

Management of Risk Framework

VERSION 0.4-2 DATE ~~November 2023~~ March 2024



Document Control:

Version	Date	Brief Summary of Changes	Author
1	06/01/22	First draft prepared	Liz Morris
2	27/01/22	ASRC approve with caveat risk appetite statement to be re-considered	Liz Morris
3	11/02/22	Small number of edits and Risk Appetite Statement added at the request of the ASRC	Liz Morris
5	18/02/22	Risk Appetite Scores removed following 15 th February Management Board request	Liz Morris
5	24/03/22	ASRC Approve revised Risk Management Framework	ASRC
6	25/07/22	MCA approval received	Ruth Adams
7	29/12/22	Name changes throughout and edits driven by the Executive Leadership Team decisions including clarification of roles & responsibilities.	Liz Morris
8	27/01/23	Version 7 changes accepted by ASRC 25/01/23	Claire James
9	17/11/23 17/11/23	Review following change to SYMCA Governance Arrangements. Also change to font size for accessibility.	Emily Hickey Claire James
10	Click or tap to enter a date.	Click or tap here to enter text.	Click or tap here

MANAGEMENT OF RISK FRAMEWORK

Introduction

Management of risk is a planned and systematic approach to the identification, evaluation, prioritisation and control of risks and opportunities facing an organisation. Effective management of risk is an integral part of good corporate governance and internal control arrangements and should be a part of everyday management processes throughout any organisation. Corporate Governance processes and arrangements have evolved over time with UK and global enhancements. Following 'lessons learned' from corporate failures.

The requirement for management of risk in combined authorities is set out in the Accounts and Audit Regulations 2015. The Regulations are applicable to South Yorkshire Mayoral Combined Authority (SYMCA) and contain provisions on financial management, annual accounts, internal control and audit procedures, which require a sound system of internal control to be maintained, which includes '*the effective arrangements for the management of risk*' (Part2, para3). The Regulations require, as part of the financial control systems measures '*to ensure that risk is appropriately managed*' (Part2, para 4).

SYMCA is committed to ensuring that robust arrangements for the management of risk are in place and operating effectively across the organisation. This is particularly important as transformation has taken place and the two predecessor organisations have integrated to bring together different processes and ways of working to harmonise to embed a single operating model. As the organisation reconsiders its structure, the continued management of risk will be an important continuity arrangement. The Executive Leadership Team (ELT), and individual directors, will champion the management of risk and ensure that appropriate arrangements are in place, maintained and reported upon on a regular and on-going basis.

This Framework sets out SYMCA approach to the management of risk, the roles and responsibilities and provides a proportionate process, which will provide a foundation for embedding Enterprise Risk Management. This structured approach takes into account the maturity of SYMCA, its risk management knowledge, longevity and the operational challenges the organisation faces both internally and externally. As part of the approach to develop and define this Framework, and as part of good project management, a post implementation review (PIR) has been undertaken. This has considered if management of risk is operating as intended and ultimately resulted in this Framework, and operating processes, being adjusted to take account of the ELT's defined direction.

Management of Risk Definitions

There are many definitions of risk, which fundamentally have at their heart that risk is *the effect of uncertainty on objectives*. The technical recording of risk is expressed in terms of the cause(s), potential event(s) and the *consequence(s)*.

- Cause, has the potential to lead to risk(s) i.e. the source and this can be structured as 'due to'.
- Event, something planned that doesn't happen or something not expected which may happen and this may be structured as 'there is a risk that' or 'leads to'.
- Consequence, the outcome of an event affecting objectives, and this may be structured as 'results in'.

Management of risk is the *co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation*.

The core of the above has been taken from the *Orange Book*, as updated in 2020, and it should be noted that a risk can be based on a threat or an opportunity.

Effective Management of Risk and its Benefits

The ELT of SYMCA has agreed to embed effective management of risk throughout the organisation by:

- ensuring this structured and consistent approach is embedded and roles and responsibilities are built into the organisational structure and reporting lines.
- using the approach to facilitate effective prioritisation of resource.
- using data and management information to build up a full picture of risks to facilitate good decision making and continuous improvement.
- ensuring continuous review of risks and mitigations takes place and management of risk performance is reported on regularly.
- ensuring that all risks are managed at the most effective and practical level and escalation takes place in line with the requirements.
- commissioning further reviews, annually, to consider any lessons, whether intended benefits have been met and if adjustment is required due of feedback and external good practice to ensure arrangements remain fit for purpose and risks are managed effectively.
- providing user friendly management of risk guidance and support based on good practice.

Implementation of the above will help build effective management of risk and will enhance management functions and processes and corporate governance within SYMCA. As such, management of risk works alongside financial management, performance management and business planning to enhance and demonstrate responsibility, transparency and accountability. It also forms a key component of the delivery of SYMCA's purpose and objectives including the Strategic Economic Plan and associated delivery plans.

Through effective management of risk, SYMCA ELT can prioritise and manage both threats and opportunities to the delivery of objectives. By implementing and embedding a continuous and standardised approach to the management of risk, a process is developed to prioritise resources, implement effective and proportionate controls to manage threats and exploit opportunities. Consequently, the aspiration of this Framework is that management of risk becomes a fundamental and demonstratable factor of all management decisions taken by SYMCA.

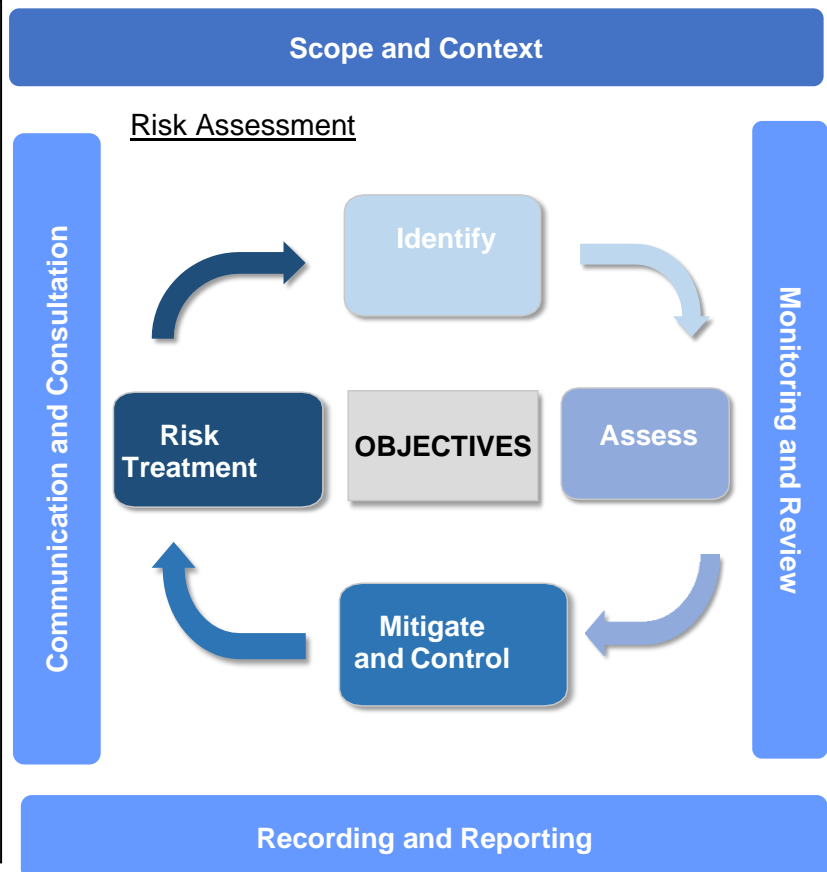
Our approach, the Management of Risk Process

The effective management of risk process is recorded below and covers each of the fundamental principles.

The management of risk process is broken down into components, depicted in the diagram. This implies the process is sequential however, it is more dynamic and is a continuous cycle of review and revisiting the steps as time and events develop and impact on the delivery and achievement of objectives. It is presented in more detail in Appendix A, Management of Risk on a Page and within the following pages.

The process has been influenced by the Risk Management Standard ISO 31000, The Orange Book, benchmarking of comparable organisations and previous processes along with experiential knowledge of good practice.

There can be many applications of the management of risk within the organisation however, the fundamental principle is to support the achievement of objectives. In the case of SYMCA this is focused on the delivery of the Strategic Economic Plan.



Each step is considered in more detail below.

Scope and Context

Management of risk in SYMCA is set against the delivery of the Strategic Economic Plan (SEP) and the operations and activities the organisation takes to deliver that. This means that risks are defined against the delivery of objectives which are set out within SYMCA plans aimed at leading to the achievement of the SEP priorities. Risks may be either internal to SYMCA or externally facing as work is undertaken with partners and stakeholders to transform the economy of South Yorkshire for its people, business and places.

Communication and Consultation

Communication and consultation are key attributes of the Management of Risk Framework and aim to assist stakeholders in understanding risk and its role as a basis on which decisions are made. Communication in this context will enhance awareness of risk and its management and consultation will take place with stakeholders to seek feedback in agreeing the Framework and the recorded risks, resulting in the Framework and outputs being co-created. Coordination across the two will ensure that the information contained within the Framework and the outputs including risk registers are relevant, accurate and timely and is set within the context of the organisation and its operating environment.

Risk Assessment Process

Risk Assessment is the overall process of risk identification, risk analysis and evaluation. The assessment should be systematic, iterative and take place dynamically and collaboratively considering the views of related stakeholders.

Objectives

As part of the business planning process, risks may be identified, considered, and recorded within the risk register template (Appendix B). In aligning risk registers to a business planning activity, where this is undertaken, risk ownership will reside with the manager and most appropriate member of the respective team.

Additionally, risks may be identified outside of the business planning process and as part of everyday operations or business as usual activity and added to the register recorded, as necessary.

Risk Identification

The risk identification step aims to identify and describe risks that may help or prevent the achievement of objectives e.g. what might happen that could affect progress, it could be negative or positive i.e. an opportunity.

There are many ways in which risks can be identified and aligned with core management including:

- Horizon scanning.
- PESTLE analysis.
- SWOT analysis considering Strengths, Weaknesses, Opportunities and Threats.
- Learning lessons from internal experience and external events.
- Root cause analysis, asking why five times to each risk event to identify a cause to be addressed.
- Control & Risk Self-Assessment, collaboratively delivered with a range of stakeholders to seek the views of all parties creating a rounded approach to identifying risk.
- Business planning and objective setting, which means that management of risk is at the heart of everything that is undertaken within the organisation.

A useful process to help write a risk for inclusion in a risk register, board papers and more widely is to think about the risk in terms of the:

- the reason for occurrence, source or cause of a risk 'due to'.
- the risk itself, an event or 'there is a risk that'.
- the consequence, the result, 'results in'.

Reason for a risk occurring The event or situation trigger (the cause / 'due to')	Risk itself Area of uncertainty, (what may happen – 'leads to' / 'there is a risk that')	Consequence of the risk The effect should the risk materialise. ('results in')
Flooding	leads to a delay in the progress of a scheme	resulting in outcomes not being realised in the timescales.
Increased cyber attacks	leads to successful infiltration	results in operational disruption, data corruption, outage and financial loss.

[SYMCA has implemented the IT system '4Risk' to record, monitor and manage risks.](#) Each risk should be recorded within the 4Risk system following agreement with the relevant Director. Appendix B [provides an example in spreadsheet format of the categories of information collected in the 4Risk system.](#)

Risk Registers

Risk Registers will take the following forms:

- **Corporate Risk Register:** this contains the main ELT held risks, which may be cross cutting, on-going or longer-term and have an impact on SYMCA and its strategic objectives. These risks are owned and updated by Executive Directors as part of their role within the ELT and reported into the ELT and ASRC quarterly. ELT has taken the decision that it will report **all** corporate risks to ASRC regardless of the current / residual score.
- **Directorate and Team Risk Registers:** these contain risks specific to SYMCA teams and can be reflective of objectives, business plans, processes, and operating environments. These risks are identified, owned, and managed by directors, managers and operational employees. Such risks are escalated and reported in line with the Recording and Reporting section of the Framework. This means high and medium / high level risks will be reported through the management hierarchy into ELT, ASRC quarterly and the MCA Board annually.

Consequently, it is the responsibility of all employees to actively identify and manage risks and opportunities to the achievement of objectives.

Grouping the Risks

The following strategic groups have been established, in which risks will be brigaded and analysed to develop corporate and board level reports. The Risk Appetite Statement (Appendix D) has been set against the groups, which were defined and adopted by the Executive Leadership Team in 2020. It is important for each risk to be allocated to an appropriate category as follows:

- **Policy** relates to the setting of interventions to tackle specific matters to develop the strategic objectives of the SYMCA.
- **Financial** relates to establishment and maintenance of financial health and wellbeing to achieve strategic and financial objectives.
- **Organisational** relates to the structure and makeup of the organisation to deliver the objectives and the corporate plan.
- **Commissioned Operations and Delivery** incorporates the programmes and projects of the MCA to deliver the objectives set for the region.
- **Legal Compliance and Regulation** relates to the obligations the MCA is required to adhere to including the upholding of laws, statutes and regulations e.g. professional standards, laws relating to ethics, bribery, corruption and fraud.
- **Transport** relates to operational transport related matters that would have historically formed part of the Passenger Transport Executive risk register.

Assess the Risk

~~Each risk should be recorded within the 4Risk system the template at Appendix B replicates the information fields within the system and is provided as an aid.~~

Once a risk has been identified, the risk owner is defined and captured within the risk register. The risk owner is the person that takes responsibility for the management of the risk. Assessment and evaluation of each risk is undertaken using a five-by-five Probability Impact Grid, as follows:

Impact	5 Critical	5	10	15	20	25
	4 Serious	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Immaterial	1	2	3	4	5
		1 Highly Unlikely	2 Unlikely	3 Possible	4 Probable	5 Highly Probable
		Probability				

Inherent Risk Score

Each risk is assessed inherently, prior to any controls or actions being established, for probability and impact and an overall risk score is created by considering the probability of the risk occurring and also the impact if it did occur. Simply, this requires the multiplication of the probability score (1-5) by the impact score (1-5) to reach an overall risk score (1-25).

Further guidance on scoring is included within the Scoring Matrix at Appendix C, which has been established to help build consistency throughout the process and organisation.

Mitigation and Control/Residual Risk Score

Each risk is assessed ~~inherently, prior to any existing controls being applied, and~~ again after the application of existing controls, (which are captured in the risk system and can be aligned to the relevant 'line of defence' for analysis and assessment purposes), to reach a current or residual risk score.

~~Appendix B, the risk register template demonstrates the flow of this risk information. The current or residual risk score provides an opportunity to rank risks and a means of prioritising to highlight risks posing the greatest threat or opportunity to the organisation. The residual risk score is the basis for escalation and reporting.~~

~~Within the risk system additional actions are recorded, which are deemed necessary to reduce the risk exposure to an acceptable level and within appetite, or to maximise the opportunity, which in turn may be used to create an action plan. An action is any activity that is planned. An action requires an owner, a deadline or timescales by when it will be completed.~~

~~Risk owners, directors and ELT can monitor and review risks, controls and track the actions through to completion. It is important that the actions are tracked to ensure that risks are treated in the right way and at the right time. An action plan may also be included in reporting to directorate management teams, ELT, Audit, Standards and Risk Committee and more widely.~~

Risk Treatment

Once the risk has been recorded, existing controls have been established and ~~a current~~inherent or residual risk score defined then a decision needs to be made as to what to do next. The risk treatment options below provide the alternatives to consider:

- Treat, take action to further reduce a risk.
- Tolerate, accept the risk.
- Transfer, pass responsibility e.g. insurance.
- Terminate, avoid the activity.
- Take up, to maximise an opportunity.
- Together, to share with partners e.g. public private initiatives/partnerships (PPI/PPP).

Target Score

Within the risk system additional actions are recorded, which are deemed necessary to reduce the risk exposure to an acceptable level (a target score) in line with the risk appetite, or to maximise the opportunity, which in turn may be used to create an action plan. An action is any activity that is planned. An action requires an owner, a deadline or timescales by when it will be completed.

Risk owners, directors and ELT can monitor and review risks, controls and track the actions through to completion. It is important that the actions are tracked to ensure that risks are treated in the right way and at the right time. An action plan may also be included in reporting to directorate management teams, ELT, Audit, Standards and Risk Committee and more widely.

Appetite

The ~~Target~~current or residual risk score should be related to the appetite the organisation has established, setting out how much risk the organisation is willing to accept. The expectation is that a risk owner will manage each risk to its lowest practical level and where it is not possible to do so a risk will be escalated through the organisational reporting structure and ultimately to ELT and ASRC. This is in line with the Recording and Reporting requirements set out below. The Risk Appetite Statement is included as Appendix D and provides a guide to risk owners and employees across SYMCA.

A further expectation is that directors and ELT will guide the executive teams into action or accept / tolerate the current level of risk i.e. the status quo.

Appendix B, the risk register template demonstrates the flow of this risk information (from inherent to residual and finally to target score). The current or residual risk score provides an opportunity to rank risks and a means of prioritising to highlight risks posing the greatest threat or opportunity to the organisation. The residual risk score is the basis for escalation and reporting.

Monitoring and Review

Monitoring and Review activities are continuous and applied across all levels of the management of risk process. This provides for and leads to assurance and improvement of the quality and effectiveness of the process, its implementation and the output e.g. risk registers (held within the 4Risk system). Ongoing monitoring and regular review are built into the management of risk process and the requirements for escalation and de-escalation are captured in the Recording and Reporting section below.

The Management of Risk Framework and operating practices ~~have been~~was subject to a post implementation ~~review to consider lessons~~. ~~This~~This has resulted in adjustments being made, ~~as instructed~~agreed by ELT.

Subsequently, the Framework and outputs will be subject to an annual review for similar purposes, learning lessons and adoption of ongoing good practice, leading to the preparation of an ELT presentation and a paper to the Audit, Standards and Risk Committee and MCA Board as part of an annual report.

Recording and Reporting

Regular reporting is required to demonstrate that action is being taken to manage risks and that this is regularly taking place. It allows SYMCA to respond to situations as they arise and make appropriate decisions to avoid issues before they happen. This forms a key aspect of the organisation's approach to governance.

The requirement is that the management of risk process and output will be documented and reported through appropriate mechanisms, in line with the table below and the arrangements for governance of the process and its output. Escalation and de-escalation of risks is in line with the table below:

Score	Rating	Monitoring and Review and Recording and Reporting *
16-25	High	Risk Owner Review = Monthly Reporting = Quarterly to directorate leadership team, ELT and to ASRC.
11-15	Med/High	Risk Owner Review = Monthly Reporting = Quarterly to directorate leadership team, ELT and to ASRC.
5-10 **	Medium	Risk Owner Review = Quarterly. Reporting = Quarterly to directorate leadership team.
1-4	Low	Risk Owner Review = Six monthly. Reporting = Quarterly to directorate leadership team.

*The frequency of Reporting may be shortened, by exception and where required, but it is not anticipated the frequency will be extended.

**Risks which have a health and safety focus have a low appetite, any scored 5 and above will be escalated to ELT for visibility, guidance and to determine regularity of reporting. All corporate risks will be reported to ASRC.

The expectation is that risks are escalated through directorate leadership teams and ELT for awareness and any additional decisions. [Any risks identified within these forums should be captured appropriately.](#) Executive escalation and reporting should always take place prior to reporting to the non-executive committees e.g. Audit, Standards & Risk Committee and MCA Board.

The Framework and its implementation will result in **all** risks being reported annually to ELT.

Directorate leadership teams, ELT and ASRC may request deep dives into the high-level risks that face the organisation on an ad-hoc basis, and this will require risk owners to develop presentations, which provide an accurate representation and provide assurance focused on the management of risks. The deep dives may be undertaken by working groups set up for a specific period or purpose.

Where it is not possible to effectively control a risk to a score lower than 12 e.g. where effective management may be outside of the organisation's control a risk may be tolerated and such risks will be reported to ELT where further action can be considered. Minutes of meetings should capture the discussion and decision(s) made.

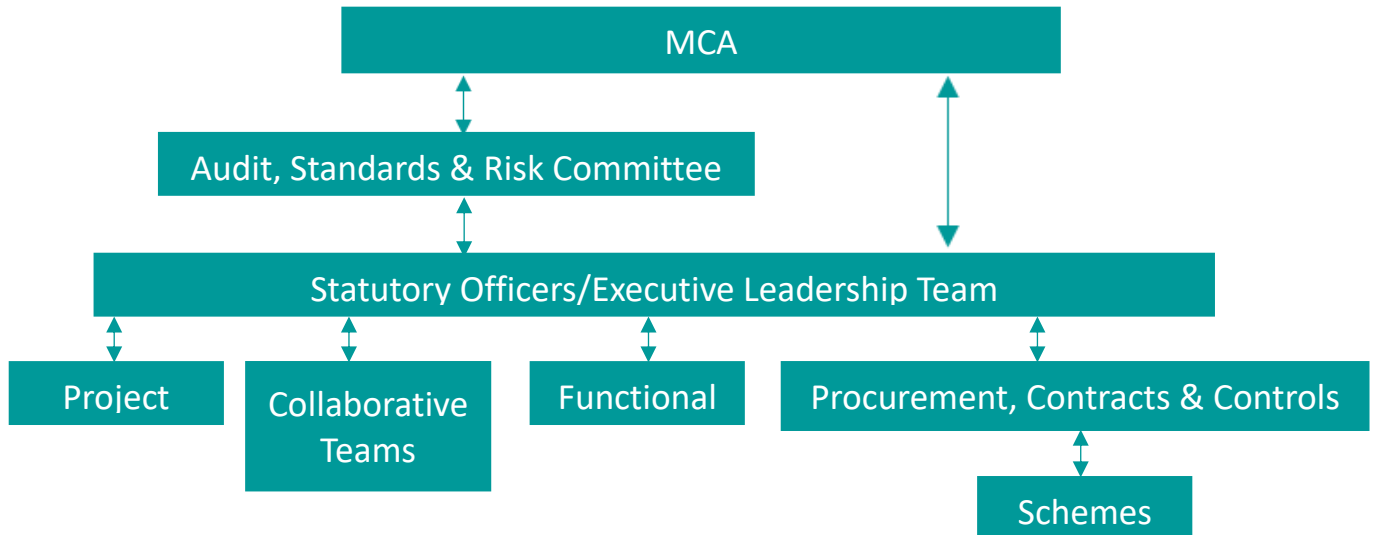
Management of Risk Technical System

SYMCA has procured the 4Risk system to administer the management of risk and to facilitate reporting through directorates to ELT and then to ASRC. Risk owners are required to maintain their risks within the system in line with the above monitoring requirements. Access

permissions and training ~~have are been~~ provided and an intranet page ~~has been developed is~~ available, which contains supporting materials.

Governance

The diagram below provides a visual representation of the flow of risk information within the standing structure of the MCA.



To supplement the above diagram, the table below provides an overview associated with risk register reporting and responsibilities to assist in decision making.

Group	Risk Reporting and Responsibility
MCA Board	<ul style="list-style-type: none"> The MCA Board will receive an annual report on the risks, the type and exposure, which is within the context of the SEP, the Corporate Plan and Business Plans. Risk Management is included as a heading within the standard MCA report format ensuring that it is available as part of decision-making. The MCA will receive an annual report from the ASRC providing their commentary on the work undertaken in year.
Audit, Standards and Risk Committee	<ul style="list-style-type: none"> The ASRC will receive risk reports as highlighted in the Recording & Reporting section of the Framework and commentary at each quarterly meeting. The ASRC will also receive an annual report and commentary. A Risk Management section is included in the standard ASRC paper template. Working groups may be set up, for a period or purpose, and risks reported with members seeking assurance as necessary.
Local Enterprise Partnership (LEP)	Management of risk is included within the standard board report format, forming a part of the decision-making process.
Thematic Boards	<ul style="list-style-type: none"> Programme dashboard relevant to the thematic area, generated from the Programme Management System, are presented at each meeting. Risk Management heading is included within the standard report format, ensuring risk information is available as part of the decision making.

Business Advisory Board	<ul style="list-style-type: none"> • <u>This board is advisory and does not have any Risk responsibilities</u>
Mayors Economic Advisory Council (MEAC)	<ul style="list-style-type: none"> • <u>This board is advisory and does not have any Risk responsibilities</u>
Statutory Officers and Executive Leadership Team	<ul style="list-style-type: none"> • The Corporate Risk Register and risks scored high and medium / high will be presented to ELT quarterly, for awareness and guidance , in line with the Recording and Reporting requirements of the Framework. • Extraordinary risk reporting may take place for topical themes e.g. deep dive consideration and reporting for critical and escalating risk topics. • Management of risk is included within the standard report format, ensuring risk information is available in decision-making.
Programme / Project Boards / Collaboration Teams	<ul style="list-style-type: none"> • Programme and project risk registers presented at each meeting in line with good practice programme and project management. • The approach to programme and project level risks will incorporate aspects of the Framework, including the probability impact grid, to ensure alignment. Risks will be escalated to the 4Risk system and reported accordingly where sufficient concern or opportunity warrant this.
Directorate Leadership Teams	<ul style="list-style-type: none"> • Directorate risks, including respective team-based risks, are presented and considered and takes forward the Recording and Reporting section of the Framework. Each director is accountable for the management of risks within their area, escalating to ELT and ASRC. • Programmes and project risks may be included.
Organisational Teams	<ul style="list-style-type: none"> • Team based risks, owned by the manager and defined team members, considered and presented at team meetings and at directorate leadership meetings. • Likely to contain risks relating to the programmes and operations of SYMCA.
Employees	<ul style="list-style-type: none"> • Individuals are responsible for highlighting risks with their managers to facilitate discussion and action. Subsequent addition to the 4Risk system takes place either by the manager or nominated risk owner.
Corporate Governance Team	<ul style="list-style-type: none"> • The Corporate Governance team will administer the Framework and 4Risk system, providing support and guidance as required and draw out reports for escalation to ELT and ASRC to an agreed timetable based on the information that is held in the 4Risk system. This is the extent of the Corporate Governance Team's responsibility. <p><i>(Directors will lead on the management of risks in their area of the business and self-serve to take forward the reporting requirements of the Framework).</i></p>

Context and Scope

The MCA have agreed a 20-year Strategic Economic Plan (SEP) to transform the South Yorkshire economy and society for People, Business and Places. The SEP paves the way to a Stronger, Greener and Fairer economy as potential is unlocked to create prosperity and opportunity for all. A Renewal Action Plan has been agreed setting out the actions needed to accelerate delivery of the SEP and a Corporate Plan and Business Plans exist to operationalise delivery and risks are in this context. The scope of risk may be internal to the MCA or externally facing.

Objectives	Identify the Risks	Assess the Risks	Mitigate and Control	Risk Treatment																																													
Objectives which are clear and understood	Threats and opportunities identified	Score the risks and consider the appetite	Controls identified to manage the risk (impact & probability)	Select and implement options to address the risks.																																													
What will be achieved? What does good look like? How will we know we have achieved it?	What could happen to hamper or enhance achievement of objectives. What concerns or opportunities exist?	What is the likelihood of the risk occurring? How serious is the impact?	What is being done to control a risk? What more can be done? Who will do this and by when?	What can be done, what are the options? Can the options be implemented? Is treatment working?																																													
<p>Objectives are set out in the SEP and respective plans to a business plan level incorporating deliverables.</p> <p>Objectives may be tiered by flowing from/to the SEP, RAP, Corporate & Business Plans. They can be incorporated into team and employee performance objectives. Defining risk is in this context.</p>	<p>There are a number of ways to identify risk & opportunity to achieve objectives:</p> <ul style="list-style-type: none"> • horizon scanning & past lessons. • SWOT analysis, Strengths to Threats. • Root cause, asking why five times. • Control, Risk Self-Assessment with a range of stakeholders. <p>It is helpful to structure risk as the:</p> <ul style="list-style-type: none"> • reason for occurrence (due to...) • risk itself (there is a risk that...) • consequence (results in...). 	<p>A Risk Owner, the individual responsible for managing a risk, is defined. An Inherent score is recorded, prior to controls, using a 5x5 scoring matrix (Guide at Appendix C).</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td></td> <td>5</td> <td>5</td> <td>10</td> <td>15</td> <td>20</td> <td>25</td> </tr> <tr> <td rowspan="5" style="writing-mode: vertical-rl; transform: rotate(180deg);">Impact</td> <td>4</td> <td>4</td> <td>8</td> <td>12</td> <td>16</td> <td>20</td> </tr> <tr> <td>3</td> <td>3</td> <td>6</td> <td>9</td> <td>12</td> <td>15</td> </tr> <tr> <td>2</td> <td>2</td> <td>4</td> <td>6</td> <td>8</td> <td>10</td> </tr> <tr> <td>1</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> </tr> <tr> <td></td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> </tr> <tr> <td></td> <td colspan="6" style="text-align: center;">Probability</td> </tr> </table>		5	5	10	15	20	25	Impact	4	4	8	12	16	20	3	3	6	9	12	15	2	2	4	6	8	10	1	1	2	3	4	5		1	2	3	4	5		Probability						<p>Identify and record existing controls to mitigate each risk.</p> <p>A Current Risk Score is added, using the 5 x 5 matrix. This is compared to the Risk Appetite to decide next steps and Treatment.</p> <p>Additional actions should be added to manage the risk to within Appetite. An action owner and deadline is established.</p>	<p>Treatment driven by comparing Current Risk Score and Risk Appetite.</p> <p>Options are:</p> <ul style="list-style-type: none"> • Treat, take action to reduce. • Tolerate, accept the risk. • Transfer, pass responsibility e.g. insurance. • Terminate, avoid the activity • Take up, pursue an opportunity • Together, share with partners e.g. public private initiatives
	5	5	10	15	20	25																																											
Impact	4	4	8	12	16	20																																											
	3	3	6	9	12	15																																											
	2	2	4	6	8	10																																											
	1	1	2	3	4	5																																											
		1	2	3	4	5																																											
	Probability																																																

Monitoring and Review

Risks, controls & process are monitored and reviewed leading to learning and improvement. Has the action been taken? If not, what next? Has anything changed?

This step is required to improve the effectiveness of the process, implementation, output and outcomes and should be planned and regularised. The results of this should be incorporated within the management of risk processes, performance measurement and reporting activities. This section includes the ongoing monitoring and review of risks by risk owners.

Recording and Reporting

This step is required to provide information for decision making, learning lessons and improving management of risk activities, process, output and outcomes. Processes, activities and output should be documented and reported through appropriate management structures.

Score	Rating	Monitoring and Review and Recording and Reporting *
16-25	High	Risk Owner Review = Monthly Reporting = Quarterly to directorate leadership team, ELT and to ASRC.
11-15	Med/High	Risk Owner Review = Monthly Reporting = Quarterly to directorate leadership team, ELT and to ASRC.
5-10 **	Medium	Risk Owner Review = Quarterly. Reporting = Quarterly to directorate leadership team.
1-4	Low	Risk Owner Review = Six monthly. Reporting = Quarterly to directorate leadership team.

*The frequency of Reporting may be shortened, by exception and where required, but it is not anticipated the frequency will be extended.

**Risks which have a health and safety focus have a low appetite, any scored 5 and above will be escalated to ELT for visibility, guidance and to determine regularity of reporting. All corporate risks will be reported to ASRC.

Communication and Consultation

Communication promotes awareness and understanding of risk management. Consultation involves obtaining feedback and information to inform decision making. Communication and Coordination with relevant stakeholders should take place during all steps of the Management of risk process and coordination between the two facilitates factual, timely, relevant, accurate and understandable exchanges of information, which should take account of data protection requirements.

Risk Register Template

Appendix B

Category	Risk Description			Owner	Pre-response assessment (inherent)			Existing Controls	Current risk assessment (residual)			Action	Action Owner	Due date 00/00/00
					Probability 1 - 5 L - H	Impact 1 - 5 L to H	Inherent Risk Score		Probability 1 - 5 L to H	Impact 1 - 5 L - H	Current Risk Score			
	Due to	Risk	Result											
Organisation	Cyber Security There is an increase in cyber-attacks which may lead to infiltration of our systems resulting in operational disruption, data corruption, outage and loss of finances.			Ruth Adams	5	5	a. Anti virus software, updated hourly, installed across all infrastructure. b. Mimecast, Advanced Threat Protection, installed, evolves to address current threats, covers email filtering to identify and block impersonators and filtering attachments for abnormalities for the IT team to check prior to release.	3	5	a. Cyber Essentials accreditation.	XXX	a.01.04.22 b.		

The assessment of risk takes account of the probability or likelihood of a risk occurring at a point in the future and the impact if it was to materialise. Each risk is scored using a five-by-five scoring matrix, a guide to the scoring is included below:

Probability, the following approach is used:

Probability Descriptor	Remote	Unlikely	Possible	Probable	Highly Probable
Score	1	2	3	4	5
Description	Highly unlikely to occur	Unlikely to occur	Could occur at some point	More likely to occur than not	Very likely to occur

Impact, the table below has been prepared to help guide colleagues, to describe the types of impact a risk may have and the different levels. The table content is not meant to be absolute and is offered as a guide for employees, risk owners, managers and directors. Additionally, where a risk has a different level of impact in several areas (or no impact at all), then the risk owner should use their professional judgement to define the impact score.

Impact Description	Immaterial	Minor	Moderate	Serious	Critical
Score	1	2	3	4	5
Reputational relates to the perception of the MCA by employees, partners and stakeholders.	Isolated, internal issue contained within the MCA no adverse publicity.	Minor internal issue, minimal external publicity, a single adverse article	Short term adverse local / regional publicity. Reduction in stakeholder confidence.	Adverse regional / national publicity. Serious reduction in stakeholder confidence.	Sustained adverse regional / national publicity. Stakeholder confidence lost.
Environmental relates to worldwide +1.5°C temperature increase and the target to be net zero by 2040.	No adverse impact on the environment.	Minor levels of carbon output or impact on the environment.	Modest levels of carbon output or adverse impact on the environment locally.	Serious levels of carbon output or impact on the environment regionally.	Critical levels of carbon output and extensive damage to the environment nationally.
Financial relates to the financial viability / health of the MCA and strength over time to achieve strategic and	Immaterial financial loss or cost, contained within budget.	Minor loss or costs that can be contained within budget.	Modest loss or costs that cannot be contained in budget requiring a new budget to be approved	Loss or costs detrimental to the financial health of the MCA. Single year risk.	Loss or costs that destabilise the financial health of the MCA. Multiple year risk.

financial objectives					
Legal and Regulatory Compliance adherence to laws and regulations incl. professional standards, ethics and fraud.	No impact or statutory compliance breach.	Minor breach in regulatory compliance.	Single breach in statutory responsibility. External recommendations and Improvement notice applied.	Multiple breaches in statutory responsibility. Improvement notices and enforcement action.	Extensive breaches in statutory responsibility and sanctions. Prosecution.
Health & Safety relates to the health & safety of MCA employees, service users, partners and stakeholders	No injury.	Minor injury suffered, no professional medical treatment required. Small number of sick days.	Injury to individual(s) requiring professional medical treatment.	Multiple serious injuries requiring professional medical treatment or hospitalisation. Enforcement agency involved.	Injury so severe that it results in fatality of individual(s). Prosecution from enforcement agency.
Employees relates to workforce planning, capacity, capability and morale of the workforce	No impact on employees, capacity or capability.	Minor or short-term reduced capacity, capability or morale.	Low employee levels Insufficient experience. Modest employee engagement.	Employee capacity or capability causes delivery failure. Low level of engagement	Strategic objectives severely impacted due to capacity or capability. Critically low level of engagement.
Digital Security relates to digital and cyber impacts	No digital security breach. Digital assets maintained.	A minor digital security breach of low level or non-sensitive data or system. Recovery quick.	A single breach of operational data or systems. Recovered and contained.	Multiple breaches of operational data or systems. Limited ability to recover or contain. Single breach of sensitive data or critical system.	Multiple breaches of data or systems including sensitive systems and personal data or loss of data itself. Enforcement agency action and fine.

<p>Programmes and Projects relates to programmes and projects the MCA undertakes to deliver its objectives internal and external.</p>	<p>Little or no slippage to delivery No threat to the intended benefits, output or outcome.</p>	<p>Minor delay, which can be managed in the respective stage. No threat to intended benefits, output or outcome.</p>	<p>Slippage delays delivery of milestone. No threat to intended benefits, output or outcome.</p>	<p>Slippage causes significant delay to milestone delivery. Serious threat to intended benefits, output or outcome.</p>	<p>Delivery of the entire programme or project threatened and or being cancelled.</p>
--	---	--	--	---	---

Risk Appetite Statement

Appendix D

Risk appetite is the level of risk that SYMCA is prepared to tolerate or accept in the pursuit of its objectives. A risk owner is required to consider the appetite level set for each risk Group and take reasonable steps to manage each risk accordingly. Where the ability to control a risk lies outside SYMCA's control the risk may be tolerated however, reporting will need to take place in line with Recording and Reporting section of the Framework document.

Risk Appetite Level	Description
Averse (A)	To be averse to risk and avoid any uncertainty.
Cautious (C)	To prefer the safe option that has a small amount of residual risk or limited potential for reward.
Open (O)	Willing to consider all options for an acceptable level of reward and value for money.

The following table provides the MCA guide.

Strategic Group	Relates to	Risk Appetite Level	What does this mean
Policy	The setting of interventions to tackle specific matters to develop the strategic objectives of the MCA.	Open	The MCA is willing to consider all options for an acceptable level of reward and value for money whilst maintaining oversight through management reporting.
Organisational	The structure and makeup of the organisation to deliver the objectives and the corporate plan.	Open	
Financial	Establishment and maintenance of financial health and wellbeing to achieve strategic and financial objectives.	Cautious	There is a preference for a safe option where the MCA is exposed to a reduced level of risk. Effective controls are required to address any remaining risk.
Commissioned Operational Delivery	The programmes and projects of the MCA to deliver the objectives set for the region.	Cautious	
Transport	Operational transport related matters that would have historically formed part of the Passenger Transport Executive.	Cautious	
Legal Compliance & Regulation	The obligations the MCA is required to adhere to including the upholding of laws, statutes and regulations.	Averse	The MCA has a very low appetite for risk and expects minimal exposure. Therefore, effective control arrangements are required to manage risk.
Outside of the Strategic Groups			
Health & Safety	Matters with a focus on health and safety.	Averse	
Cyber Security	Matters with an increased cyber security focus	Averse	