West Yorkshire Combined Authority

Corporate Risk Management Strategy

January 2020

Document History

Version	Comments	Date
0.1	First draft for approval 06/10/17	September 2017
0.2	CT Amends	October 2017
0.3	LP Further Amends	October 2017
0.4	LP amends following LT/Governance & Audit Committee feedback	November 2017
0.5	LP amends following consultation with DPO and to include Internal Audit recommendations	May 2018
0.6	GL amends Risk Register hyperlink and information on Regulatory and Compliance Board	Feb 2019
0.7	GL makes updates to document to include recommendations of Internal Audit	May 2019
1.0	Draft refresh for consultation	October 2019
1.1	GL makes updates to document to include recommendations of Internal Audit	November 2019
1.2	GL incorporates feedback on risk v issue, escalation, risk culture, information governance	November 2019
1.3	GL further amends - LEP Board and Section 73 Chief Finance Officer	December 2019
1.4	GL incorporates feedback from SMT	December 2019
1.5	GL updates hyperlinks	December 2019
1.6	Approved by Governance and Audit Committee	January 2020

1. Policy Statement

1.1. Risk management is a planned and systematic approach to the identification, evaluation, prioritisation and control of risks and opportunities facing an organisation, and to establish and maintain an appropriate risk appetite with proportionate boundaries and tolerances.

1.2. The West Yorkshire Combined Authority recognises that effective risk management is an integral part of good corporate governance and as such should be a part of everyday management processes across the organisation. The Combined Authority is committed to ensuring robust risk management arrangements are in place and operating effectively at all times.

1.3. The Senior Leadership Team (SLT) will champion risk management by ensuring that appropriate arrangements are maintained, monitored and controlled. This is demonstrated by the appointment of the Director of Corporate Services as the Combined Authority's Senior Information Risk Officer (SIRO), to reinforce to all employees the importance of compliant and effective information management and governance. The Director of Corporate Services is the nominated organisation's Risk Champion at SLT level.

1.4. The LEP has agreed that the Combined Authority will manage risks on the LEP's behalf, through the section 73 Chief Finance Officer.

1.5. This strategy clearly sets out the roles and responsibilities of the day to day management of the risks affecting the Combined Authority.

1.6. The Combined Authority commits to:

- Use a structured and consistent risk management approach to focus discussion, prioritise resources and enable justifiable risk-taking.
- Ensure that risk management is applied in a scalable and proportionate way.
- Make the best use of management information to build a complete picture of the key risks and issues and to jointly report on risk and performance management.
- Ensure risks are owned and managed in line with the organisation's commitment to outcomes-based accountability.
- Listen to feedback and regularly review our risk management arrangements to make sure they are still fit-for-purpose.
- Ensure that all risks are managed at the most effective and practical managerial level.

2. Achieving Effective Risk Management

2.1. This will be achieved by:

- Embedding clear risk management roles and responsibilities and formal risk reporting lines.
- Integrating a process for continuous review of risks, including proactive management and monitoring of mitigating actions.

- Incorporating risk management into the Combined Authority's decision-making arrangements.
- Applying principles of risk management to budget and project planning processes.
- Actively involving elected members in the risk management process.
- Regularly monitoring and reviewing our risk management arrangements to ensure they remain effective and comply with risk management standards, legislation and good practice.
- Establishing a network of champions and coordinators across the organisation to embed best practice and promote the Corporate Risk Strategy.
- Incorporating embedding risk management into the annual business planning process and incorporating risk actions into individual performance reviews.
- Providing relevant and easy-to-use risk management guidance and information, based on industry best practice.

3. Benefits

3.1. Risk management is acknowledged as an integral part of good management and a key feature of corporate governance. Effective risk management works alongside our financial management, performance management, annual business planning process and other elements of strategic and operational management to demonstrate transparency and accountability and to support the successful delivery of the commitments laid out in our Corporate Plan.

3.2. Effective risk management is a continuous process which enables us as an organisation to effectively prioritise and manage both the threats and opportunities to our ability to deliver on our commitments. By embedding a standardised approach to risk management, we are able to more efficiently prioritise resources, implement effective and proportionate controls to threats, and exploit commercial or collaborative opportunities. To achieve this, risk management should be a fundamental consideration of all decisions taken within the Combined Authority, at all levels of management.

4. Risk and Risk Management Definition

4.1. Risk

Whilst many definitions for risk exist, the definition used by the Combined Authority is as described in ISO 31000, as "the effect of uncertainty on objectives". This effect may be positive, negative or a deviation from the expected, and the risk is often described by an event, a change in circumstances or a consequence.

4.2. It must be noted that risks can be positive in consequence, as noted in HM Treasury Orange Book.

4.3. "Risk is most commonly held to mean "hazard" and something to be avoided. But it has another face - that of opportunity. Improving public services requires innovation - seizing new opportunities and managing the risks involved.

4.4. *Risk management covers all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress. Good risk management helps reduce hazard and builds confidence to innovate.*

-HM Treasury

Risk v Issue

4.5. Issues are events that have happened, were not planned, and are currently affecting the Combined Authority, service area, portfolio or project in which they sit. Risks, should they occur, become issues.

4.6. If a risk has materialised and become an issue, the risk will need to be re-assessed to consider whether there is a continuing threat it may occur again. If not, the risk can be closed and should be reported through the escalation and reporting routes described in section **9.6.** If within a project or programme managed by the Combined Authority, the issue should be recorded in an issue log (templates are available from the Portfolio Management and Assurance team).

5. Risk Appetite Statement

5.1. Risk appetite is the level of risk the Combined Authority is prepared to tolerate or accept in the pursuit of its strategic objectives. Our aim is to consider all options to respond to risk appropriately and make informed decisions that are most likely to result in successful delivery and deliver value for public money, whilst encouraging acceptable levels of risk-taking in pursuit of innovation and transformational change.

5.2. Despite mitigation, some risks can never be removed. The purpose of the appetite is to help the organisation prioritise categories of risks and to determine how to most efficiently divert resources into mitigating action.

5.3. The acceptance of risk is subject to ensuring that all potential benefits and risks are fully understood and that appropriate measures to mitigate risk are established before decisions are made.

5.4. As the Combined Authority is a multi-faceted organisation with a variety of functions, stakeholders and aims, a variable risk appetite has been set for the organisation depending on the area of risk to which it relates. The risk appetite has been set from 1 to 5, to align with the organisation's risk assessment matrix and allow easy comparison. In normal circumstances, if a risk is found to have a higher rating than the appetite allows for, mitigating action must be implemented to reduce the risk to a level within tolerance. For example, a risk relating to 'People and Culture' found to be 'High (4)', should be reduced at a minimum to 'Medium (3)' to fall within the organisation's appetite. Please be aware that there will always be risks which cannot be reduced to within acceptable levels. This is often the case if the risk falls beyond the control of the Combined Authority, or we have a statutory duty to deliver a service with a high level of inherent risk. In this case a discussion and decision to 'Tolerate' the risk must be taken. If, after relevant mitigation, a risk falls considerably outside the Risk Appetite, this may be grounds to consider the risk for escalation.

Risk Appetite Categories

5.5. The organisation's risk appetite is split into the following key categories:

5.5.1. **Legal Compliance and Regulation** – This refers to the Combined Authority's obligations to observe and uphold a variety of laws, statutes, conventions and regulations in relation to (amongst others): professional standards, ethics, bribery, fraud and information governance.

5.5.2. **Operational and Service Delivery –** The Combined Authority is a public body delivering a variety of services to the region. This refers to any risk arising from the nature of the Combined Authority's business and operations, for example, the risk of a failure to deliver expected services to customers, or to fail to provide the required quality in services.

5.5.3. **Finance and Resources –** the Combined Authority aims to maintain its long-term financial viability and its overall financial strength whilst aiming to achieve its strategic and financial objectives and to innovate in getting value for money, subject to the following minimum criteria:

- the Combined Authority is required to set a balanced overall revenue budget by February every year and Directors must then contain net expenditure within approved service totals;
- An appropriate level of unallocated general reserves, calculated in accordance with the approved risk-based reserves strategy; and
- Working within a set of Treasury management principles that seek to protect funds rather than maximise returns.

5.5.4. **Reputational –** This refers to the perception and reputation of the Combined Authority by its stakeholders, partners and staff.

5.5.5. **Transformational Change –** The environment the Combined Authority works in is continually changing through both its internal operations and the services it provides. This refers to any risk arising from change initiatives to enable the Combined Authority to best deliver on its long-term commitments to the region.

5.5.6. **Development and Regeneration –** the Combined Authority has a continuing obligation to invest in the development and regeneration of the region. A level of inherent risk exists to allow the Combined Authority to continue to be progressive and innovative in the delivery of this objective.

5.5.7. **Safety and Security –** This refers to any risk to the safety, wellbeing and security of the Combined Authority's staff, service users and stakeholders, as well as its physical assets, facilities and buildings.

5.5.8. **Environmental –** The Combined Authority has a responsibility to support the Leeds City Region in becoming carbon neutral by 2038. It also has a responsibility to safeguard the environment from undue physical damage or disturbance. This refers to any risk which may impact on these obligations.

Review

5.6. The Combined Authority's risk appetite statement is to be reviewed annually by SLT, Regulatory and Compliance Board, the Risk Coordinators and Governance and Audit Committee.

Table 5.1: Combined Authority risk appetite levels

	Low ↔ High Appetite					
	1	***2***	***3***	***4***	***5***	
Legal Compliance and Regulation	**1**					This is something for which the Combined Authority has no appetite for and expects minimal exposure to risk. Where it relates to a service which must be provided, significant controls must be in place.
Safety and Security	**1**					
Finance and Resources		**2**				There is a preference for what are deemed to be 'safe' options where there is a reduced degree of risk. Good controls are expected to be in place where risk remains.
Reputational		**2**				
Environmental		**2**				
Service Delivery and Operational			**3**			The Combined Authority accepts a level of risk may remain in the delivery of services in pursuit of our corporate priorities. The chosen option must present a healthy level of reward in relation to the risk faced.
Transformational Change				**4**		This is an area in which the Combined Authority has an increased appetite for risk. More uncertainty can be tolerated in seeking opportunities for improvement, commercialisation or innovation.
Development and Regeneration				**4**		

6. Risk Management Approach

Risk Registers

6.1. The Combined Authority collates risks into the following registers. These can be summarised as follows:

- **Corporate Risk Register** – contains the main on-going or long-term risks to the Combined Authority and its strategic objectives on an organisational. These

risks are owned and managed by the Senior Leadership Team, the register is updated and reported on by the Transformation and Performance Team.

- **Directorate Risk Register/s** – contain risks specific to the business plans, processes and operating environment for each directorate. These risks are managed by Directors and their Heads of Service. Risks within Directorate Risk Registers can be escalated to the Corporate Risk Register through Senior Management Team.
- **Service and Team Risk Register/s –** contain risks specific to the operations and processes of delivering services within each team. These risks are managed by the relevant Head of Service and Team Managers. Risks within Service and Team Risk Registers can be escalated through Directorate Management Teams.
- **Compliance Risk Registers –** registers such as the Health and Safety risk register and the Information Governance risk register contain risks which are cross-organisational but focus around one particular risk type. Whilst these are updated and monitored by corporate teams to ensure overarching risks are managed through appropriate policies and procedures, operational risks are owned by the individual teams and service areas in which the risk exists, and the implementation of specific controls must be carried out by these teams at the local level. Risks within these registers can be referred to another relevant register by the DPO, Health and Safety Business Partner, or the Regulatory and Compliance Board.
- **Portfolio Risk Register/s** – contains risks specific to the portfolio of funding programmes. These risks are managed by the Portfolio Management Group. Risks within the Portfolio Risk Register can be escalated to the Corporate Risk Register by the Portfolio Management Group.
- **Funding Programme Risk Register/s** – contains risks specific to each of the Funding Programmes that the Combined Authority is responsible for. These risks are managed by the relevant Programme Funding Group. Risks within Funding Programme Risk Registers can be escalated to the Portfolio Management Risk Register by the relevant Programme Funding Group.
- **Project and Programme Risk Register/s** – contain specific risks related to individual projects and programmes and are owned by project and programme managers with oversight from the relevant Head of Service. Risks within these registers can be escalated to the relevant Funding Programme Risk Register by the relevant Project or Programme Board.

6.2. Unless a project or programme is not sponsored by the Combined Authority, all risk registers must use the Risk Register Template available here.

6.3. All risk registers must be stored in line with our data and information governance policies available here, and made available to the Transformation and Performance Team or Internal Audit on request.

Inherent and Residual Risk

6.4. Inherent and residual risk (sometimes referred to as gross and net risk), refers to the level of the risk faced before any mitigating action (inherent/gross), and the remaining risk once all mitigation has been put in place (residual/net).

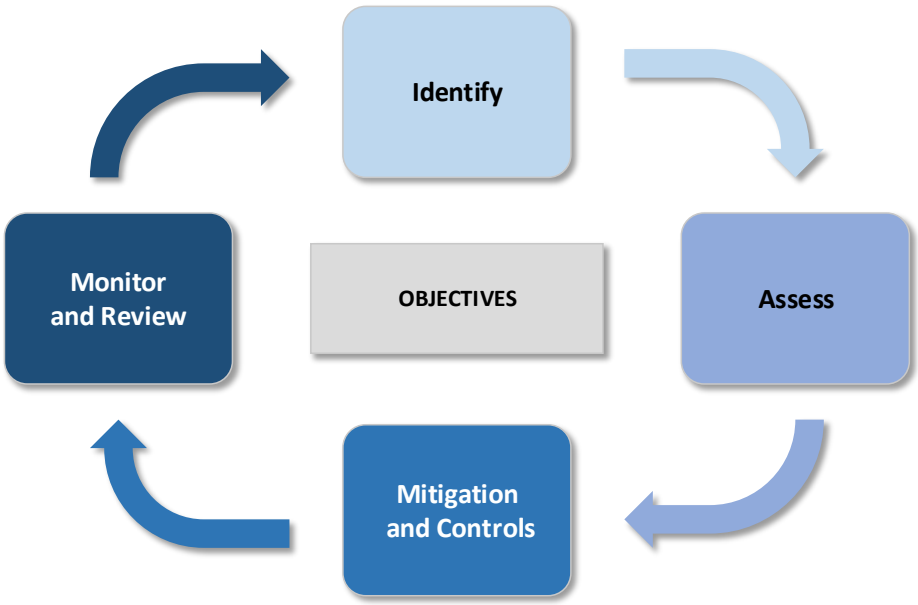
6.5. Our organisational risk register template focuses only on the residual/net risk, i.e. the risk that we are facing *as of this moment* taking into account all existing mitigating action. This is because the environment in which we operate is prone to circumstantial changes, and rarely will a risk have no existing controls or mitigation in place when assessing its rating.

6.6. The risk register template automatically populates the travel of a risk (the change in severity since previous review). Any risks substantially increasing in severity are likely to require more formal discussion and/or mitigating action.

Risk Management Process

6.7. The risk management process is broken down into 5 key steps below. The process is a series of logical steps to progress through, when managing any given risk.

6.8. The process is cyclical, and it is often necessary to revisit earlier steps and carry them out again to ensure you have a complete picture of the threats or opportunities to the activity or outcome you are assessing.



6.9. Further details on each of these stages, with a summary of recommended actions and outcomes, is provided in a 'Risk Management Process on a Page' document below. The full version can be seen on the following page.

6.10. Please note, risks which have passed or no longer exist should not be deleted. Risks should be marked as closed in the status column of the register, and greyed out. If a risk has changed substantially in nature it should be closed and a new entry added, rather than reworded.

Risk Culture

6.11. Effective risk management comes from a position of knowledge. Only by discussing risks can we as an organisation determine the correct action to take, and proactively managing risk events before they occur often saves significant time and resources than reactively managing issues. All managers and staff should strive to create an open and honest environment where the disclosure and discussion of risks is welcomed and encouraged.

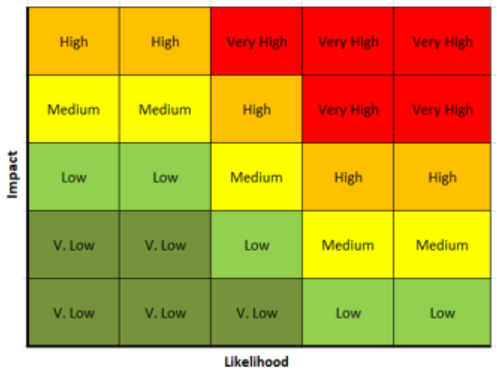
6.12. Recognising and raising a risk does not indicate ownership of the risk to the staff member who raised the risk. Each area of the organisation has a responsibility to raise risks of behalf of the Combined Authority as a whole.

Risk Language

6.13. To help record and frame risks in a uniform way, the following standardised phrasing has been introduced into Risk Register templates and should be used. You should note: the reason for the risk occurring ("Due to…"); the risk itself ("There is a risk of…"); and the consequences ("Which may result in…").

West Yorkshire Combined Authority

Risk Management Process on a Page

Step:	1. Objectives *In order to effectively identify risks, clear objectives must be set and understood.*	2. Identify *Once objectives are understood, all threats and opportunities to achieving these must be identified.*	3. Assess *To prioritise the most serious risks, and consider the organisation's risk appetite.*	4. Mitigation and Control *To manage risks, mitigations must be put in place to reduce either their impact or likelihood.*	5. Monitor and Review *To ensure mitigations are implemented, and to record risks and track changes.*
Ask:	What are we trying to achieve? What outcomes will determine our success?	What will stop us achieving these objectives? (threat) What additional benefits could we exploit from this? (opportunity)	What is the likelihood of the risk occurring? What would the level of impact be if it happened?	What can we do about it? Who will be involved, and when can this be completed by?	Where do we record the risk? What if a risk has changed?
Do:	Objectives can be assessed depending on the circumstance: in the case of project management this might be through the outline business case. For a Directorate management team this might be from 1-year business plan objectives. Consider using: - Project or programme planning documentation - Outline business case - Corporate Plan - Annual business plans - Organisational values *Once key risks have been identified and assessed, business or project plans may need to be revised to incorporate planned mitigations.*	The following methods can be used to identify a range of risks: - SWOT analysis (Strengths, Weaknesses, Opportunities and Threats are considered). - PESTLE analysis (Political, Economic, Social, Technological, Legal and Environmental risks are considered). - Root cause analysis (include asking the question 'why?' five times to each concern, to deduce original cause). - Review lessons learnt logs - Horizon scanning and benchmarking Refer to our organisation's risk prompt list on the Risk Register Template to see additional key categories of risks and opportunities to consider. Group workshops can be particularly useful to identify the widest range from all stakeholder viewpoints. Once identified, duplicate risks can be combined, and owners assigned.	All identified risks must be scored on the organisation's 5x5 matrix (below), which provides an overall risk rating based on the likelihood and impact of a risk. Further guidance can be found within risk registers.  Once each risk has an overall risk rating, this should be compared against the organisation's risk appetite.	There are 5 key ways to respond to a risk: - **Tolerate:** accept the risk at its current level (refer to the organisation's risk appetite). - **Treat:** Implement controls to reduce the likelihood or impact. - **Transfer:** insuring against the risk or passing responsibility (not always possible). - **Terminate**: avoid the activity entirely (not always possible). - **Take the opportunity:** to exploit an opportunity risk. The risk bow-tie template and guidance can help map and plan mitigating actions. *If mitigating action is assigned to someone other than the Risk Owner, this must be noted in the risk register*.	Enter all risks into the relevant risk register. If necessary start a new one with this template. For key actions and mitigations, consider including in the action owner's performance management reviews. Ensure that risk registers are reviewed with the following regularity: **Very High:** 1- 3 months **High:** 1 - 3 months **Medium:** 3 - 6 months **Low:** 6 - 12 months **Very low:** 6 – 12 months All risk registers should be reviewed in full at least annually. More guidance here.
Output:	Clear objectives which are easily understood	List of identified risks. Identified risk owners.	Risk ratings for all identified risks. Clearly defined high priority risks.	Mitigating actions and owners. Escalation if necessary. Risk 'bow-tie' analysis	Up to date risk registers. Structured reviews.

Risk Rating

6.14. Once each risk has been assessed for probability and impact, the overall risk rating is determined by considering both probability of the risk occurring and the impact it would have if it did occur. The scoring system is demonstrated by the following matrix:

Impact						
	5 Critical	High	High	Very High	Very High	Very High
	4 Serious	Medium	Medium	High	Very High	Very High
	3 Moderate	Low	Low	Medium	High	High
	2 Minor	V. Low	V. Low	Low	Medium	Medium
	1 Insignificant	V. Low	V. Low	V. Low	Low	Low
		1 Very Unlikely	2 Unlikely	3 Possible	4 Likely	5 Very Likely
		Likelihood				

6.15. Further guidance on risk rating can be found within risk registers and in **Appendix 2.**

Risk Reviews

6.16. It is recommended that risks are reviewed with at least the regularity noted below. If the risks relate to a project or programme, reviews may need to be conducted more frequently as determined by the relevant project or programme Board. For more guidance on risk reviews, please see here.

Very High Risks	Review every 1 – 3 months
High Risks	
Medium Risks	Review every 3 – 6 months
Low Risks	Review every 6 – 12 months (consider very low risks for closure)
Very Low Risks	
Full Register Review	Review registers in full at least annually
New risks can be raised at any relevant management meeting, or in between formal review.	

7. Embedding Risk Management

Training and Awareness

7.1. All members of staff have a responsibility to understand and help implement the principles of the Corporate Risk Management Strategy. Only with a common understanding of risk management can we ensure that risks are communicated, managed and recorded effectively across the organisation.

7.2. To achieve this, it is crucial that all staff are confident in applying risk management principles and techniques, understand the principles contained within the Risk Management Strategy, and recognise the importance of risk management to good business governance and practice.

7.3. The Transformation and Performance Team provide a range of self-help resources to assist with effective risk management, predominantly through the Transformation and Performance intranet page. A risk toolkit and suite of guidance documents are available here. In addition to this, the team are available to support the delivery of focussed risk workshops and focussed 1-1 sessions with risk owners and managers. Staff will be kept up to date on developments and upskilling opportunities via notices on the intranet homepage, via Corporate Risk Management section of the intranet or through the Transformation and Performance Business Partners.

Risk Coordinators and Champions

7.4. In order to support the objective of embedding risk management across the organisation, a network of staff with increased risk management awareness and understanding is necessary. Identifying a small group of individuals with greater risk involvement will enable the efficient pooling of training opportunities, and provide a distinct forum for the discussion of risk activities and management.

7.5. Risk Champions will be established throughout the organisation. As colleagues with greater risk awareness they will act as exemplars for risk management and will promote and champion the Corporate Risk Strategy across the organisation. For maximum effect, Champions must be established at every managerial level of, with presence on every major committee or board within the organisation.

7.6. Supporting this will be a network of Risk Coordinators, with a minimum of one coordinator per Directorate. Risk Coordinators are responsible for updating the risk register for which they are responsible on a rolling basis, and reporting cross-Directorate risks to the Coordinators Group for consideration.

7.7. In certain areas of the organisation the role of Champion and Coordinator may be given to the same member of staff. Where this is not the case, they will be required to work together to ensure risks within their area of responsibility are recorded promptly and accurately.

Digitising Risk Management

7.8. To be effective, risk management must be embedded into day-to-day management, consuming the minimal amount of administrative time to effectively support the objectives of the business. To do this, we will endeavour where possible to automate processes using available technology, including automated notifications for escalations or reminders for risk reviews.

7.9. All registers, wherever possible, should be stored SharePoint, to assist with version control, automated notification, and user access management.

8. Programme and Project Risk

8.1. All programmes and projects must create, baseline and maintain a risk register. The format of these is to be determined by the sponsors. However, sponsors as a minimum are required to submit their key risks to the Combined Authority's Portfolio Management and Appraisals team (PMA) using the Risk Register template and included in the Expression of Interest and Business Case at the appropriate Decision Points, as part of any change request and as part of the Combined Authority's monitoring and reporting requirements.

8.2. All transport projects must also include a Quantified Risk Allowance (QRA) at Decision Points 3, 4 and 5 of the Assurance Framework (Outline Business Case, Full Business Case and Full Business Case with Finalised Costs). The probability value will be agreed with the Combined Authority. It would typically be expected that the Promoter would include either the P50 or P85 value. The value would be decided by the Promoter in association with the Combined Authority and would depend on local circumstances associated with the project.

8.3. Non-transport projects must include a costed risk register, which can be in a simpler form, which must be agreed with the Combined Authority.

8.4. The QRA / Costed Risk Register amount will not be held by the Combined Authority and therefore will not be managed at portfolio level, but will be managed by the programme and / or project and included in the funding agreed and detailed in the funding agreement between the Combined Authority and the Promoter. It will be the responsibility of the Promoter to manage the QRA. It is also the responsibility of the Promoter to advise the Combined Authority through the Combined Authority monitoring and reporting requirements on the status of the QRA amount.

9. Risk Escalation and Reporting

9.1. Formal processes have been established for transferring, escalating and de-escalating risks between register, which are detailed in the following table.

9.2. A network of Risk Coordinators and Risk Champions has been established to provide support and advice on escalation and on the correct areas to manage each risk, and how to recommend risks for consideration on other registers.

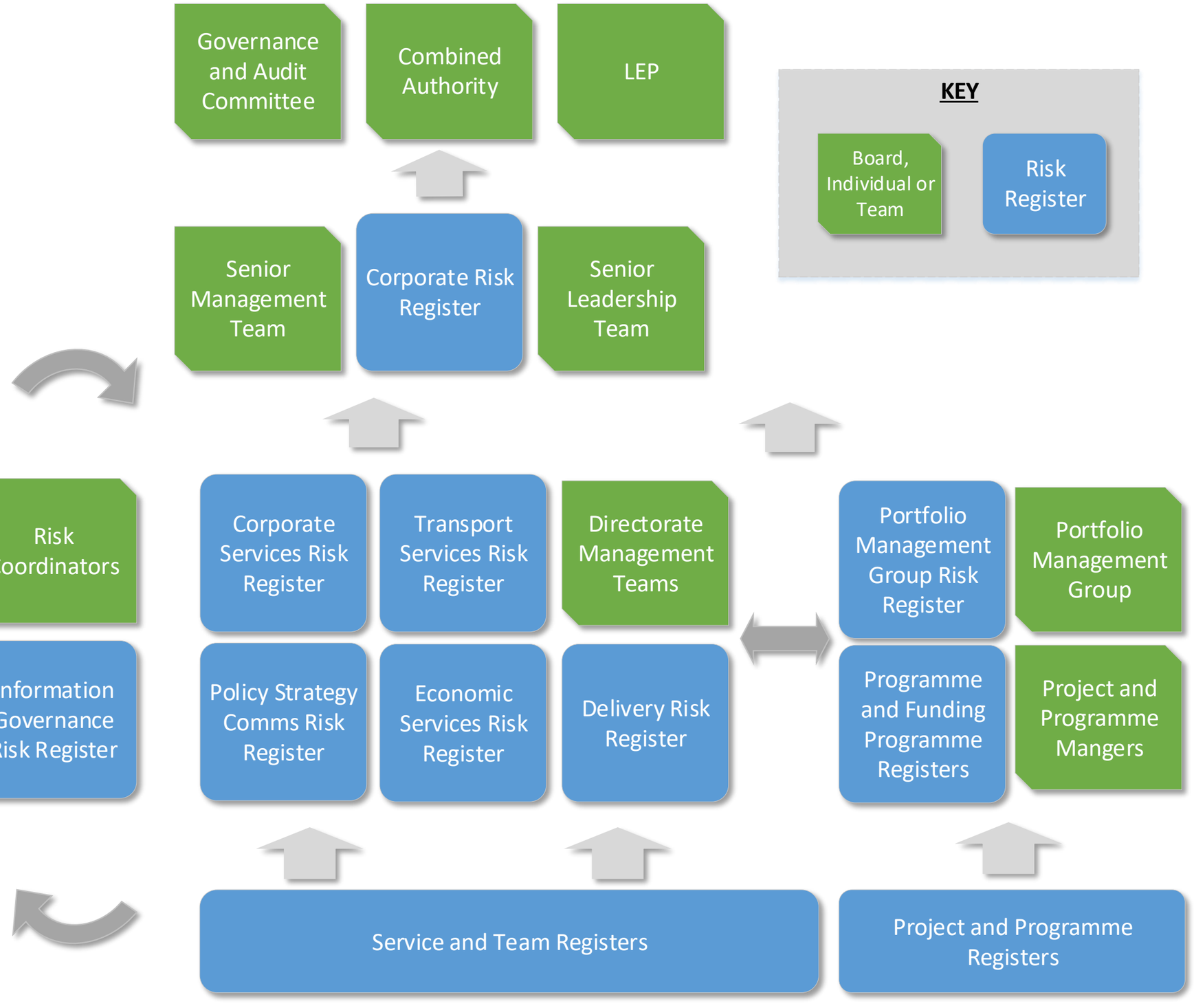
9.3. There are a number of ways a risk can be reported, such as:

- A verbal report to a line manager
- By e-mail, or writing to a relevant colleague
- Raising the concern in your own team meeting or asking your line manager or Head of Service to raise it in a relevant management meeting
- please remember you don't have to wait for a meeting to raise a risk……

9.4. If you are aware of a risk and unsure who to raise it with or how and where to record it, please speak to a relevant line manager, your area's Risk Coordinator

or the Transformation and Performance Team. Any risks which are rated very high must be considered for escalation by the owners of that register.

9.5. The formal routes for risk escalation and reporting are summarised by the diagram below



9.6. Additional detail on escalation and reporting arrangements is provided in the table below *(T+P Team refers to the Transformation and Performance Team, **R+C** refers to **Regulatory and Compliance Board**, **CRR** refers to the **Corporate Risk Register**, **PMA** refers to **Portfolio Management and Appraisal Team**, **PMG** refers to **Portfolio Management Group**).*

Risk Register	Owned/ updated by	Escalates to	Reporting and review	Assurance/ oversight by
Corporate	• Owned by SLT • Updated by T+P Team	Risks from the Corporate Risk Register can be de-escalated by **SLT** to **Directorate, Service or Team** risk registers. *A risk on the Corporate Risk Register may have iterations on Directorate register to ensure appropriate management at the relevant levels.*	Reported to every Combined Authority and LEP Board meeting through a performance snapshot provided by the T+P Team. Routine updates provided quarterly to SMT and SLT by T+P Team, urgent updates reported via standing agenda items.	• SMT • T+P Team • Risk Coordinators
Directorate	• Owned by DMT • Updated by Risk Coordinator	Directorate risks can be escalated to the **Corporate Risk Register** through the standing item on **SMT or SLT agenda**, or via the **T+P Team**. Risks to any other Risk Register can be recommended through the **Directorate's Risk Coordinator** or through the **relevant management team**.	DMT to review registers in line with recommended timescales (see section **6.16**) Individually assigned risk actions to be incorporated into and reported through 1-1s and performance reviews.	• R+C Board • SMT • T+P Team
Information Governance	• Owned and updated by Regulatory Lawyer and Data Protection Officer	IG risks can be escalated to the **relevant service or team** by the **IG team** or **R+C Board**. Significant organisational risks can be referred to Corporate Services DMT for consideration on **Corporate Services Risk Register** or escalation to the **CRR**.	IG risks reported to R+C Board through standing agenda item and through routine IG update.	• R+C Board
Health and Safety	• Owned and updated by Health and Safety Business Partner	Health and Safety risks can be escalated to the **relevant service or team** by the **Health and Safety Business Partner** or **R+C Board**. Significant organisational risks to be referred to Corporate Services DMT for consideration on **Corporate Services Risk Register** or escalation to the **CRR**.	Health and Safety risks reported to R+C Board through standing agenda item and through routine Health and Safety update.	• R+C Board
Service and Team Registers	• Owned by Head of Service or Team Manager • Updated by Risk Coordinator or Team Member	Service and Team level risks can be escalated to the **relevant DMT** by the **Risk Coordinator** or **Team Manager** from that service or team.	Service and Teams to review registers in line with recommended timescales (see section **6.16**) Individually assigned risk actions to be incorporated into and reported through 1-1s and performance reviews.	• Relevant DMT • Risk Coordinators
Portfolio Risk Register	• Owned and Updated by Portfolio Lead (Monitoring and Reporting)	Significant changes to be reported to **PMG** and **Director of Delivery.** Portfolio risks can be escalated to the **Delivery Directorate Risk Register** and/or the **CRR** by the **Director of Delivery**, through the standing item on **SMT or SLT agenda**.	Bi-monthly review by the Portfolio Management Group.	• Delivery DMT
Funding Programme	• Owned and updated by Officer delegated by Funding Programme Board	Funding Programme Risks can be escalated to the **Portfolio Risk Register** via the **PMA.**	Funding Programme risks reported to the relevant Funding Programme Board through scheduled meetings.	• PMG • PMA
Programme	• Owned and updated by Programme Manager	Significant changes to be reported to the relevant **Funding Programme Board** and **Senior Responsible Owner (SRO).** If changes affect the funding programme risk register, **SROs to report to Funding Programme Board.**	Programme risks reported to the relevant Programme Board through scheduled meetings.	• Finding Programme Board • PMA
Project	• Owned and updated by Project Manager	Significant changes to be reported to the relevant **SRO**. If significant, **SROs** to report to relevant **Programme Board.** If the project is not part of a programme, if changes affect the funding programme risk register, **SROs** to report to **Funding Programme Board**	Project risks reported to the relevant Project Board through scheduled meetings.	• Programme Board – if N/A then Funding Programme Board

APPENDIX 1 – RISK MANAGEMENT ROLES AND RESPONSIBILITIES

Group	Responsibilities
Combined Authority Members	• Reviews the Corporate Risk Register each meeting through a performance update
Governance and Audit Committee	• Responsible for seeking adequate assurance that risk management responsibilities and processes within the Combined Authority are fit for purpose.
LEP Board	• Agree with the Section 73 Chief Finance Officer the budget risks facing the LEP, at the beginning of the financial year • Reviews the Corporate Risk Register each meeting through a performance update
Senior Leadership Team	• Approves the Risk Management Strategy • Reviews the Risk Management Strategy annually • Owns and reviews the Corporate Risk Register • Reviews any risks escalated to the Corporate Risk Register
Senior Management Team	• Reviews the Corporate Risk Register quarterly
Regulatory and Compliance Board	• Reviews risk management arrangements and the management of significant organisational risks. • Considers new areas of risk to which the Combined Authority is exposed, the management of these risks, training in risks and awareness of risks across the organisation. • Reviews progress on the internal audit plan, ensuring any emerging risk issues are appropriately addressed • Reviews Health and Safety and IG risks which need to be escalated to the Corporate Risk Register
Directorate Management Teams	• Owns the Directorate Risk Register • Reviews Directorate Risk Register and escalates significant risks to the Corporate Risk Register

Group	Responsibilities
Portfolio Management Group and Programme Funding Groups	• Owns their Risk Register • Significant changes to be reported to the relevant Senior Responsible Owner (SRO) • If changes affect the funding programme risk register, SROs to report to PMA team
Project, Programme and Service Managers	• Owns individual project, programme and service risk registers • Significant changes to be reported to the relevant SRO • If project changes affect the programme risk register, SROs to report to relevant Programme Board • If the project is not part of a programme, if changes affect the funding programme risk register, SROs to report to PMA team
Transformation and Performance Team	• Updates and administers the Risk Management Strategy and the Corporate Risk Register • Prepares risk and performance reports for SMT, SLT, the Combined Authority, LEP and Regulatory and Compliance • Reports to Governance and Audit Committee on risk matters as required • Coordinates training and awareness raising activities
All CA Staff	• Consider the risks to the achievement of their team's objectives and the Combined Authority's priorities. • Ensure that any risks which they cannot manage or that have a cross-cutting impact are escalated to their managers. At a Head of Service level, this may mean adding the risks to the directorate risk register. At a directorate level, this may mean escalating a risk to the Corporate Risk Register.
Internal Audit (3rd line defence)	• Uses risk management techniques in its audit processes • Considers the corporate risk register when developing its audit plan.
Risk Champions	• To be familiar with and champion risk best practice, in line with the Corporate Risk Management Strategy • To ensure any risks raised when the Risk Coordinator is not present, are communicated to them for addition into the relevant risk register.

Group	Responsibilities
Risk Coordinators	• To update the risk register of the team or area which they are responsible • To escalate and report risks to other Risk Coordinators.
SIRO	• Champion risk-based information governance. • Ensure sufficient resources are made available to manage risks to information governance.
DPO	• Advise the Combined Authority of its information risk obligations, monitor compliance and raise awareness. • Report information risks to the Senior Information Risk Owner (SIRO).
Health and Safety Business Partner	• Ensure and embed a risk-based approach to Health and Safety across the Combined Authority
Section 73 Chief Finance Officer	• Responsible for ensuring the risk management strategy addresses risks arising in relation to LEP activity • Responsible for ensuring the process for the LEP board to oversee risk and escalation of risk analysis and risk management requirements within the LEP • Agree with the LEP board the budget risks facing the LEP at the beginning of the financial year

APPENDIX 2 – ASSESSMENT MATRICES

ASSESSMENT OF RISKS

Likelihood

If you're not sure about the percentage chance of a risk happening over a given timescale and you don't have the data to assess its frequency, use the probability descriptors (i.e. 'Very Unlikely', 'Possible' etc.) to determine the most suitable score.

The risk timescale – i.e. the period of time during which the risk could materialise - will vary according to the type of risk it is. For example:

- For a budget risk, it might be expected to materialise over this financial year or over the period of the Medium Term Financial Plan.
- For a project risk, it could be either over the whole of the project lifecycle or for a particular phase within the project.
- With regard to an event, the timescale will be from now until the date of the event.
- For a number of the more cross-cutting strategic risks such as those on the corporate risk register, it is likely that the risk could materialise at any time. When considering a Directorate or Corporate risk, this should be considered against existing and future business plans and any timescales indicated in these.

Likelihood Score	1	2	3	4	5
Likelihood Descriptor	**Very Unlikely**	**Unlikely**	**Possible**	**Likely**	**Very Likely**
It is…	Very unlikely to occur	More likely not to occur	Could occur at some point	More likely to occur than not	Very likely to occur
% Likelihood	Less than 5% chance	between 5% and 30% chance	Between 30% to 60% chance	Between 60% to 90% chance	More than 90% chance

Impact

Many risks could have a range of consequences: for example, a Health & Safety breach could affect an individual as well as lead to reputational and financial damage for an organisation. It's therefore possible that you assess the risk as having an impact of '3' using the Health & Safety impact, '2' for Finance and '4' for reputation.

Although you could break the risk down into several different risks covering all these areas and then score each of them to address the varying impact scores, often this can crowd a risk register and take the focus away from the actual risk 'event': i.e. the Health & Safety incident. Where possible, it's better to have 1 risk and use your best judgement to give an overall single impact assessment score. In the example above, this might be a '3' if you were to average the 3 impact scores or '4' if you decided to go with a worst-case scenario.

Impact Score	1	2	3	4	5
Impact Descriptor	**Insignificant**	**Minor**	**Moderate**	**Serious**	**Critical**
Projects / Programmes	Little or no schedule slippage. No threat to anticipated benefits & outcomes.	Minor delays but can be brought back on schedule within this project stage. No threat to anticipated benefits & outcomes.	Slippage causes delay to delivery of key project milestone but no threat to anticipated benefits / outcomes.	Slippage causes significant delay to delivery of key project milestone(s). Major threat to achievement of one or more benefits / outcomes.	Significant issues threaten entire project. Could lead to project being cancelled or put on hold.
Financial Impact	No or minimal financial cost.	Losses / costs incurred of 1-2% of budget.	Losses / costs incurred of 3-5% of budget.	Losses / costs incurred of 6-10% of budget.	Losses / costs incurred of more than 10% of budget. Not covered by insurance.
Reputation	No adverse publicity. Rumours.	Single adverse article in local media or specific professional journal. WYCA / Partner one of a number of agencies referred to.	A number of adverse articles in regional / social media mentioning WYCOMBINED AUTHORITY / Partner. Some recirculation via social media. Single request for senior officer / member to be interviewed on local TV or radio. Adverse reaction by LCR residents in social media / online forums. Short-term reduction in public confidence.	Series of adverse front page / news headlines in regional or national media. Wider recirculation via social media. Sustained adverse reaction by LCR residents in social media etc. Repeated requests for senior officer / member to be interviewed on local TV or radio. Long-term reduction in public confidence.	Sustained adverse publicity in regional media and / or national media coverage. Extensive / prolonged recirculation via social media channels. Repeated requests for Leaders / Chief Execs / WYCA MD to be interviewed on national TV or radio. Possible resignation of senior officers. Total loss of public confidence.

Service Interruption	Negligible. No impact on services.	Minor inconvenience for service users and staff. Services quickly restored.	Some client dissatisfaction but services restored before any major impacts.	Major disruption to service delivery. This could be through a single event or a series of outages.	Massive disruption to services. Recovery difficult or even impossible.
Staff	No impact on staff or service delivery.	Short-term low staffing level that temporarily reduces service quality. No impact on staff morale.	Medium-term low staffing level / insufficient experienced staff to deliver quality service. Some minor staff dissatisfaction.	Late delivery of key objective / service due to lack of experienced staff. Low staff morale.	Non-delivery of key objective / service due to lack of experienced staff. Very low staff morale.
Legal and Compliance	No or minimal impact or breach of guidance / statutory duty.	Minor breach of statutory legislation / regulation. Reduced performance rating if unresolved.	Single breach in statutory duty. Challenging external recommendations / improvement notice.	Several breaches in statutory duty. Enforcement action and improvement notices. Critical report. Low performance rating.	Multiple breaches in statutory duty. Prosecution. Complete systems / service change required. Severely critical report. Zero performance rating.
Health & Safety	No ill effects	Short-lived / minor injury or illness that may require First Aid or medication. Small number of work days lost.	Moderate injury / ill-effects requiring hospitalisation. Risk of prosecution from enforcement agencies.	Single fatality and / or long-term illness or multiple serious injuries.	Multiple fatalities and / or multiple incidences of permanent disability or ill-health.
Digital Security	No digital breach of systems or data.	Single breach of non-sensitive, non-business critical systems or data. Any loss quickly recovered and contained.	Single breach of data or systems which are operational or public-facing. Data recovered and contained.	Multiple breaches of data or system with limited ability to recover or contain the loss, or single breach of sensitive data or business-	Multiple breaches of one of more datasets including sensitive personal data, or sustained breach of business-critical or public facing systems,

				critical system.	with limited means of recovery
Environmental	Carbon neutral or negative output in comparison to alternatives. No adverse effects on air, land or water quality.	Low levels of carbon output. Minimal adverse effects on air or water quality to controlled geographic area.	Moderate levels of carbon output in comparison to alternatives. Some adverse effects on air or water quality to compact geographic area.	Noticeably higher levels of carbon output in comparison to alternatives. Noticeable adverse impact on air or water quality in wider geographic area/s.	Significantly higher carbon output in comparison to alternatives. Significant harmful effect on air or water quality to large or multiple geographic area/s.
Infrastructure	No effect on local infrastructure, communities or the environment.	Superficial damage to local infrastructure (e.g. minor road) but little disruption caused.	Medium damage to local infrastructure (e.g. minor road) causing some disruption.	Key elements of local infrastructure (e.g. school, major road) damaged causing major disruption.	Extensive damage to critical elements of local infrastructure (e.g. school, hospital, trunk road) causing prolonged disruption.