Grant Thornton

An instinct for growth™

Sheffield City Region Mayoral Combined Authority & South Yorkshire Passenger Transport Executive

Risk Management Review

May 2020

Andrew Smith
Director
T: 0161 953 6900
E: Andrew.J.Smith@uk.gt.com

Lisa MacKenzie
Internal Audit Manager
T: 0121 232 5157
E: Lisa.P.Mackenzie@uk.gt.com

Contents

Report distribution:

- Dave Smith, Managing Director (SCRMCA)
- Stephen Edwards, Executive Director (SYPTE)
- Ruth Adams, Deputy Managing Director (SCRMCA)
- Steve Davenport, Monitoring Officer (SCRMCA)
- Noel O'Neill, Interim Group Chief Financial Officer
- Stephen Batey, Head of Governance and Compliance (SCRMCA)
- Mike Thomas, Head of Financial Services
- Claire James, Governance and Compliance Officer (SCRMCA)
- Andy Mumford, Financial & Project Accountant (SYPTE)
- Dawn Marshall - Secretary to Head of Financial Services

For action:

- Ruth Adams, Deputy Managing Director (SCRMCA)
- Steve Davenport, Monitoring Officer (SCRMCA)
- Mike Thomas, Head of Financial Services
- Claire James, Governance and Compliance Officer (SCRMCA)
- Andy Mumford, Financial & Project Accountant (SYPTE)

Responsible Executives:

- Noel O'Neill, Interim Group Chief Financial Officer

Grant Thornton | An instinct for growth™

Executive Summary

Background

Risk is defined as an event or situation that could impact positively or negatively on the achievement of an organisations objectives. Risk management is defined as the culture, activities and structure that are directed towards the effective management of potential opportunities and threats to an organisation.

Effective risk management processes are central to providing the Board with assurance on the framework for achieving objectives. Effective risk management is imperative not only to provide a safe environment and quality services, but it is also significant in the financial and business planning process.

Effective risk management is a fundamental element of an organisations' governance framework and system of internal control. The risk management process involves the identification, evaluation and treatment of risk as part of a continuous process aimed at helping the organisation and individuals reduce the incidence and impact of risks that they face. Risk management is the responsibility of all staff and is a fundamental part of both the operational and strategic thinking of every part of the service delivery within the organisation.

The Mayoral Combined Authority Constitution specifies that the Audit and Standards Committee should oversee the effectiveness of the Authority's risk management arrangements.

The PTE reports corporate strategic risks and issues on a quarterly basis to the Audit and Risk Committee.

Objectives

The objective of the review was to provide an independent assessment of the design and operational effectiveness of the SYPTE's and SCRMCA's Risk Management Arrangements.

Objectives *(continued)*

Our review will focus on the following potential risk areas:

- Lack of a robust strategy, policy and procedures may lead to inconsistent or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.

- Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.

- Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.

- Inadequate escalation and de-escalation processes may lead to ineffective risk management.

- Lack of consistent management information and reporting may lead to ineffective risk management or false assurance being received.

Limitation of scope

Our findings and conclusions are limited to the risks identified above. The scope of this audit does not allow us to provide an independent assessment of all risks and controls associated with project management.

Where sample testing has been undertaken, our findings and conclusions are limited to the sample tested only. Please note that there is a risk that our findings and conclusions based on the sample may differ from the findings and conclusions we would reach if we tested the entire population from which the sample is taken.

Executive Summary

Conclusion

Significant assurance with some improvement required

We have reviewed the processes and controls around the Authority's Risk Management arrangements. The controls tested are set out in our Audit Planning Brief.

We have concluded that the processes provide **SIGNIFICANT ASSURANCE WITH SOME IMPROVEMENT REQUIRED** to the Committee.

We have provided this opinion based on the fundamentals and key elements expected to be in place as part of an organisation's Risk Management Framework. While acknowledging both organisations follow a different approach / process we have concluded that both organisations have in place:

- A Risk Management Governance Framework
- Authority Risk Management Lead Officer
- Risk Management Strategy and Policy/process
- Risk Registers

From our work, it is clear that those officers charged with the responsibility for risk management have a good understanding of risk management principles.

There is now an opportunity for both organisations to build on their existing arrangements to further enhance and embed arrangements and work towards having in place enterprise wide risk management and develop their risk maturity.

The findings of our review and subsequent recommended action is designed to assist the Authority's in working towards this goal.

Good practice

We have identified the following areas of good practice:

- Following a negative External Audit Review of its Risk Management processes two years ago, the MCA arrangements has carried out a significant amount of work to improve its arrangements, including developing and agreeing its strategy and framework.

- The PTE has significantly developed its reporting processes including utilising the functionality of the 4Risk system to produce specific oversight information such as top rated risks, heat maps and Authority risk profile.

Areas requiring improvement

We identified some areas where improvements can be made:

- The Risk Management Strategies are now due for review. There is an opportunity for both Authority's to take a collaborative approach in refreshing their Strategies, with a view to aligning their current processes and identifying the integration of roles, responsibilities and reporting requirements.

- Working towards enterprise wide arrangements, both Authority's need to ensure there is a consistent agreed approach to recording, monitoring, updating and scoring and moderating risks.

- There is scope to expand and develop Risk Appetite across both Authority's, in particular to align with decision making processes.

- The MCA is currently reliant on manual spreadsheet software to record, mange and monitor its risk. This is labour intensive in terms of updating and reporting progress, with limited reporting functionality. It is recommended the option of expanding the use of the 4Risk system is considered as an option moving forward.

Recommendations

Based on our findings, we have raised 18 recommendations. The grading of these recommendations is shown below:

	High	Medium	Low	Improvement
Detailed findings	-	1	17	-

Acknowledgement

We would like to take this opportunity to thank your staff for their co-operation during this internal audit.

Action Plan

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Risk Maturity	As part of our audit testing we have carried out a Risk Maturity Assessment to provide an overview of the extent to which the board and management determine, assess, manage and monitor risks. Our assessment determines whether elements of the risk management framework such as risk registers, risk appetite and reporting are comprehensive and whether risk management is embedded across the whole Authority. See **Appendix 1** Our assessment has considered a number of key areas of the risk management framework including: • Leadership • Risk Strategy and Policies • People • Processes • Risk Handling and • Outcomes. The outcome of our assessment is considered against five levels of Risk Maturity. For both the SCRMCA and SYPTE, the outcome of our assessment has identified both organisations as Risk Defined, working towards Risk Managed. This can also be described as "Emerging" as shown in **Appendix 2**. Both Authority's demonstrate the key characteristics of a Risk Management Framework expected to be in place at this level. The Risk management maturity timeline shown at **Appendix 3** is an example of how the current arrangements can now be further embedded, along with consideration of the outcome of our review, to enable the Authority's to become risk managed and working towards risk enabled.	

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of a robust Strategy, policy and procedures may lead to inconsistent or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**MCA** The MCA does not currently have an annual Business or Corporate plan and therefore local Strategic Objectives have not been set. Sheffield City Region's (SCR) vision is contained within the 10-year Strategic Economic Plan (SEP). The SEP, which was approved in 2014, is a formal statement that captures the ambition, vision and strategic priorities of SCR. The Risk management Policy states: "The MCA is accountable for agreeing a Strategic Economic Plan (SEP) which captures the ambition, vision and strategic priorities of the MCA and the LEP. The LEP lead on the development of the SEP with the support of the SCR Executive Team who develop the plan and establish a set of commissioning plans against the priorities of Skills, Infrastructure, Transport, Housing and Business Growth." The Risk Management Policy / risk registers are therefore not aligned to MCA Strategic Objectives, they are currently categorised by theme. However the Authority's Assurance Framework and therefore subsequent decision-making processes are aligned to the 10-year Strategic Economic Plan. **Recommendations**	A conscious decision was taken to categorise risk by theme and instil Risk Management principles whilst a new SEP was being delivered and the devolution deal being completed. The principles of Risk Management are now embedded and the time is right to link risks to our strategic objective.
	Issue identified: At the time of our review, the MCA did not have an annual Business or Corporate Plan setting out is short to medium term Strategic Objectives. **Risk:** The Authority may not have fully identified its local strategic objectives and the importance that **short-term objectives** play in achieving the long term vision. **Recommendations:** • The Authority to produce an annual Corporate Plan setting out its local strategic objectives and how these contribute to achieving the long term vision. • Following agreement of its objectives, the Authority to consider and identify the risks that may prevent achievement.	**Actions:** Agreed. A Corporate Plan setting out its strategic objectives will be developed in 2020/21 linked closely to the Strategic Economic Plan alongside the devolution agreement. Risks will be identified against those objectives. **Responsible Officer:** Ruth Adams/Claire James **Executive Lead:** Dave Smith **Due date: 3**1st **December 2020**

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of a robust Strategy, policy and procedures may lead to inconsistent or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**MCA** The Authority have produced a Risk Management Policy, which is available within the public domain of the MCA website. The policy was produced in April 2018 and reviewed and updated in April 2019. The policy has been subject to review by Audit Committee and approved by the MCA Board. The policy will continue to be reviewed on an annual basis. The Authority has been subject to a number of transformational changes over the past year including becoming a legal employing organisation, restructuring of its Governance Arrangements and introduction of Thematic Boards. Further developments are still expected with the development of a refreshed Strategic Economic Plan and Local Industrial Strategy. The recent breakthrough and progress with South Yorkshire devolution will now also change the landscape, risk profile and appetite of the Authority. There is an opportunity for the Authority to ensure the 2020 refresh of the Risk Management Policy includes the re-alignment and restructuring of the Authority and identifies the change of profile and appetite for risk that devolution may create. **Recommendations**	
	Issue identified: The Risk Management Policy does not reflect the current structure or profile of the Authority. **Risk:** Risks and potential opportunities may not be fully identified or effectively managed. **Recommendations:** • The Authority to ensure that the 2020 review and refresh of the Risk Management policy reflects the current structure of the Authority, in particular including roles and responsibilities related to risk management of the Thematic Boards. • There is an opportunity to carry out this review alongside the SYPTE with a view to aligning current processes and identifying the integration of roles, responsibilities and reporting requirements.	**Actions:** Recommendation agreed. **Responsible Officer:** Claire James & Mike Thomas **Executive Lead:** Noel ONeill **Due date:** 30th June 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**MCA** Roles and responsibilities for Risk Management are clearly defined within the risk management process. However the risk management process does not give an overview of process and procedures, for example while roles and responsibilities are outlined in terms of responsibilities, it does not include information on reporting requirements, oversight, meetings and frequency etc. The Mayoral Combined Authority Constitution specifies that the Audit and Standards Committee should oversee the effectiveness of the Authority's risk management arrangements and those arrangements of SYPTE. This is reflected within the Audit and Standards Committee (A&SC) TOR as: "Its purpose is to provide independent review and assurance to Members on governance, risk management and control frameworks." It describes its role and function as: "to oversee the effectiveness of the Authority's and SYPTE's risk management arrangements, " Strategic Risks are owned by the Statutory Officers Group and managed through Strategic Risk Management Action Plans. The Statutory Officers Group TOR confirms that it is responsible for " Providing overview and management of strategic risks" Programme risk oversight sits with Thematic Boards. We examined the TOR for each of the Boards and confirmed that all show there responsibilities for risk management as: "Identifying and recommending mitigations for any programme risks or poor performance". The effectiveness of SCR's risk management approach is reviewed as part of the Annual Governance Review and is reported on in the Annual Governance Statement. A review of the Risk Management arrangements, including a review of the Strategy & Policy took place early in the year and was reported to Audit Committee in April 2019. We noted that, while there is no reference within the MCA report in respect of the effectiveness of the PTE's arrangements and whether there has been a review and what oversight has taken place, there are a series of processes that have been put in place by the PTE Audit & Risk Committee (A&RC), designed to give the MCA assurance. The MCA has sight of the PTE A&RC's ToR and workplan; it has copies of the minutes of meetings where risk management is always considered; it has a copy of the PTE A&RC annual report that specifically discusses Risk Management including what has happened in the year, what the Committee have considered and what improvements need to be made. We also note that the Chair of A&RC attends the MCA A&SC and can provide any update the Committee require or answer questions on the minutes of the PTE meetings.	

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**MCA** **Recommendations**	
	Issue identified: Operational process and procedures are not fully documented. **Risk:** The Authority may fail to effectively manage its risks **Recommendations:** The Risk Management policy to be expanded to include an overview of process and procedures, specifically around specifically reporting requirements, oversight, meetings and frequency	**Actions:** Recommendation agreed **Responsible Officer:** Claire James **Executive Lead:** Stephen Batey **Due date:** 31st July 2020
	Issue identified: The MCA does not formally report its oversight and review of the effectiveness of the PTE's risk management arrangements. **Risk:** The Authority does not meet its responsibilities set out in its Terms of Reference. **Recommendations:** The MCA to ensure that as part of its annual reporting, it includes the effectiveness of both the MCA's and the PTE's risk management arrangements, for example by including the processes in place for the PTE A&RC to provide the MCA assurance.	**Actions:** SYPTE Audit & risk papers are shared with MCA Audit and Standards Committee. MCA annual reporting will also include the oversight arrangements and processes in place that provide assurance in respect of the effectiveness of the PTE's risk management arrangements. **Responsible Officer:** Claire James **Executive Lead:** Stephen Batey **Due date:** 31st July 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**MCA** Knowledge of how to manage risk is essential to the successful embedding and maintenance of effective risk management. The Risk Management policy states that Key SCR Executive Team roles are required to complete appropriate Risk Management training. While it is noted that initial qualification training has been undertaken, it is noted that two of these key officers have now left the Authority. There is currently no ongoing training plan in place to ensure that all officers charged with responsibility for risk management have access to training or guidance. Risk Management Training does not currently form part of an Authority's induction programme. **Recommendations**	
	Issue identified: There is currently no training programme in place, and no succession planning for training key officers. **Risk:** The Authority may fail to effectively manage its risks **Recommendations:** Ensure that all officers charged with responsibility for risk management have access to training or guidance. The Authority to consider including Risk Management Awareness / Training as part its induction programme.	**Actions:** Recommendations agreed **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** 31st July 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** The Authority's Risk Management Process is robust in outlining the key elements of the risk management cycle, supported by assessment and scoring methodology. The process for managing Strategic and Operational risks is described "The recording, control and monitoring of strategic and operational risks is facilitated through Governance and Compliance function within the SCR Executive Team. Risk Management Action Plans (Risk Registers) incorporate specific information about individual risks, the existing controls in place, and action plans intended to further mitigate those risks". It has been confirmed that there is an annual review of all risks at a Senior level and risk registers and their subsequent actions plans are formally reviewed and updated on a regular basis. However, it is not explicitly clear how often this is undertaken and the risk management process does not currently specify its requirements. There may be a disconnect to identifying strategic, corporate and operational risks. While it is acknowledged that programme risks are managed at a programme level, the format of the risk registers does not easily identify between strategic and corporate or high level risk. It is not explicitly clear where there is movement in a risk, whether risks are controlled and managed or whether further escalation may be required. The current format of the registers is designed at a very high level and lends itself to managing risk at a strategic level and could be easily converted to an Assurance Map. There is an opportunity to review the current process for managing and monitoring risk with a view to splitting strategic and corporate or operational risks to ensure these are monitored and controlled at the most appropriate level.	

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** **Recommendations**	
	Issue identified: Monitoring and oversight arrangements may not be robust. It is also not explicitly clear where there is movement in a risk, whether risks are controlled and managed or whether further escalation may be required. **Risk:** The Authority may fail to effectively manage its risks **Recommendations:** • The Authority to review the current format of its risk registers, to ensure there is clarity and evidence of movement in a risk and whether risks are controlled and managed or if further escalation may be required. • Consideration to be given to separating very high strategic risks and operational / corporate risks to ensure all risks are appropriately managed and mitigated / controlled at the correct level.	**Actions:** Recommendations agreed **Responsible Officer:** Claire James **Executive Lead:** Stephen Batey **Due date:** September 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** Risks are scored based on their current risk score at the time of identifying and recording; the scoring methodology used is based on a 4x4 likelihood x impact. Scoring is not identified as Inherent and residual similar to what is usually seen in a risk management scoring methodology. Target scores are also not recorded. It is therefore difficult to monitor / see any movement in risk or provide assurance that the controls or actions being taken are adequately mitigating or controlling the risk. It is also not clear if there is robust scoring moderation in place. Our review of the Authority's risk profile showed that the following were currently scored as the Authority's top four highest score and lowest scored risks:	

Highest Scored Risks	Current Risk Score	Lowest Scored Risks	Current Risk Score
Organisational Performance	9	Programme and Portfolio Management	2
Strategy Led Prioritisation	8	Decision Making and Transparency	3
Risk Management	8	Leadership and Organisational Capability	3
Compliance	8	Ethics and Integrity	4

The design of the registers doesn't currently differentiate the Authority's risk profile. Risks are mapped to themes rather than objectives, therefore all risks receive the same oversight and monitoring regardless of score.

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** **Recommendations**	
	Issue identified: There is currently no robust scoring moderation in place and the current design of the registers and reporting processes doesn't currently differentiate the Authority's risk profile. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The Authority to ensure there is moderation of risk scoring to ensure its risk profile is accurately represented. The Authority to consider developing heat maps to record its risk profile and movement in risk.	**Actions:** Recommendations agreed and linked to earlier actions **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** September 2020
	Issue identified: Risks are mapped to themes rather than objectives, therefore all risks receive the same oversight and monitoring regardless of score. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The Authority to consider and agree its reporting and oversight requirements at each level of its Governance process.	**Actions:** Recommendations agreed and linked with earlier actions **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** 31st December 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** While the standard methodology is used at a strategic level, it may not be embedded across the Authority. While risk management processes are developing and embedding across the Authority, there is a risk of this having a silo effect with differing and inconsistent approaches developing. For example, programme risk oversight sits with Thematic Boards. Performance dashboards are now reported to each Thematic Board meeting, supported by individual programme dashboards which identify programme risks, mitigations and scoring. However these are currently produced by the PPU team, therefore there is currently no assurance that the strategy / policy are being consistently applied. Our review of programme board dashboards noted some inconsistencies in the reporting of the overall risk assessment, with some reporting by number and others by RAG rating. We also noted that while strategic risk current scores are scored in accordance with the agreed 5x5 scoring methodology, the scoring used as part of the programme board dashboards uses a 4x4 methodology.	
	Issue identified: There is an inconsistent approach to scoring risk. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The Authority to provide clarity and agreement on the approach to be taken to scoring risk and ensure there is a consistent approach to managing risk throughout all departments.	**Actions:** Recommendations agreed and linked to above **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** September 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**MCA** Risk appetite or risk acceptance is the overall level of risk an organisation is prepared to tolerate or accept in order to deliver objectives and services, i.e. the amount of risk that an organisation is prepared to seek, accept, tolerate. The Risk Management Policy describes risk appetite as "Risk appetite and risk acceptance both set boundaries for how much risk the organisation is prepared to accept in the pursuit of achieving its objectives. Appetite and acceptance are considered through the escalation process. Risk exposure and the requirement for action is considered case by case acknowledging that appetite will differ depending on context". The paragraph, although accurate, is quite generic and does not describe how it would be applied or used in managing risk within the MCA. In practice Risk appetite is not yet applied or embedded within the Authority. In developing its overall arrangements for managing risk, there is an opportunity for the MCA to expand and develop its Risk Appetite and documented Risk Appetite Statement by agreeing its tolerance for risk and the amount of risk it is willing to take, mapped against each risk theme. This can be applied by including within its scoring methodology, linking to Risk Registers; particularly in setting acceptable target scores and within its decision making processes. An example of Risk Appetite is shown at Appendix 4 along with an example of how this can be mapped to the Authority's key themes at Appendix 5. **Recommendations**	
	Issue identified: The Authority has not yet defined its appetite for risk. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The MCA to define and develop its risk appetite and acceptance model that will enable decision makers to be better aware of the risks being taken to achieve the Authority's goals and objectives and informs a consistent approach to risk-based decision-making at all levels.	**Actions:** Recommendations agreed and will be done alongside objective setting. Linked to earlier actions. **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** 31st December 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate escalation and de-escalation processes may lead to ineffective risk management.	**MCA** The policy describes the following process under risk reporting and escalation; "To ensure effective risk management, risks are reported and escalated to the appropriate level in the business. SCR has a reporting and governance structure that is based on a top-down meets bottom up approach which supports risk management at strategic, operational and project/scheme level." The policy states that Strategic Risks are owned by the Statutory Officers Group and managed through the Strategic Risk Management Action Plan and Operational risks are managed by the appropriate SCR Executive team. However, the actual process followed is not clearly defined. The current Risk Management Actions Plans are linked by themes and covers a very high level risk (strategic in most cases), but with no distinction between strategic / operational, some "themes" have been populated with low level operational risks, but receive the same oversight / scrutiny at a strategic level. **Recommendations**	
	Issue identified: Escalation and de-escalation processes are not clearly defined. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The Authority to define its level of scrutiny and oversight, supported by a clear escalation and de-escalation processes.	**Actions:** Recommendation agreed **Responsible Officer:** Claire James **Executive Lead:** Stephen Batey **Due date:** 30th June 2020

Action Plan - SCRMCA

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of consistent management information and reporting may lead to ineffective risk management or false assurance being received.	**MCA** While risk is discussed at both Statutory Officers and Senior Management Team, there is currently no agreed reporting methodology or format. From our review of Audit Committee papers it was noted that an overview and summary of risks have been reported upon twice in the last financial year: April and October 2019. The Risk Management Policy states that the Audit and Standards Committee reviews group risk profile and strategic Risk Management Actions Plans (Risk Registers), but does not state frequency. It is also noted that there is no consistent reporting methodology. In April all strategic risks were provided in their risk register format and in October a summary of all risks was provided. However this does not show the risk score, mitigation or movement. It does not provide explicit assurance to the Committee that risk is appropriately managed. There is an opportunity for the Authority to review and agree its requirements for reporting and oversight, for example top 5 risks, or risks not on track etc. There is also an opportunity for the Authority to consider if the technology it uses has the required sophistication and functionality to produce the information required, or if it should consider alternative options for example a risk management system. **Recommendations**	
	Issue identified: A lack of comprehensive reporting methodology or format. **Risk:** Board Committee and Groups charged with the responsibility for the oversight and management of risk may not receive the assurances required to effectively discharge their duties. **Recommendations:** • The Authority to consider and agree its reporting format and expectations, including the frequency of reports and information required for example, top five risks, new risks, movement in risk etc. • The Authority to review its current use of technology and consider whether there is an option to expand / share the use of the 4Risk system.	**Actions:** Agreed but action is 2 fold. Look at the frequency of reporting now but develop more comprehensive approach as strategic objectives are embedded. **Responsible Officer:** Claire James/Mike Thomas **Executive Lead:** Phase 1 Stephen Batey Phase 2 Ruth Adams **Due date:** 31st March 2021

Action Plan – SCRMCA & SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**Application of Risk Appetite** Risk appetite varies for each initiative or individual area of the SCRMCA's and SYPTE's business. Stating the risk appetite for each matter is important to assess each item of business on an individual basis. The use of a risk appetite matrix on each of the appropriate Board papers enables the Board to see at a glance where the overall risk appetite sits to enable this to be taken into account and aligned with its decision making processes. **Recommendations**	
	Issue identified: Decision making may not be aligned with the Authority's appetite for risk. **Risk:** Inappropriate decisions may be made. **Recommendations:** The Authority's to consider introducing a simple risk appetite matrix to be completed as part of the Board overview reports to enable decisions to be made inconsideration and alignment with the Authority's risk appetite for example (for illustration purposes only):	**Actions:** Recommendations agreed as earlier **Responsible Officer:** Claire James **Executive Lead:** Ruth Adams **Due date:** 31st December 2020

	Avoid	Minimal	Cautious	Open	Seek	Mature
Financial / VFM					√	
Compliance / Regularity		√				
Reputation			√			
Appetite	None	Low	Moderate	High	Significant	

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of a robust Strategy, policy and procedures may lead to inconsistent or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**PTE** The PTE have developed an Annual Business Plan for 2019/20. The plan clearly set out the Authority's strategic objectives / priorities for the financial year 2019/20, which have been developed in consultation with SCRMCA and the Executive Board. They are based on an evaluation of ongoing commitments and specific deliverables mapped against SCR Transport Strategy goals and policies. The plan clearly sets out the PTE's timeline of key activities along with responsible officers and timelines etc, however the Authority's Risk Management Framework and Strategy is not currently aligned to these Strategic Objectives. While there is a framework in place, operational risk registers are aligned to service area, therefore the risk to not achieving Authority Strategic Objectives may not be fully identified, recorded and monitored. The Authority has a Risk Management Strategy which is underpinned by a policy statement. The Strategy and policy is comprehensive in its descriptions and expectations and includes the key elements expected. However, the strategy is dated 2017 and is now due for review and updating as appropriate. There is an opportunity to do this alongside the SCRMCA to integrate the systems and align processes, in particular to consider how the PTE risks may impact and / or integrate with those SCR strategic risks. **Recommendations**	
	Issue identified: The Risk Management Strategy is dated 2017 and is due to be reviewed and refreshed. **Risk:** The Risk Management Policy may not reflect the current structure or profile of the Authority. **Recommendations:** • The Authority to review and refresh of the Risk Management Policy. There is an opportunity to carry out this review alongside the MCA with a view to aligning current processes and identifying the integration of roles, responsibilities and reporting requirements.	**Actions:** Recommendation agreed **Responsible Officer:** Mike Thomas **Executive Lead:** Noel O'Neill **Due date:** 31st July 2020

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**PTE** Roles and responsibilities for Risk Management are clearly defined within the Risk Management Strategy and Policy. However this does not give an overview of process and procedures, for example while roles and responsibilities are outlined in terms of outcomes, it does not include information on how this will be achieved for example reporting requirements, oversight, meetings and frequency etc. The Strategy confirms that the Audit and Risk Committee have delegated responsibility to provide assurances to SYPTE on the adequacy and effectiveness of the Risk Management Framework and challenge, through the consideration of periodic reports, how the Risk Management Framework is being implemented, and its overall impact. This is reflected within the Audit and Risk Committee TOR as: The Committee will advise the Head of Financial Services (Responsible Finance Officer), the Directors and the Executive Board on: "..The comprehensiveness and adequacy of the processes for risk, control and governance and of the Annual Governance Statement; the establishment and effective implementation of good risk management practices". Our review of other key Board and Sub Committee Terms of Reference found that the Executive Board is charged with "Overall responsibility for risk management including approval of the risk management strategy." Our review of Trust Exec Board minutes show regular report of risk, however the TOR do not document the requirements for oversight, monitoring and reporting. We note that Programme Board roles and responsibilities for risk management are clearly stated within its Terms of Reference including "Consider any emerging risks, either to individual projects, or to the organisation which could affect wider project progress." Membership, reporting and meeting arrangements are also clearly stated (although it is acknowledged that these arrangements are not risk management specific.	

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Lack of robust governance arrangements including clearly defined roles and responsibilities and training for risk management may lead to inconsistent, or inappropriate approaches to risk management. The Authority may fail to effectively manage its risks.	**PTE** **Recommendations**	
	Issue identified: Operational process and procedures are not fully documented. **Risk:** The Authority may fail to effectively manage its risks **Recommendations:** The Risk Management policy to be expanded to include an overview of process and procedures, specifically around specifically reporting requirements, oversight, meetings and frequency	**Actions:** Recommendations agreed **Responsible Officer:** Mike Thomas **Executive Lead:** Steve Davenport **Due date:** 30th June 2020
	Issue identified: The Exec Board Terms of Reference do not explicitly state how it will discharge its responsibilities. **Risk:** The Authority may fail to effectively manage its risks **Recommendations:** The Authority to review the Exec Board Terms of Reference and update to reflect the responsibilities of the Board specifically in terms of oversight, reporting and monitoring arrangements	**Actions:** Recommendations agreed **Responsible Officer:** Steve Davenport **Executive Lead:** Steve Davenport **Due date:** 30th June 2020

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**PTE** The PTE's Risk Management Strategy clearly sets out the Authority's Risk Appetite model and risk tolerance levels. However it is noted that the strategy includes outdated operational detail in respect of the numbers and scoring of risk and categories at the time the document was produced. Appetite is clearly linked to the Authority's scoring methodology with clear routes for escalation to Departmental and Senior Management Team for those scoring 12 or above: However, while the policy is clear in its process for scoring and escalation, it is not clear if the methodology is fully applied at division level, specifically around setting target scores and through risk monitoring arrangements. There is an opportunity for the Authority to further develop its overall arrangements for managing risk, to expand and develop its Risk Appetite and documented Risk Appetite Statement by agreeing its tolerance for risk and the amount of risk it is willing to take, mapped against each risk theme. This can be applied by including within its scoring methodology, linking to Risk Registers; particularly in setting acceptable target scores and within its decision making processes. An example of Risk Appetite is shown at Appendix 4 along with an example of how this can be mapped to the Authority's key themes at Appendix 5.	

©

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**PTE** **Recommendations**	
	Issue identified: The Authority has not yet fully embedded its appetite for risk. **Risk:** The Authority may fail to effectively manage its risks. **Recommendations:** The Authority to further develop its overall arrangements for managing risk, to expand and develop its Risk Appetite and documented Risk Appetite Statement by agreeing its tolerance for risk and the amount of risk it is willing to take, mapped against each risk theme.	**Actions:** Recommendations agreed alongside earlier recommendations on risk appetite. **Responsible Officer:** Mike Thomas **Executive Lead:** Steve Edwards **Due date:** 30th September 2020

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**PTE** The Authority uses a bespoke Risk Management System "4risk™". The software enables the Authority to manage its risk and establish enterprise-wide risk management , the software includes the following functionality: • Recording of risk at strategic, operational, and project level • enables reporting on profiling, categorisation and prioritisation of risks • provides visibility of the controls environment • tracks progress of actions through to implementation and outcome. Risks are recorded straight into the system, usually with oversight and assistant from the risk management lead. The system is supported by guidance and information with embedded scoring methodology etc. As part of our review, we sample tested 11 risks from the risk register, We noted the following findings: • In five cases, the quarterly update reports show that progress against actions has not been updated and the due dates have been rolled forward. • One risk, including the risk scoring had been changed within register. Risk 473 was originally in respect of the delayed opening of the Rotherham Interchange. This risk was then changed to "snagging" following the opening, however should have been closed down and a new risk entered. • In three cases the documented controls are actions taken or required. • In four cases the current risk score and the target risk score were the same, however the risk is still on the risk register and still being monitored. (in two of these cases the risk score was 3).	

Action Plan - SYPTE

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2.

Issue	Findings and Recommendation	Action Plan
Inadequate processes for identifying, assessing, documenting, monitoring and reporting risks or Inconsistent scoring may lead to ineffective risk management.	**PTE** **Recommendations**	

	Issue identified:
	
	Operational weaknesses within the process for recording and managing risk.
	
	Risk:
	
	The Authority may fail to effectively manage its risks.
	
	Recommendations:
	
	The Authority to ensure there is a process in place to oversee the accuracy and management of risk within the 4Risk system, including:
	
	• Risk action dates are not rolled forward, risk action progress is received and updated at least quarterly to enable timely and accurate reporting. Escalation processes are in place where this has not been received.
	
	• Risks are not changed within the system. Where a risk is now mitigated or controlled, this should be closed and any new or emerging related risks recorded, assessed and scored as a new risk.
	
	• Risk mitigating controls should be recorded and not confused with actions taken or planned to be taken. Categories and examples of controls include:
	
	  - Foundational – control that prevents something occurring (usually at the start of a process). Examples include, policy and procedure – stating what can and can't be done, or IT system controls (e.g. access restrictions)
	
	  - Specific – a control that is applied specifically during a process, for example, someone having to approve a task / expenditure, which prevents fraud or error.
	
	  - Monitoring – typically a detective control, at the end of a process. Examples include, management reporting, system exception reports
	
	• Where risks are controlled, managed or mitigated and have reached the target score, these should be closed down within the system.
	
	• The Authority should ensure that any training needs are identified and addressed.
		Actions:
		
		Recommendations agreed
		
		Responsible Officer:
		
		Andy Mumford/Mike Thomas
		
		Executive Lead:
		
		Steve Edwards
		
		Due date: On-going

Appendices

Grant Thornton | An instinct for growth™

Appendix 1 – Risk Maturity Assessment

Risk Maturity Assessment

Risk Maturity Assessment
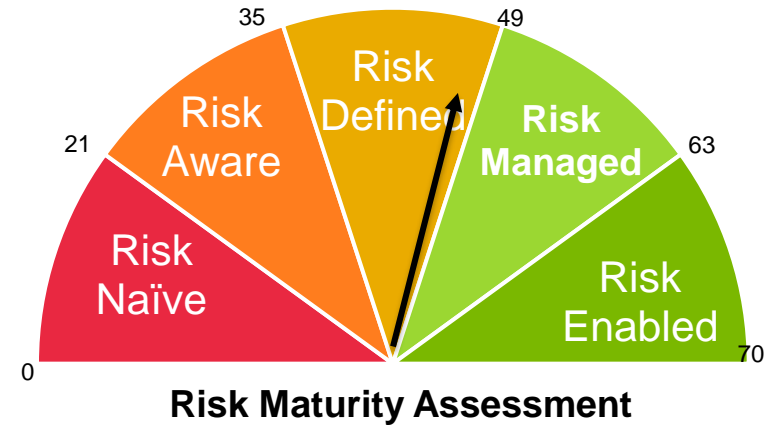
Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise wide approach to risk management developed and communicated	Risk management and internal control fully embedded in the operations

Appendix 2 – Risk Maturity Assessment

RISK MANAGEMENT MATURITY MODEL

Risk Maturity Level (vertical axis)

Key Charactristics (horizontal axis)

Very Basic
Level 1
- The organisation has minimal or no awareness and understanding of risk management.
- Risk management is performed on an ad hoc basis by individuals.
- No processes in place.

Basic
Level 2
- Risk management applied inconsistently with limited standardisation.
- Some formal processes in place.

Emerging
Level 3
- A risk management framework exists with defined and documented risk management principles.
- Risk management applied consistently throughout the organisation.
- Not all processes have been fully implemented.

Mature
Level 4
- The organisation is proactive in risk management.
- Risk management is consistently and fully implemented across the organisation.
- Key risk indicators are used for major risks.
- Risk management processes are monitored and reviewed for continuous improvements.

Advanced
Level 5
- Risk management is considered a value driver and proactively used for day to day decision making and pursuit of opportunities.
- KRIs and predictive risk analytics are proactively used to identify and monitor risks.
- Advanced and sophisticated risk management processes are used.

Grant Thornton | An instinct for growth

Appendix 3 - Risk management maturity timeline

Appendix 4 – Example of Risk Appetite

Risk Level		Descriptor	Appetite
0	Avoid	Avoidance of risk and uncertainty is a Key Organisational objective	None
1	Minimal	(as little as reasonably possible) preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential	Low
2	Cautious	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward	Moderate
3	Open	Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	High
4	Seek	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)	Significant
5	Mature	Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust	

Appendix 5 – Example of Risk Appetite

Risk Levels ▸	0	1	2	3	4	5
Key Elements ▾	**Avoid** Avoidance of risk and uncertainty is a Key Organisational objective	**Minimal (ALARP)** (as little as reasonably possible) preference for ultra-safe delivery options that have a ow degree of inherent risk and only for limited reward potential	**Cautious** Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward	**Open** Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	**Seek** Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)	**Mature** Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
Financial/VFM	Avoidance of Financial loss is a key objective. We are only willing to accept the low cost option as VfM is the primary concern.	Only prepared to accept the possibility of very limited financial loss if essential. VfM is the primary concern.	Prepared to accept possibility of some limited financial loss. VfM Still the primary concern but willing to consider other benefits or constraints. Resources generally restricted to existing commitments.	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise on opportunities.	Investing for the best possible return and accept the possibility of financial loss (with controls may in place). Resources allocated without firm guarantee of return – 'investment capital' type approach.	Consistently focussed on the best possible return for stakeholders. Resources allocated in 'social capital' with confidence that process is a return itself.
Compliance/ Regulatory	Play safe; avoid anything that could be challenged, even successfully.	Want to be very sure that we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any challenge are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better regulation.

Appendix 6 – Staff involved and documents reviewed

Staff involved

- Claire James, Governance and Compliance Officer (SCRMCA)
- Andy Mumford, Financial & Project Accountant (SYPTE)
- Noel O'Neill, Interim Group Chief Financial Officer
- Ruth Adams, Deputy Managing Director (SCRMCA)

Documents reviewed

- PTE Risk Management Strategy
- MCA Risk Management Policy & Risk Management Process
- PTE Business Plan 2019/20
- Authority Risk Registers
- Board and Sub Committee Terms of Reference, reports and minutes

Appendix 7 - Our assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Description
Significant assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management. These activities and controls were operating with sufficient effectiveness to provide significant assurance that the related risk management objectives were achieved during the period under review. Might be indicated by no weaknesses in design or operation of controls and only IMPROVEMENT recommendations.
Significant assurance with some improvement required	Overall, we have concluded that in the areas examined, there are only minor weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review. Might be indicated by minor weaknesses in design or operation of controls and only LOW rated recommendations.
Partial assurance with improvement required	Overall, we have concluded that, in the areas examined, there are some moderate weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide partial assurance that the related risk management objectives were achieved during the period under review. Might be indicated by moderate weaknesses in design or operation of controls and one or more MEDIUM or HIGH rated recommendations.
No assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are not suitably designed to achieve the risk management objectives required by management. Those activities and controls that we examined were not operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review Might be indicated by significant weaknesses in design or operation of controls and several HIGH rated recommendations.

Appendix 7 - Our assurance levels *(cont'd)*

The table below describes how we grade our audit recommendations.

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	▪ Key activity or control not designed or operating effectively ▪ Potential for fraud identified ▪ Non-compliance with key procedures / standards ▪ Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	▪ Important activity or control not designed or operating effectively ▪ Impact is contained within the department and compensating controls would detect errors ▪ Possibility for fraud exists ▪ Control failures identified but not in key controls ▪ Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	▪ Minor control design or operational weakness ▪ Minor non-compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or which represent best practice advice	▪ Information for management ▪ Control operating but not necessarily in accordance with best practice

Grant Thornton
An instinct for growth™