Grant Thornton

An instinct for growth™

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

Internal Audit 2020/21

Risk Management

July 2021

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

John Owens
Internal Auditor
T: 0121 232 8757
E: john.owens@uk.gt.com

Contents

Report distribution:

Responsible Executives:

- Ruth Adams, Deputy Chief Executive (MCA)

- Stephen Edwards, Executive Director (PTE)

For action:

- Claire James, Senior Governance and Compliance Officer (MCA)

- Nigel Cairns, Head of Facilities & Infrastructure (PTE)

For Information:

- Dave Smith, Chief Executive (MCA)

- Tim Taylor, Director of Customer Services (PTE)

- Steve Davenport, Principal Solicitor and Secretary to the Executive & Monitoring Officer

- Gareth Sutton, Group Finance Director

- Mike Thomas, Deputy Section 73 Officer

- Dawn Marshall, Secretary to the Group Finance Director and Deputy Section 73 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 PTE's and MCA's Risk Management Arrangements.

Our review focussed 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.

This report does not constitute an assurance engagement as set out under ISAE 3000.

Executive Summary

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.

Our review has been undertaken to provide assurance in respect of the arrangements in place for the year 2020/21 and up to the period of finalising the Head of Internal Audit Opinion. We have provided our opinion based on the fundamentals and key elements of a Risk Management Framework being in place but recognising these are still embedding in some areas where changes have been made.

We acknowledge that both the PTE and MCA are now in a transitional year of integration and the risk management framework will be subject to a full review. Where possible, we have therefore structured our audit recommendations to ensure that where actions may affect the joint governance structures in the future these are designed to be undertaken collaboratively and not in isolation of either organisation. There is an opportunity to further enhance and embed arrangements and work towards having in place enterprise wide risk management and a further developed risk maturity. In reaching this goal, we recognise there are a number of areas which are subject to consideration as part of the Integration legal, policy & compliance workstream. As such have not been raised additional recommendations within this report, including:

- Agreeing a joint approach and governance framework supported by an updated strategy and policy.
- Implementing a new approach to reporting.
- Consideration of expanding the use of the electronic 4Risk system to negate reliance on manual spreadsheet systems.
- Agreeing and application of a joint approach to risk appetite.

Conclusion - continued

We also note that the MCA has produced a 2021/22 Corporate Plan which supports the vision of the Strategic Economic Plan, the Renewal Action Plan and incorporates the Transport Strategy goals and objectives of the PTE. There is scope and opportunity as part of the wider integration agenda to further align the risks facing the integrated Authority to the objectives of these strategic plans

The PTE arrangements in place have remained stable over the last year. We noted improvements in the commitment to providing timely progress update reports by action owners and at the time of our review there were no overdue actions. However, we also noted that some of the issues that were raised as part of the 2019/20 Internal Audit review have yet to be addressed, for example updating the Risk Policy and ensuring the overview of process and procedures, specifically around risk appetite, reporting requirements, oversight, meetings and frequency is clearly defined. However, we do acknowledge that the wider integration agenda now supersedes the requirement for the PTE to implement a number of these actions in isolation.

It is clear to see that the MCA has invested significant time and resource into reviewing and updating its arrangements. This is evidenced by a full review and refresh of arrangements, an updated Strategy, re-formatted risk registers and approval of key appointments to drive change. Work is ongoing to develop and embed risk management arrangements further and we acknowledge this is work in progress. We did note there were some actions arising from the 2019/20 review which remain in progress specifically around reporting requirements and aligning processes with the PTE. We note that these will now be considered as part of the wider integration agenda.

Our work has concluded that the fundamental and key elements for managing risk are in place as part of the overall governance framework of both organisations, but there is still some embedding required for example ensuring that operational practises align with the strategy, particularly where changes continue to be made and to ensure that reporting arrangements provide the assurance required by the Audit and Standards Committee.

Where actions arising form the 2019/20 Internal Audit review were not fully implemented, these will continue to be followed up with progress reported to Audit Committee within the Recommendation Tracker report.

Executive Summary

Good practice

Both organisations currently follow a different approach and process, we have concluded that both organisations have in place:

- A Risk Management Governance Framework
- Risk Management Lead Officer
- Risk Management Strategy and Policy/process
- Risk Registers
- Reporting and oversight arrangements

As part of our review we have also carried out our risk maturity assessment and confirm that both organisations are assessed as risk defined. The MCA assessment has shown some increase since last year. Details are shown at Appendices 1 – 3.

Recommendations

Based on our findings, we have raised 5 recommendations. The grading of these recommendations Is shown below:

Detailed findings	High	Medium	Low	Improvement
PTE	-	-	1	1
MCA	-	-	1	1

Acknowledgement

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

Action Plan - PTE

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.

Risk 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.	The Risk Management Strategy and the Policy Statement were issued in 2017. It is noted that the documents are generally adequate, however, there is a requirement for an annual review to be undertaken as required in paragraph 4.2 of the Strategy. This finding was also raised as part of the 2019/20 Internal Audit review, but as yet has not been implemented. We also reported that while the policy does articulate risk appetite, there was an opportunity for the Executive to further develop its overall arrangements for managing risk, to expand and develop its Risk Appetite by agreeing its tolerance for risk and the amount of risk it is willing to take. We do note however that the integration of the PTE and MCA supersedes the requirement for the PTE to implement these actions in isolation and note there will be a full review of arrangements as part of the legal, policy & compliance workstream of the integration process. In the interim, we note the Executive's plan to refresh the PTE Risk Management Policy so it is as closely aligned as possible to the MCA's policy which was approved by the MCA Board in November 2020. There is also opportunity to benchmark the processes in place against good practice. There are a number of good practice standards, including the BSI Risk Management standard (ISO31000). It should be noted, however, there is no requirement to be accredited.	N/A

Action Plan - PTE

Risk 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.	The PTE does not currently have dedicated resource for the administration and management of risk. The responsibility for the co-ordination and reporting of risk, using the 4Risk system, has been delegated to the Finance and Project Manager, who reports to the Senior Finance Manager. However, the risk role is in addition to substantive responsibilities. It was also noted that the Senior Finance Manager does not provide oversight for the risk management function. Our review identified that the Finance and Project Manager does not hold a risk management qualification, although understands the subject. The Finance and Project Manager undertakes induction for new staff, briefing all new starters on risk management. Where there are new risk owners, personal and specific training is also provided. We acknowledge the limitations of roles and size of the organisation, and recognise there may be an opportunity to consider this in collaboration with the MCA as part of the wider integration agenda.	N/A

Action Plan - PTE

Risk 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.	A bespoke Risk Management System "4risk™" is used by the PTE to manage risk, 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 control environment • tracks progress of actions through to implementation and outcome. Potential risks can be identified at any level of the Executive, although it is usual practise for the initial articulation, scoring and recording of the risk to be completed in conjunction with the guidance of the risk lead. Risks are scored using a 5 x 5 impact and likelihood matrix and all new risks are reported to Audit and Risk Committee. All risks have a risk owner with access to the 4Risk software to add, change or close risks. Risks are reviewed on a regular basis by the action owners and progress updates are included. The Finance and Project Manager also undertakes a bi-monthly monitoring review to provide moderation of scoring and to ensure any changes to risks, including the closing of risks, are supported by appropriate mitigation and reasons. Where progress updates have not been included, action owners are reminded to ensure these are updated prior to the Audit and Risk Committee cycle reporting. From our review of the risk register we confirmed that risks are updated on a regular basis by the action owners and at the time of our review there were no overdue actions outstanding. We noted that there is currently no feedback loop to the recording of risk where there may have been near misses which may have occurred on site. We acknowledge that there is a process for reporting incidents (i.e. slips trips and falls), however there isn't a process for reporting near misses, however there are mitigations in place to reduce the likelihood for example of a customer being struck by a vehicle. We carried out sample testing of five risks to verify that they had been accurately captured, scored and mitigated with appropriate SMART actions in place. The results of the test concluded that the risks are captured and accurately scored, mitigated and monitored.	N/A

Action Plan - PTE

Risk 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.	**Issue identified:** There is currently no formal process for reporting near misses for consideration as an emerging or existing risk. **Risk:** The Executive may fail to effectively manage its risks. **Recommendations:** The PTE to strengthen the mitigations in place based on relative risk of each site, for example Sheffield being of higher risk than Barnsley. Ensure that any emerging risks for example a new driver or changes to stand allocation are monitored.	**Action:** Management agrees with the recommendation. The process will be implemented in consultation with the Health & Safety Officer. **Responsible Officer:** Nigel Cairns, Head of Facilities & Infrastructure **Executive Lead:** Tim Taylor, Director of Customer Services **Due date:** 30 September 2021

Action Plan - PTE

Risk Issue	Findings and Recommendation	Action Plan
Inadequate escalation and de-escalation processes may lead to ineffective risk management.	A full review of all risks is undertaken on a bi-monthly basis and any changes including changes of risk scores are included within a heat map. The escalation and de-escalation of risks are indicated by directional arrows and supported by additional narrative to explain the movement of risk in the body of the report . The heat map is included in the Risk Management reports presented for review to the Audit and Risk Committee, Transport Officers Board and the Management Board.	N/A
Lack of consistent management information and reporting may lead to ineffective risk management or false assurance being received.	The Audit and Risk Committee receive risk management reports quarterly. The Transport Officers Board and the Management Board review risks bi-monthly. Our review of evidence provided confirmed this process in place. However, we did note that the same report was provided for each oversight group and due to the timing of meetings, any updates or revisions arsing from these may not have been included within the report to subsequent meetings. For example, the risk register provided to the Audit and Risk Committee in May 2021 did not include risks relating to the integration of the PTE with MCA, however we note that the discussion had taken place at Senior Management Team prior to this meeting and it was agreed that this would be included.	
	Improvement Point: The Executive to ensure that any updates or revisions arising from Senior Management or oversight groups are reflected in the risk management report prior to any meetings thereafter.	This finding has attracted an 'Improvement Point' as opposed to a formal recommendation, and as such does not require a management response.

Action Plan - MCA

Risk 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.	Following a full internal Management Board review and Internal Audit Report in 2020, the risk management framework of the MCA was revised and refreshed. The Audit and Standards Committee endorsed the revised policy and process in October 2020 and, following their recommendation, it was approved and adopted by the MCA at their meeting in November 2020. From our review of the policy, we acknowledge that The MCA has adopted the 'Management of Risk' (MoR®) principles of risk management which are aligned to the international standard for risk management ISO31000:2009. The policy has also been updated to reference its risk appetite and acceptance level. This is currently being further embedded by developing a 'risk management strategy' for each activity so the agreed risk appetite can be documented. A risk management strategy describes the specific risk management activities that will be undertaken and will be specific to the activity concerned but, will also reflect the organisational approach to risk management. Guidance on determining whether a risk management strategy would be of use and a template to assist in its development forms part of the risk management tool kit. However, currently the risk management strategies for specific activity is not yet in place.	N/A
	Issue identified: The Authority has not yet fully embedded its appetite for risk. **Risk:** The Authority may fail to effectively manage its risks in line with its agreed appetite and tolerance level. **Recommendations:** The Authority to establish its risk management strategy for each of its activities to ensure risks are managed in alignment with its agreed appetite and tolerance level.	**Actions:** Recommendation agreed. We will establish risk management strategies for programmes of work in line with agreed policy. **Responsible Officer:** Claire James, Governance and Compliance Officer **Executive Lead:** Ruth Adams, Deputy Chief Executive **Due date:** 31st December 2021

Action Plan - MCA

Risk 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.	As part of the review of the risk management arrangements, overall responsibility has been included with the Deputy Chief Executive's portfolio. Operational management is administered by the Senior Governance and Compliance Officer who maintains the risk registers, prepares reports for the Audit and Standards Committee and advise on risk throughout the Authority. We also note there is approval to appoint additional resource. A number of risk champions have also been appointed at all levels of staff within the Authority. The Senior Governance and Compliance Officer and other key staff have undertaken Risk Management Practitioner courses provided by the Knowledge Academy.	N/A

Action Plan - MCA

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.	The Risk Management Framework and supporting processes have been subject to a full review and refresh. Risks are categorised into 5 themes, each having Executive Lead ownership: Deputy Chief Executive: • Strategy Focus. • Organisational Management • Governance and Compliance Management Group Finance Director: • Budget and Financial Management • Programme Management The risks to each theme are fully documented within the Authority's risk register. We did note that the Authority does not currently have an electronic software solution in place and is reliant on a manual spreadsheet. There is an opportunity as part of the wider integration agenda to consider the electronic system currently in use at the PTE as the joint Authority system for risk management. Risks are scored using a standard 5 x 5 matrix which aligns to the methodology used within the Board scorecard reports. Each risk is scored individually, however, each theme shows an average mitigated probability and average impact. We have acknowledged that in addition to the risk registers, high risks are identified individually within the cover paper report for Board Members oversight. The supporting action plan records the action required, target completion dates status update reports. This allows for oversight of implementation and any slippage which is reported to and monitored by the Audit and Standards Committee. We also noted that the Deputy Chief Executive is responsible for identifying the risks relating to the integration of MCA and PTE. We have reviewed the related documentation and noted that it includes work programmes to mitigate the risks that have been identified.	
	Improvement Point: The Authority to consider its use of average RAG ratings within the Risk Registers and whether there is a risk of false assurances being provided, particularly where a theme is rated as low overall but includes high or medium risks.	This finding has attracted an 'Improvement Point' as opposed to a formal recommendation, and as such does not require a management response.

Action Plan - MCA

Issue	Findings and Recommendation	Action Plan
Inadequate escalation and de-escalation processes may lead to ineffective risk management.	Risk are reviewed by the Executive Lead in conjunction with individual assigned action owners to confirm the status of actions and to update the action logs within the risk register. Any decisions to close actions are also approved by the Executive lead. Risks are subject to varying levels of monitoring and oversight, for example where the risk environment has changed Management Board are included within the oversight process, or where a fundamental change may be required a risk workshop will be held. Regular monitoring and oversight is included as part of the standard Management Board agenda. The discussions include the following questions: • Is the identification of the risk and how it is defined correct? • Are the mitigations still valid or do we need to amend mitigations? • As a result are there new actions? Any changes are captured in revised templates that form the basis of a risk paper that goes to Management Board and then to Audit and Standards Committee. We also noted that the Authority is establishing a Corporate Assurance Board which will sit alongside the Management Board which will consider risk movements for the red risks or ones moving to higher impact or likelihood.	N/A
Lack of consistent management information and reporting may lead to ineffective risk management or false assurance being received.	A risk oversight report, supported by the full risk registers are reported to each meeting of the Audit and Standards Committee. We also noted that the Authority's Thematic Board receives scorecards which include specific operational Board risks. We also noted that the Authority is in the process of implementing a cross cutting place based report which looks across all programme funds to see if there are risks linked to geography. Reporting of risk is an area recognised by the Authority as developing and embedding. From our review of Audit and Standards Committee oversight reports this is evident through the year with developments including the use of heat maps to show the movement of risk and risk profile by theme across the Authority. During the transitional period of integration, reporting requirements should continue to be considered to ensure the arrangements provide the assurance required by the Audit and Standards Committee.	N/A

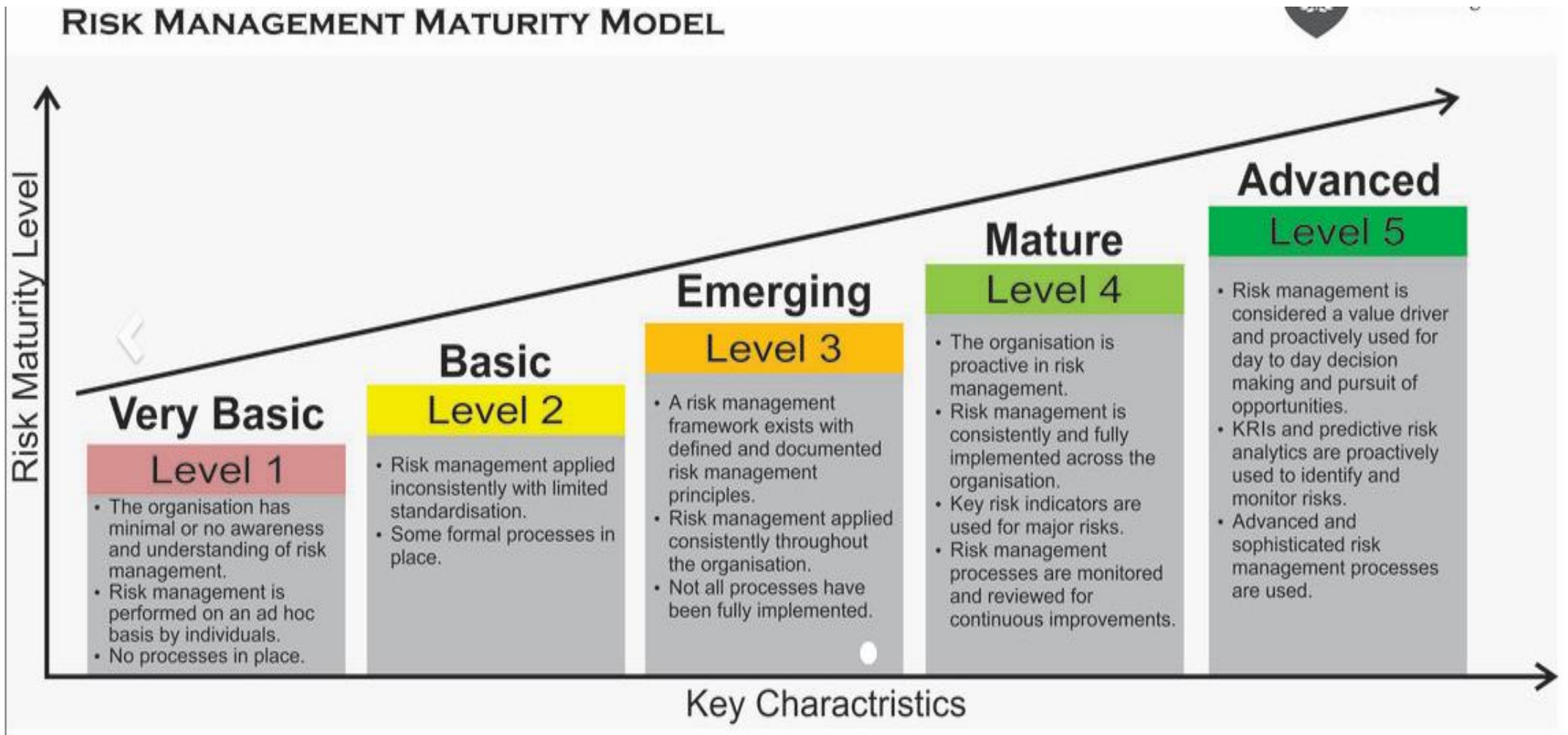# Appendices

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

Appendix 3 - Risk management maturity timeline

Risk-naive | Risk-aware | Risk-defined | Risk-managed | Risk-enabled

Risk maturity (y-axis)

Time/organizational evolution (x-axis)

Focus on compliance
Low investment
Ad hoc controls
Silo-based controls
Emphasis on mitigation
Tactical risk management
Fragmented implementation
Development of policies and procedures
Senior management commitment
Risk appetite defined
Pilot on key projects
Coordinated governance, risk, and control framework
Regular risk communication
ERM in place
Consistent language
Consistent practice
Fully embedded processes
Continuous improvement

Grant Thornton | An instinct for growth™

Appendix 4 – Staff involved and documents reviewed

Staff involved

- Claire James, Governance and Compliance Officer (MCA)
- Andy Mumford, Financial & Project Accountant (PTE)
- Ruth Adams, Deputy Chief Executive (MCA)

Documents reviewed

- MCA & PTE Risk Management Strategy
- MCA Risk Management Policy & Risk Management Process
- PTE Business Plan 2020/21
- MCA Corporate Plan 2021/22
- SEP
- Authority Risk Registers
- Board and Sub Committee Terms of Reference, reports and minutes

Appendix 5 - 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 5 - 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