a scheme, project or programme.

Audit and Standards Committee
A statutory committee responsible for monitoring the integrity of the financial statement of the company; the effectiveness of the internal audit function; the external auditor's independence and objectivity and the effectiveness of the audit process; the effectiveness of risk management arrangements.

Avoid
As risk response that seeks to eliminate a threat by making a situation certain.

Collaborative Group
Cross organisational collaborative working for a defined number of policy or programme development areas.

Corporate Governance
The ongoing activity of maintaining a system of internal control by which an organisation can ensure that effective management systems, including financial monitoring and control systems, have been put into place to protect assets and the reputation of the organisation.

De-escalation
A risk can be de-escalated should it become manageable within tolerance thresholds.

Early Warning Indicator
Abbreviated to EWI. A leading indicator for an organisational objective measured ultimately by a key performance indicator (KPI)

Enhance
A risk response for an opportunity that seeks to increase the probability and/or impact to make it more certain.

Escalation
A risk should be escalated where a higher level of consideration is required should a risk exceed the tolerance threshold.

Exploit
A risk response for an opportunity that seeks to make the uncertain situation certain.

Impact
Impact is a result of a particular threat, or opportunity, actually occurring.

Inherent risk
The exposure arising from a specific risk before any action has been taken to manage it.

Issue
A relevant event that has happened, was not planned and required management action. It could be a problem, benefit, query or concern, change request or risk that has occurred or has materialised.

Issue actionee/Issue action owner
A role or individual responsible for the management and control of all aspects of individual issues, including the implementation of the measure taken in respect of each issue.

Key Performance Indicator
Abbreviated to KPI. A measure of performance that is used to help an organisation define and evaluate how successful it is in making progress towards its organisational objectives.

Management of risk
Systematic application of policies, procedures, methods and practices to the task of identifying and assessing risks, and then planning and implementing risk responses. This provides a disciplined environment for proactive decision making.

Objective
Something to be achieved.

Operational or functional risks
Risks that occur in operational or functional areas of the organisation and may have an impact on the achievement of organisational objectives. These may occur due to system failures, inadequate procedures or controls or human error.

Opportunity
An uncertain event that would have a favourable impact on objectives or benefits if it occurred.

Outcome
The result of change. Outcomes are achieved as a result of the activities undertaken to effect the change.

Output
The tangible product of a planned activity.

Probability
This is the evaluated likelihood of a particular threat or opportunity actually happening, including a consideration of the frequency of with which this may arise.

Programme
An organisational structure created to co-ordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to the organisations' strategic objectives.

Programme risk
Risk concerned with the successful delivery of a programme of work.

Project (also see scheme)
A series of tasks to be completed to reach a specific goal or set of objectives outcomes.

Project risk (also see scheme risk)
Project risks are those concerned with the successful completion of the project. Where a project forms part of the delivery of a programme, these are often referred to as 'scheme' risks.

Proximity (urgency)
The time factor of a risk i.e. the occurrence of risks will be due at particular times, and the severity of their impact may vary depending on when they occur.

Reduce
A risk response for a threat that seeks to reduce probability and/or impact.

Residual risk
The risk remaining after the risk response has been successfully applied.

Risk
An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.

Risk actionee/Risk action owner
Some actions may not be in the remit of the risk owner to control explicitly; in that situation there should be nominated owner of the action to address the risk. He or she will need to keep the risk owner apprised of the situation.

Risk appetite
The amount of risk the organisation or activity is willing to accept.

Risk capacity
The maximum amount of risk that an organisation or activity can bear, linked to factors such as financial and reputation.

Risk cause (or trigger)
A description of the source of the risk i.e. of the event or situation that gives risk to the risk.

Risk effect
A description of the impact that the risk would have on the organisation or activity should the risk materialise.

Risk estimation
The estimation of probability and impact of an individual risk.

Risk evaluation
The process of understanding the net effect of the identified risks when aggregated together.

Risk event
A description of the area of uncertainty in terms of the threat or opportunity.

Risk exposure
The extent of risk borne by the organisation or activity at a particular time.

Risk identification
Determination of what could pose a risk; a process to describe and list sources of risk.

Risk log
See risk register.

Risk management
Systematic application of policies, procedures, methods and practices to the task of identifying and assessing risks, and then planning and implementing risk responses.

Risk management policy
A high-level statement showing how risk management will be handled throughout the organisation. This can be combined into one document with the risk management process if appropriate.

Risk management process guide
Describes the series of steps and their associated activities, necessary to implement risk management. This can be combined into one document with the risk management policy if appropriate.

Risk management strategy
Describes the goals of applying risk management to a particular activity, the process that will be adopted, the roles and responsibilities, risk thresholds, the timing of risk management intervention, the deliverables, tools and techniques that may be used, the reporting requirements.

Risk manager
A role or individual responsible for the implementation of risk management for particular activities.

Risk owner
A role or individual responsible for the management and control of all aspects of individual risk, including the implementation of the risk responses and mitigations.

Risk profile
Describes the types of risks faced by the organisation or activity and the level of exposure.

Risk register
A record of all identified risks relating to an activity including their status and history.

Risk response
Action that may be taken to bring the situation to a level where the exposure to risk is acceptable.

Risk tolerance
The threshold levels of risk exposure that, with appropriate approvals, can be exceeded, but when exceeded will trigger a response i.e. escalation.

Risk tolerance line
A line drawn on the summary risk profile. Risks above this line cannot be accepted without escalation.

Scheme or project
Where a project forms part of the delivery of a programme, these are often referred to as ‘scheme’ risks.

Scheme risk
A scheme is a project within a funded programme. Scheme risks are those concerned with the successful completion of the scheme.

Senior responsible owner
The single individual with overall responsibility for ensuring that an activity meets its objectives and delivers its outcomes.

Stakeholder
Any individual or group (internal or external) that can be affected by, or perceive itself to be affected by, an activity.

Statement of internal control
A narrative statement by the organisation confirming there is an ongoing process for the identification and management of significant risks.

Strategic risk
Risk concerned with the achievement of the strategic objectives of the organisation.

Summary risk profile
A simple mechanism to increase the visibility of risks. It is a graphical representation of information normally found on a risk register.

Threat
An uncertain event that could have a negative impact on objectives.

Transfer
A risk response whereby a third party takes on responsibility for an aspect of a risk.

Urgency (proximity)
The time factor of a risk i.e. the occurrence of risks will be due at particular times, and the severity of their impact may vary depending on when they occur.