CAMBRIDGESHIRE AND PETERBOROUGH COMBINED AUTHORITY

Risk Management

Internal audit report: 1.20/21

FINAL

15 January 2021

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

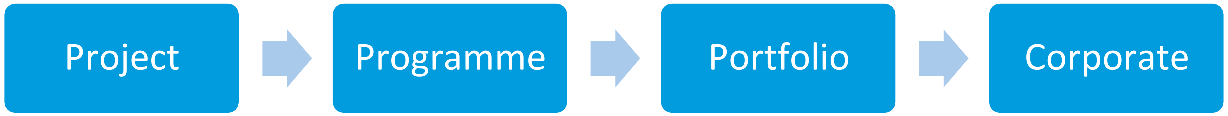
1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to sample test, or complete full population testing using data analytics tools.

Why we completed this audit

An audit of risk management was undertaken as part of the approved 2020/21 internal audit plan to review the risk management in place to identify, monitor and manage risks threatening the achievement of the organisation’s objectives.

The Authority implemented a revised Risk Management Strategy in January 2020 which was developed by the Transport Programme Coordinator. The organisation is focusing on embedding this throughout the organisation, having implemented new levels of risk registers. The Strategy consists of four levels of risk register, which are shown within the diagram below. The primary organisational risk register is the Corporate Risk Register, which is presented to the Authority’s Audit and Governance Committee on a regular basis. Sitting beneath the Corporate Risk Register is the Portfolio Risk Register that holds risks on a portfolio level. There are four portfolios within the Authority; Housing, Business and Skills, Corporate Services and Transport and Strategy, however Transport and Strategy manage their risks on Programme Risk Registers. The Programme Risk Registers contain risks that have common attributes across multiple projects and that may affect the delivery of such projects. Project Risk Registers are specific to each individual project. At the time of our audit, the Authority had 37 active projects.



Risks are categorised as Red, Amber or Green risks.

- Green – residual score between 1 and 4 - Can be ‘Accepted’ and may not require action plans.
- Amber – residual score between 5 and 10 - Require action plans and / or to be closely monitored as appropriate.
- Red – residual score between 15 and 25 - Require action plans and / or to be closely monitored as appropriate.

Conclusion

Our review found that the organisation was making some good progress towards embedding its risk management processes. This has primarily been driven by the introduction of the Risk Management Strategy and the development of various levels of risk registers, some of which are still under development. The control framework does, however, require strengthening to ensure that all areas of risk can be consistently managed, reviewed and reported.

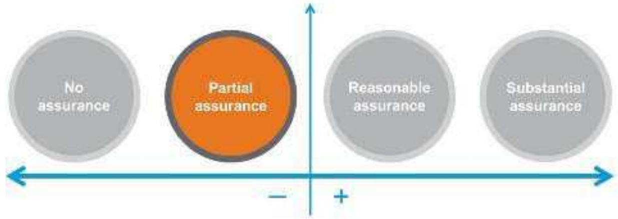
We noted that the Authority was yet to undertake detailed risk management training, specifically in ensuring risks are clear and mitigation plans and actions are specific, measurable, achievable, realistic and time relevant (SMART). This was reflected through our review in that we noted two risk registers were yet to be fully completed and that the remaining risk registers we reviewed were not consistent in design with specific risks and SMART mitigation plans and actions. In addition, we noted the Authority does not capture evidence of the review and scrutiny of the Corporate Risk Register at an Executive level and is yet to implement a reporting framework for risk registers below the Corporate level. We further noted that risk escalation was done at the discretion of risk owners and therefore could be subjective and inconsistent.

We also found that minimum frequencies for the review of risks have not been formally documented and noted that as the organisation takes positive steps towards its compliance with the new risk management strategy and processes, it would be equally important to link assurances to the individual risks to provide insight into the management of organisational risk.

Whilst we note some improvements and progress during the year, it is evident that further work is still required to ensure a fully robust and effective risk management framework is in place across the Authority. The actions identified during our review will further embed the organisations risk management culture and controls which are planned to be driven by the Corporate Management Team. We propose to undertake a follow up review at the end of the financial year to determine progress made in implementing the agreed actions, which will inform our year end opinion.

Internal audit opinion:

Taking account of the issues identified, the Board can take partial assurance that the controls upon which the organisation relies to manage this area are suitably designed and consistently applied. Action is needed to strengthen the control framework to ensure this area is effectively managed.



Key findings

Throughout our review we identified the following weaknesses:

Guidance and Training

We reviewed the Risk Management Strategy and noted that although information on mitigation and risk controls were included, the Strategy did not include guidance on ensuring mitigations and controls were SMART.

We also reviewed the All Team Meeting Risk Workshop presentation dated July 2020 and noted that the workshop provided an overview of recording and reviewing risks, however, it did not provide guidance on how risks and mitigation plans and actions should be recorded in the register and that they should be SMART. This aligns with our findings in management action four in section two of this report. **(Medium)**

Risk Register Completeness

We reviewed the Corporate Services Portfolio Risk Register and Strategy Programme Risk Register and noted that both registers were incomplete. We were advised that the organisation was aware of this and was working to ensure that these risk registers are fully populated.

There is a risk that without ensuring portfolio risk registers are complete, with risks including mitigation plans and actions and scored appropriately, that the Portfolio does not have sufficient oversight of its risks and therefore cannot manage them effectively. **(Medium)**

Risk Register Content

We noted through our sample testing of the four risk register levels, exceptions that could be categorised into key themes. This included that risk causes and effects were not consistently specific in defining what has caused the risk, and subsequently how the risk materialising would affect the Authority. There is a greater chance of the risk materialising if the cause and effect of risks are not clearly defined.

We also noted that mitigation plans designed to define the current controls in place did not always clearly demonstrate how the controls in place have mitigated the risk down to the residual risk score. For example, for Risk 7 on the Corporate Risk Register relating to Brexit, it was not clear how the controls in place reduced the impact of Brexit on the organisation's Growth Ambition Programme from an inherent risk score of 16 (4 x 4 – red risk) with 'likely' likelihood and 'major' impact to a residual risk score of four (2 x 2 – green risk) with 'unlikely' likelihood and 'marginal' impact. We also noted that as per the Risk Management Strategy, this risk could be 'Accepted' and may not require action plans, which does not appear to be the appropriate treatment for such a risk.

We also found through review of the varying risk registers that mitigation actions to define the future plans required to mitigate the risks were not consistently applied and were not documented in a SMART format. We also found that progress against future actions was not being clearly and consistently recorded.

There is a risk that if mitigation plans do not clearly define how controls currently in place are managing the risk, the organisation may not be fully assured that the risk is being effectively managed and that the residual risk scoring is representative of the status of the risk.
If SMART mitigation actions are not clearly defined, there is a risk of slippage against actions required to manage the risk which may lead to a greater chance of the risk materialising.

Finally, we noted that four of the five Project Risk Registers reviewed did not record inherent risk scores. We noted that just one risk score was used throughout each of the four Project Risk Registers we sampled. There is a risk that the effectiveness of controls in reducing risks from inherent scores to residual scores is not demonstrated at a project level. This may lead to difficulty in determining whether risk scoring is accurate which could lead to a greater chance of the right actions and controls being put in place and ultimately in risks materialising.
(Medium)

Risk Review Frequency and Risk Appetite

Risk Review Frequency

We noted through review of the Risk Management Strategy that it did not set out the minimum risk review frequency for each type of risk. We did note the positive observation that the risk matrix had been designed so that a risk of 'monumental' impact (1), even with a 'rare' (1) likelihood, was classed as an amber risk, with the requirement for the risk to have action plans developed and to be closely monitored as appropriate. Without, however, the minimum frequency for risk review being set and formally documented, there is a greater chance of risks materialising due to regular reviews not taking place.

Risk Appetite

We noted that the Relationship between Risk and Change Control document was in draft and not in use at the time of the audit but confirmed through review of papers for the 27 November 2020 Audit and Governance Committee that the paper requested the Committee recommend the adoption of the proposed document to the Combined Authority.

We noted that the proposed process for setting the risk appetite was focussed on projects and business cases and used financial cost as its sole measure to set the risk appetite (in monetary value). We noted that without a wider concept and definition of the organisation's risk appetite including all types of risk, it may be difficult for the organisation to understand where a risk on the corporate risk register, for example, has exceeded the risk appetite in areas such as reputational, compliance or regulatory risk.

The widening of this concept of risk appetite will ensure that all types of risks can be assessed against the risk appetite, not solely those relating to business cases and projects. Following this, the mechanism for review of risks to ensure that they remain within the organisation’s risk appetite should also be documented. Where these areas relating to risk appetite are not documented and in operation, there may be a greater chance of risks materialising. **(Medium)**

Reporting Framework

Corporate level

We reviewed the July and draft October 2020 Audit and Governance Committee meeting minutes and confirmed that the Corporate Risk Register had been received and reviewed. We did, however, note that the Risk Management Strategy stated that the Audit and Governance Committee has the responsibility of reviewing the Corporate Risk Register, together with progress of mitigating actions and assurances. We noted that as progress of mitigating actions and assurances are not documented in the Corporate Risk Register, the organisation is unable to clearly evidence how the Committee has fulfilled this particular duty.

We also noted through review of the Risk Management Strategy that the Combined Authority Management Team is responsible for review and scrutiny of the Corporate Risk Register at an Executive level. However, we were informed by the Authority that the Management Team do not have a Terms of Reference, neither are they supported by minutes or action logs and therefore we were unable to confirm that the forum’s risk management responsibilities had been formally defined and that the appropriate level of scrutiny at meetings was taking place.

Portfolio, Programme and Project level

We further noted through review of the Risk Management Strategy that the Authority has not developed a reporting framework for Portfolio, Programme and Project risk registers to ensure adequate scrutiny and oversight of risks at all levels throughout the organisation. We were advised that the focus is on ensuring risk registers are fully complete and accurate, after which a clear reporting framework will be implemented and documented. Where a regular framework for the reporting, review and challenge of risks is not operating and formally documented, there is a greater chance of risks materialising. **(Medium)**

Assurances

From review of the organisation’s various risk registers and through discussion with the Transport Programme Coordinator, we noted that the organisation does not currently link assurances to its risks (controls) to identify if their mitigation controls are working as intended. This can be used to further inform the risk scoring and understand if the risk is closer to materialising.

Without the organisation linking its risks to assurances the organisation cannot be assured that the mitigating controls are operating as intended and could result in risk materialising due a control not operating as intended. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

Risk Management Strategy

We reviewed the Risk Management Strategy and confirmed that it clearly defined the roles and responsibilities of key staff groups i.e. corporate risk owners, portfolio directors, programme and project risk owners and key governance forums eg Board, Audit and Governance Committee and Project Management Office stakeholders. We confirmed through review of the January 2020 Board meeting minutes that the Strategy was approved with further review required every three years. We confirmed through review of email correspondence that the Strategy was shared with all staff on 3 February after its approval and that the Strategy was available to staff through the Shared Drive.

Risk Management Methodology

We reviewed the Risk Management Strategy and confirmed that it defined the organisation's risk management methodology which consisted of a five-stage risk management cycle. We noted that compliance with the Strategy is monitored through the cycle and that it is the responsibility of the risk owner to ensure compliance. We noted through review of the Risk Management Strategy that risk identification processes had been noted including gap analysis brainstorming and various organisational analysis techniques such as SWOT and PESTLE. We also noted that the methodology defined how risks are assessed using a 5x5 likelihood and impact matrix and RAG rating to determine the severity of the risk.

Director Risk Workshop

We reviewed the Director Risk Workshop presentation, delivered at the end of 2019 and noted that it provided an overview of the new Strategy contents including risk scoring, risk register structure, roles and responsibilities and escalation. We were informed by the Transport Programme Coordinator that the Workshop was delivered to all members of the Combined Authority Management Team.

We have also agreed one 'low' priority management action, detailed further in section two, below.

Risk Management Questionnaire

We circulated a questionnaire to 45 individuals within the Authority to determine their thoughts on how risk management is being embedded. We received 29 responses, with 16 respondents being risk owners. Our findings are as follows.

We noted that our findings were largely positive with the exception of questions six and ten relating to risk management being well embedded within the organisation and risks being de-escalated when control have been applied.

With regards to question ten, 'risks are promptly de-escalated when controls have been applied' 12 respondents (41 per cent) responded that they didn't know and three (10 per cent) disagreed. This supports the management action agreed in this review to ensure that there is a consistent approach for risk escalation and de-escalation across the organisation.

With regards to question six, 'risk management is well embedded in the organisation' we noted that 14 respondents (48 per cent) either didn't know or disagreed with the statement. We appreciate that the organisation's risk management framework is relatively new, with the updated strategy being implemented in January 2020. We have agreed actions regarding the completeness of risk registers, implementing a review and reporting framework and ensuring further training is conducted to assist in ensuring risk management is well embedded in the organisation.

In addition to the above questions, we included a free-text response to allow respondents to elaborate on their findings. A summary of the responses can be found at Appendix B.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

1. Training				
Control	The Authority delivered a Risk Workshop based on the agreed Risk Management Strategy to an all team meeting in July 2020 to provide training on the new Strategy to staff. Whilst this covered risk management principles, training on the recording and management of risks in the risk register has not been delivered.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We reviewed the Risk Management Strategy and noted that although information on mitigation and risk controls were included, the Strategy did not include guidance on ensuring mitigations and controls were SMART. We also reviewed the All Team Meeting Risk Workshop presentation dated July 2020 and noted that the workshop provided an overview of the recording and review of risks, however, it did not provide guidance on how risks and mitigation plans and actions should be recorded in the register and that they should be SMART. This links in with our findings in management action four below. In addition, our risk management questionnaire identified through use of free-text comments that although training had taken place within the Authority, there was scope for further training to be carried out particularly around day-to-day management of risk. We noted that when respondents were asked if 'I have had sufficient training with respect to my responsibilities for risk management' a third of respondents (10 out of 29) either didn't know or disagreed with the statement. There is a risk that without adequate guidance and training in place for risk owners, risks and mitigations are not captured and monitored as required, resulting in a greater chance of risks materialising.			
Management Action 1	We will ensure that there is appropriate training and guidance in place for risk and action owners to ensure risks and mitigation plans and actions are effectively identified, recorded and managed.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

2. Frequency of Risk Review and Risk Appetite

Control	Risks are categorised as Red, Amber or Green risks by the Combined Authority. • Green – residual score between 1 and 4 - Can be 'Accepted' and may not require action plans. • Amber – residual score between 5 and 10 - Require action plans and / or to be closely monitored as appropriate. • Red – residual score between 15 and 25 - Require action plans and / or to be closely monitored as appropriate. The Risk Management Strategy does not set out the minimum frequency with which each type of risk (Red, Amber and Green) should be reviewed. The Strategy also does not currently document the organisation's risk appetite, although a separate Draft Relationship Between Risk and Chance Control Document is currently being produced to document this.	**Assessment:** **Design** × **Compliance** N/A
Findings / Implications	<u>Minimum Risk Review Frequency</u> We noted through review of the Risk Management Strategy that it did not set out the minimum risk review frequency for each type of risk. We did note the positive observation that the risk matrix had been designed so that a risk of 'monumental' impact (1), even with a 'rare' (1) likelihood, was classed as an amber risk, with the requirement for the risk to have action plans developed and to be closely monitored as appropriate. This is in line with best practice. Without, however, the minimum frequency for risk review being set and formally documented, there is a greater chance of risks materialising due to regular reviews not taking place. <u>Risk Appetite</u> We noted that the Relationship between Risk and Change Control document was in draft and not in use at the time of the audit but confirmed through review of papers for the 27 November 2020 Audit and Governance Committee that the paper requested the Committee recommend the adoption of the proposed document to the Combined Authority. Review of the draft document found that, with regards to risk appetite and tolerance, the document refers to each risk having a qualitative assessment of its likelihood and impact (as per the relevant risk scores recorded in the risk registers). It further explains that the organisation is moving towards an approach of documenting the risk treatment (accept, avoid, transfer or reduce) for each documented risk. Following the qualitative assessment and documenting of the risk treatment, the risk owner is responsible for providing an approximate financial value of each risk. As each risk is quantified throughout the lifetime of the project, the approximate financial implication of the project is calculated and may change. This is then to be assessed against the organisation's financial risk appetite. We noted that the process for setting the risk appetite was focussed on projects and business cases and used financial cost as its sole measure to set the risk appetite (in monetary value). We noted that without a wider concept and definition of the organisation's risk	

2. Frequency of Risk Review and Risk Appetite				
	appetite including all types of risk, it may be difficult for the organisation to understand where a risk on the corporate risk register, for example, has exceeded the risk appetite in areas such as reputational, compliance or regulatory risk. The widening of this concept of risk appetite will ensure that all types of risks can be assessed against the risk appetite, not solely those relating to business cases and projects. The mechanism for review of risks to ensure that they remain within the organisation's risk appetite should also be documented. Where these areas relating to risk appetite are not documented and in operation, there may be a greater chance of risks materialising.			
Management Action 2	The Risk Management Strategy will be updated to include the minimum review frequency for each type of risk (Red, Amber and Green). This should include sufficient (at least annual) oversight over risks rated as monumental and rare. The organisation's concept of risk appetite will also be widened to include various types of risks apart from financial risk relating to business cases and projects. This risk appetite will be clearly documented in the Relationship between Risk and Change Control document along with the mechanism to ensure that risks are regularly reviewed to ensure they remain within the organisation's risk appetite.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

3. Incomplete Risk Registers			
Control	The Authority has four levels of risk registers from the Corporate Risk Register to Project Risk Registers. The Corporate Services Portfolio Risk Register and Strategy Programme Risk Register are yet to be fully completed.	**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We reviewed the Corporate Services Portfolio Risk Register and noted that the register was incomplete. We noted that for the Corporate Services Register, of the 48 risks identified, 12 had not been provided with an inherent risk score and 13 were yet to be provided with a complete mitigation plan, actions and owners as well as a residual risk score. We reviewed the Strategy Programme Risk Register and noted that it was yet to be fully completed, with three of the 24 risks listed awaiting inherent risk scores. There is a risk that without ensuring risk registers are complete, with risks scored appropriately and mitigation plans documented, that the portfolio does not have oversight of all of its risks and therefore cannot manage them effectively.		

3. Incomplete Risk Registers				
Management Action 3	We will ensure that all incomplete risk registers are fully completed, inclusive of inherent and residual risk scores, mitigations and owners.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

4. Risk Register Content		
Control	The Authority has in place a Corporate Risk Register that defines risks identified at the organisational level. Beneath the Corporate Risk Register are the Portfolio, Programme and Project Risk Registers. For each register, each risk is allocated an ID, cause, event and effect. The Register also gives the risk an inherent score based on the impact and likelihood of the risk, with a mitigating plan, mitigating action and action owner. Risk owners are also assigned to each risk. The risk is subsequently scored a residual risk score. Mitigating actions are not assigned timeframes for completion.	**Assessment:** **Design** × **Compliance** N/A
Findings / Implications	We selected a sample of 10 risks from the Corporate Risk Register (Corporate level), 10 risks across the Corporate Services and Housing Portfolio Risk Registers (Portfolio level), 10 risks across the Transport Strategy and Delivery Programme Risk Registers (Programme level), and 15 risks across five Project Risk Registers (Project level). We identified through our review of the four levels of risk register that exceptions could be categorised into key themes which we have listed below. <u>Specific Risk Cause and Effect</u> We noted through our review that the risk cause and effects were not consistently specific in defining what it is that caused the risk and subsequently how the risk materialising would affect the Authority. For example, we noted that for Delivery Programme Risk Register ID 11, Partner Delivery Capacity, the risk effect was noted as ‘reduced teams due to critical delivery redeployment’ which does not provide detail as to the specific effect of the risk on the Authority. There is a risk that if risks and risk effects are not clearly defined, there is a greater chance of the risk materialising. <u>Mitigation Plans and Actions</u> We noted through our review, that the use of mitigation plans designed to define the current controls in place and mitigation actions to define the future plans required to mitigate the risks were not consistently applied. We particularly noted that at Programme level, eight of the 10 risks were utilising the mitigation plans column as future mitigating actions and current controls in place were not featured on the register.	

4. Risk Register Content

We also noted that mitigation plans detailing the current controls in place did not always clearly demonstrate how the controls in place have mitigated the risk down to the residual risk score. For example, for Risk 7 on the Corporate Risk Register relating to Brexit, it was not clear how the controls in place reduced the impact of Brexit on the organisation's Growth Ambition Programme from an inherent risk score of 16 (4 x 4 – red risk) with 'likely' likelihood and 'major' impact to a residual risk score of four (2 x 2 – green risk) with 'unlikely' likelihood and 'marginal' impact. We also noted that as per the Risk Management Strategy, this risk could be 'Accepted' and may not require action plans, which may not be the appropriate treatment for such a risk.

We also found through review of the varying risk registers that mitigation actions to define the future plans required to mitigate the risks were not consistently documented in SMART format. Whilst we noted that at Project level, nine of our sample of 15 risks had identified a mitigation action due date, in all cases this was out of date with little evidence of review maintained. We also found that progress against future actions was not being clearly and consistently recorded.

The organisation cannot be assured that the risk is being effectively mitigated and there is also a risk of actions to develop further controls to mitigate the risk not taking place in a timely manner. This may lead to a greater chance of the organisation's risks materialising.

<u>Risk Scores</u>

We noted that four of the five Project risk registers reviewed did not contain inherent and residual risk scores, they only contained the inherent risk score. There is a risk that the effectiveness of controls in reducing risks from inherent scores to residual risk scores is not demonstrated at project level. This may lead to difficulty in determining whether risk scoring is accurate which could lead to a greater chance of risks materialising.

<u>Training</u>

Supporting our findings, we noted that whilst the requirement for SMART actions was included within the Corporate Risk Register 'Example Risk Register' tab, we did note that the format of the Example Risk Register was not consistent to that used in the Corporate Risk Register, so detailed guidance was not in place for both the mitigation plan and mitigation action columns. There is therefore a risk that without adequate guidance and training in place for risk owners; risks and mitigations are not captured as required, resulting in a greater chance of the risk materialising. We have agreed a management action relating to training in management action 1 of this report.

Management Action 4	We will review the current risk registers in place to ensure that all risk events, cause and effects are clearly documented with inherent and residual risk scores. Risk scoring will be reviewed in the context of current controls and future plans to ensure they are an accurate representation of each risk. In addition, we will ensure that mitigation plans and actions are identified, recorded and are SMART. Progress against action plans will be clearly recorded and monitored.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

5. Risk Escalation Process				
Control	The Strategy identifies a number of risk identification processes including risk gap analysis and workshops and brainstorming. As reporting is not currently taking place at an operational level, there is no evidence of new and emerging risks being considered. The Strategy documents what the escalation process is between project, programme, portfolio and corporate risk registers. The responsibility lies with the risk owner to promote the risk to the next level. The Strategy does not define the process for the de-escalation of risks.	**Assessment:** **Design** × **Compliance** N/A		
Findings / Implications	We noted through review of the Risk Management Strategy that risk identification processes had been noted including gap analysis brainstorming and various organisational analysis techniques such as SWOT and PESTLE. However, we noted through our review that, as reporting at an operational level is not documented and recorded throughout the Authority, we were not able to confirm that new and emerging risks are being considered. We also noted through review of the Strategy, that escalation of risks is at the discretion of the risk and action owners. We noted through our review of the Portfolio, Programme and Project risk registers that a column was included noting if escalation was required. Two risks on the Housing Portfolio risk registers were marked as requiring escalation, however, they were not present on the Corporate Risk Register. We were advised that these had been recently marked for escalation and were planned to be presented at the November 2020 meeting of the Audit and Governance Committee to consider whether escalation to the Corporate Risk Register was required. We further noted through review of the Risk Management Strategy that there was no defined process for the de-escalation of risks once controls had been applied. Supporting our finding, we noted in our risk management questionnaire that of 29 respondents, 12 responded with ‘don’t know’ and three with ‘disagree’ when asked if ‘risks are promptly de-escalated when controls have been applied’. We also corroborated our findings with the results from the risk management questionnaire and noted that eight of 29 respondents either disagreed with or did not know if roles and responsibilities for risk management had been well defined. There is a risk that if escalation and de-escalation of risks is solely at the discretion of risk and action owners, application of the escalation model may be subjective and inconsistently applied. The Authority should consider, in addition to the existing control of risk owner judgement, the use of risk scoring criteria to provide a consistent level at which risks are considered for escalation and de-escalation through the risk register structure.			
Management Action 5	We will consider, in addition to the existing control of risk owner judgement, the use of set levels of risk scores to identify risks to be considered for escalation and de-escalation.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Low

6. Scrutiny of Risk Registers				
Control	Strategic Risks in the Corporate Risk Register should be reviewed monthly by the Combined Authority Management Team. The Corporate Risk Register should also be reviewed on a quarterly basis by the Audit and Governance Committee. The organisation has not developed a reporting framework for Portfolio, Programme and Project risk registers to ensure adequate scrutiny and oversight of risks at all levels throughout the organisation.	**Assessment:** **Design** × **Compliance** N/A		
Findings / Implications	**<u>Monitoring arrangement for the Corporate Risk Register</u>** <u>Audit and Governance Committee</u> We reviewed the July and draft October 2020 Audit and Governance Committee papers and confirmed that the Corporate Risk Register had been received at each meeting. We noted that risks were presented in order of RAG and that one risk regarding climate change was requested by members to be included on the register. However, we noted that the Risk Management Strategy stated that the Committee has the responsibility of reviewing the Corporate Risk Register together with progress of mitigating actions and assurances. We noted that as progress with mitigating actions and assurances are not documented, the Committee has not been able to fulfil its duties with regards to risk management. <u>Combined Authority Management Team</u> We noted through review of the Risk Management Strategy that the Combined Authority Management Team is responsible for review and scrutiny of the Corporate Risk Register at an Executive level. However, we were informed by the Authority that the Management Team do not have a Terms of Reference, neither are they supported by minutes or action logs and therefore we were unable to confirm that the forums risk management responsibilities had been formally defined and that the appropriate level of scrutiny at meetings was taking place. **<u>Monitoring arrangements for Portfolio, Programme and Project Registers</u>** We noted that the Authority has not developed a fully operating reporting framework for Portfolio, Programme and Project risk registers to ensure adequate scrutiny and oversight of risks at all levels throughout the organisation. We were advised that the focus is on ensuring risk registers are fully complete and accurate, after which a clear reporting framework will be implemented and documented. Where a regular framework for the reporting, review and challenge of risks is not operating and formally documented, there is a greater chance of risks materialising			
Management Action 6	We will evidence scrutiny of the Corporate Risk Register at executive level. This could be in the form of minutes, action notes or progress notes retained on the risk register.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

6. Scrutiny of Risk Registers				
Management Action 7	Once the risk registers have been completed at all levels, we will ensure that an appropriate risk monitoring framework is formally documented and implemented. This will include Terms of References for governance forums that have risk management responsibilities.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

7. Assurances		
Control	The organisation does not link assurances to its risks (controls) to identify if their mitigation controls are working as intended. Linking assurances to risks and their associated controls would support the organisation in determining if the controls are operating effectively and helping to manage the risk(s).	**Assessment:** **Design** × **Compliance** N/A
Findings / Implications	From review of the organisation's various risk registers and through discussion with the Transport Programme Coordinator, we noted that the organisation does not currently link assurances to risks (controls) to identify if their mitigation controls are working as intended. This can be used to inform the risk scoring and understand if the risk is closer to materialising. For example, for a risk relating to the achievement of the financial budget, an associated control may be that financial reporting is taking place at the Finance Committee each period. The assurance for this control would be the outcome of the last period of reporting. If the last report shows that the income and expenditure is in line with the budget, this indicates positive assurance and may indicate that there is a reduced chance of the risk materialising, which may impact the residual risk score. Conversely, if the financial performance is significantly over budget, this indicates negative assurance for the financial reporting control and may indicate the need for the risk score to be increased and/or additional controls or actions to be introduced. Without the organisation linking its risks to assurances the organisation cannot be assured that the mitigating controls are operating as intended and could result in risk materialising due a control not operating as intended.	

Management Action 8	Once the organisation has fully embedded its risk management, reporting and review arrangements, it will consider utilising assurances to assist in the review and accurate scoring of risks.	**Responsible Owner:** Corporate Management Team, to be led by CFO and MO	**Date:** 31 March 2021	**Priority:** Medium

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
Risk Management	7	(9)	0	(9)	1	7	0
Total					**1**	**7**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: QUESTIONNAIRE RESULTS

We circulated a questionnaire to 45 individuals within the Authority to determine their thoughts on how risk management is being embedded and we received 29 responses. 12 respondents provided comments to their answers and we have provided a summary of the responses below.

Are there any other comments you would like to make about the risk management culture at your organisation?
Positive Comments • The risk culture has continued to evolve and develop over the last 12 months and is continuing to do so. • Improvement in risk management can be seen across the Authority. • Senior management provide good leadership in terms of risk management and actively encourage risks to be raised and discussed. • The CPCA Risk Management Strategy and 10 Point Guide are useful.
Potential Areas for Improvement • Risk register training has been received, however more training on how risks are expected to be managed on a day to day basis would be appreciated. • The Corporate Risk Register is discussed, however there could be further risk discussions at a team level to ensure wider engagement. • Risk management is not yet a routine across the Authority. • Departmental risks are not communicated across departments and so a risk management/crisis communications plan cannot be implemented. • Risk management processes are in place however using them well will be the next steps.

APPENDIX C: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the area under review
To review the effectiveness of risk management and assurance arrangements in place to identify, monitor and manage risks threatening the achievement of the organisation's objectives.

1.1 Scope of the review

The following areas will be considered as part of the review:

- A Risk Management Strategy has been developed by the organisation and agreed by the Board;
- The Risk Management Strategy clearly defines the Authorities risk appetite, methodology and scoring criteria as well as the processes in place to ensure that they are complied with;
- The provision of risk management training to all relevant staff members with risk management responsibilities;
- The presence and completion of project, programme, portfolio and corporate risk registers (including controls, mitigations and identified actions in risk registers) which are clear, specific, adequately worded and unambiguous. We will assess the quality of information within the registers
- The cause and effect of each risk is clearly documented within the risk registers. Each risk has an inherent and current risk score;
- Responsibility for each risk has been assigned to an accountable person with the appropriate delegated authority to manage the risk;
- Processes are in place to identify and assess risks at the operational level and escalate them to the appropriate level;
- Processes have been established to ensure that new and emerging risks are shared at an operational and strategic level;
- Arrangements for the reporting, scrutiny and discussion of risk registers at each level; and
- Review of how assurances are utilised to confirm that controls are effectively operating to mitigate key risks.

We will utilise a risk management culture questionnaire as part of our audit approach to gauge the views of staff throughout the organisation on the effectiveness of risk management arrangements in place.

The following limitations apply to the scope of our work:

- The scope of this review is limited to those areas examined and reported upon in the areas for consideration in the context of the objectives set out for this review above.
- This review will not comment on whether individual risks are appropriately managed, or whether the organisation has identified all of the risks and opportunities facing it.
- We will not conduct any testing to verify the outcome of any assurances received.
- We do not endorse a particular means of risk management.
- It remains the responsibility of senior management to agree and manage information needs and to determine what works most effectively for the organisation.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- Our testing will be compliance based and sample testing only.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Debrief held	3 December 2020	**Internal audit Contacts**	**Daniel Harris, Head of Internal Audit** Daniel.Harris@rsmuk.com 07792 948767 **Jay Desai, Manager** Jay.Desai@rsmuk.com 07436 268278
Draft report issued	11 December 2020		
Responses received	15 January 2021		
Final report issued	15 January 2021	**Client sponsor**	Robert Parkin, Chief Legal Officer (Monitoring Officer)
		Distribution	Robert Parkin, Chief Legal Officer (Monitoring Officer) Dermot Pearson, Solicitor Francesca Houston, Transport Programme Coordinator Susan Hall, Governance Assistant Anne Gardiner, Scrutiny Officer