BEDFORDSHIRE FIRE & RESCUE AUTHORITY

Risk Management

FINAL

Internal audit report: 5.17/18

25 April 2018

RSM

CONTENTS

Debrief held	16 February 2018	**Internal audit team**	Daniel Harris - Head of Internal Audit Louise Davies - Client Manager Farjad Shah – Senior Auditor
Draft report issued	28 February 2018		
Responses received	25 April 2018		
Final report issued	25 April 2018	**Client sponsor**	Darren Cook - Group Commander
		Distribution	Darren Cook, Group Commander

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Risk Management has been undertaken at the Authority to provide assurance over the effectiveness of the risk management framework and the supporting governance processes to ensure risks to the achievement of the Authority's objectives are identified and managed effectively.

Individual risks are recorded on and managed using the Abriska system. The system retains an audit trail of previous changes to individual risks and also provides comparative data such as the number of risks on a month by month basis along with how risk scores have changed over time. At the time of review, there were a total of 38 risks on the Corporate Risk Register.

As per the Service Assurance Framework, the Corporate Management Team is responsible for the risk management programme with the aid of the Head of Organisational Assurance.

Three Policy and Challenge Groups are in place with responsibility for reviewing risks on a quarterly basis, as follows:

- Corporate Services;
- Human Resources; and
- Service Delivery.

The Audit and Standards Committee receive a Corporate Risk Register Report on a quarterly basis detailing changes to all risks on the Corporate Risk Register. The Corporate Management Team (CMT) and Service Delivery Leadership Team (SDLT) are also provided with an update on the Corporate Risk Register on a monthly and quarterly basis, respectively.

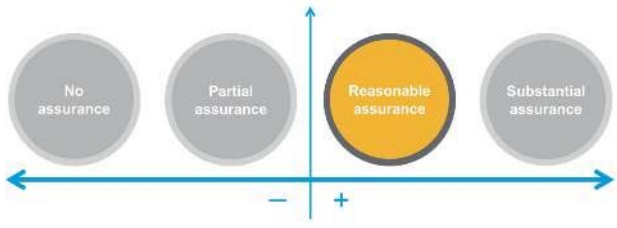
1.2 Conclusion

During our review, we found that the Corporate Risk Register (CRR) was largely complete (with only one action missing a due date and owner), with all risks being described using the cause-effect model. We also confirmed that there was a consistent process for the reporting of new risks to the Corporate Management Team (CMT) for review.

We noted issues, however, with the format of the CRR (it did not detail controls, assurances or gaps in controls and assurances), the scoring of risks (scoring was not undertaken using the correct rationale) and scrutiny of risk scores.

Further areas for improvement were found with respect to the Service Assurance Framework, risk management training and the Terms of References (ToRs) of various forums.

Internal audit opinion:
Taking account of the issues identified, the Authority can take reasonable assurance that the controls in place to manage this area are suitably designed and consistently applied. However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified area(s).



1.3 Key findings

The key findings from this review are as follows:

Business Continuity Strategy

The Service is in the process of drafting a Business Continuity Strategy which sets out, in addition to business continuity related objectives, the link between risk management and business continuity. Through review of the Draft Business Continuity Strategy, we confirmed that a section had been included detailing the relationship between business continuity and risk management, and that various references to risk had been included throughout the document, demonstrating appropriate alignment to risk management.

Corporate Risk Register

Through review of the Corporate Risk Register, we noted that there was a total of 38 risks. In all cases, we confirmed that risks had been described using the cause-effect model and that a risk owner had been assigned against all risks.

We also confirmed that all risks were assigned an inherent and residual risk score using the scoring matrix in line with the Service Assurance Framework, with the total risk score being correctly calculated in all instances.

Risk Management Responsibility and System Training

We confirmed through review of the Service Assurance Framework that responsibility had been clearly assigned for the Service's risk management programme. We also confirmed during our review that operationally, the Corporate Risk Register was being maintained by the Head of Organisational Assurance, as identified in the Service Assurance Framework.

In terms of training with respect to the Abriska system, the Head of Organisational Assurance advised that they had not yet received system training since being assigned responsibility for the maintenance of Abriska. We were provided with email correspondence confirming that relevant system training had been booked in March 2018. We are therefore satisfied that this is receiving adequate management attention.

Corporate Management Team (CMT) and Service Delivery Leadership Team (SDLT)

Through review of the CMT meeting minutes for October 2017, November 2017 and January 2018 and the SDLT meeting minutes for July 2017, October 2017 and January 2018, we confirmed that the Corporate Risk Register was a regular agenda item being subject to review, with evidence of discussions taking place around key issues and changes/updates to risk We also confirmed that actions were being included in the action logs with responsible owners and due dates assigned, and followed up during subsequent meetings.

We noted, however, the following issues, resulting in three **'medium'** priority management actions:

Corporate Risk Register Format

A management action had been agreed during our 2016/17 Risk Management review in regard to the updating of the Corporate Risk Register with the following key columns: mitigating controls, assurances against controls and gaps in controls and assurances. We found, however, that the Corporate Risk Register had not been updated to reflect these requirements. This may result in risks not being effectively monitored and gaps not being identified in controls and assurances to mitigate against. **(Medium)**

Risk Scoring

As the Service do not document mitigating controls, we discussed the rationale behind the inherent and residual risk scoring with the Head of Organisational Assurance. We identified through our discussion that the Service assign the inherent risk score based on existing measures in place surrounding the risk, as opposed to a score based on the risk if no controls or other mitigating factors were in place. Moreover, we were advised that the residual risk score is according to mitigating actions being undertaken to address the risk, as opposed to existing controls in place.

Inappropriate risk scoring can lead to the ineffective prioritisation of risks, potentially leading to the Service not focusing their efforts on the most key risks. **(Medium)**

Corporate Risk Register Reports

The following management action had been agreed in the 2016/17 Risk Management review: "Where updates and assurances against risks are reported as part of Corporate Risk Register reports, risk scores will also be included for review as to whether they require revising."

Through review of the last two quarterly Corporate Risk Register Reports for the three Policy and Challenge Groups (between September 2017 and January 2018), we found that risk scores had not been included where updates were being provided for risks. Moreover, despite there being updates against 10 risks (positive assurances etc.), there had been no changes to risk scores.

Through review of the corresponding meeting minutes of the three Policy and Challenge Groups, we noted that there was a lack of evidence of discussion around the scoring of risk despite updates being provided against risks. This issue was also found to be the case during our review of risk reporting to the Audit and Standards Committee, with minimal discussion being noted around the scoring of risks.

If risk scores are not actively considered and revised in line with assurances and updates against risks, this can lead to risks not being prioritised and potentially managed appropriately. **(Medium)**

We have also agreed a further seven **'low'** priority management actions, included in the detailed findings in section 2.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
Risk Management	7	(10)	3	(10)	7	3	0
Total					**7**	**3**	**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.

1.5 Progress made with previous audit findings

Date of previous audit	Low	Medium	High
Number of actions agreed during previous audit	0	4	0
Number of actions implemented/ superseded	-	0	-
Actions not yet fully implemented:	-	4	-

As part of this review, little progress has been demonstrated in implementing the management actions agreed during out 2016/17 Risk Management review:

- Policies and procedures had not been updated to include all agreed areas;
- The format of the Corporate Risk Register had not been updated to include key areas, such as mitigating controls and assurances;
- A Risk Champion had been assigned to carry out reviews of the Corporate Risk Register, however this was not at an appropriate frequency; and
- Risk scores were still not being provided as part of Corporate Risk Register reports to key forums (Policy and Challenge Groups and the Audit and Standards Committee).

2 DETAILED 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 regulatory scrutiny/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, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

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.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Area: Risk Management								
1	The Service is in the process of drafting a Business Continuity Strategy which will set out, in addition to business continuity related objectives, the link between risk management and business continuity. The Service has also produced a Service Assurance Framework in February 2018 which triangulates business continuity, information security and risk management,	No	N/A	Through review of the Draft Business Continuity Strategy, we confirmed that a section had been included detailing the relationship between business continuity and risk management, and that various references to risk had been made throughout the document, demonstrating appropriate alignment to risk management. We reviewed the Service Assurance Framework (produced in February 2018) and confirmed that it included coverage of risk management, business continuity and information security.	Low	The Service Assurance Framework will be updated to ensure that there is clear linkage between business continuity, information security and risk management.	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	detailing roles and responsibilities, key objectives and monitoring arrangements.			We noted, however, that each area was referred to largely in isolation of other areas and there was little linkage between them. Without appropriate triangulation between business continuity, information security and risk management, the Service may not effectively benefit from the linkages between the arrangements of each area, such as the consideration of business continuity risks when carrying out a Business Impact Analysis (BIA).				
2	The Service have in place a Corporate Risk Management Policy which is supported by a Risk Management Service Order and details the various processes in place for risk management. These documents are out of date and have not been reviewed recently, as the documents are due to be replaced by the Service Assurance Framework.	Yes	No	A management action had been agreed during our 2016/17 Risk Management review with respect to updating of the Corporate Risk Management Policy and the Risk Management Service Order. We were advised by the Head of Organisational Assurance that the Policy and Service Order had not been updated as these are due to be replaced by the Service Assurance Framework, with relevant content being transferred as appropriate. We noted, however, that none of the above documents included key areas in respect of risk management, such as key risk definitions and the escalation process for risks identified by staff.	Low	When updating the Service Assurance Framework with content from the Corporate Risk Management Policy / Risk Management Service Order, the following additional information will be included: • Key risk definitions; • Minimum frequency for risk reviews by risk owners; • Escalation process for new/emerging risks identified by staff; and • Risk appetite statement (clearly identifying the level of	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				Moreover, although a section had been included on risk appetite, this was simply a 5x5 risk scoring matrix (impact and likelihood) and was not accompanied by any narrative or an indication as to what level of risk the Service were willing to tolerate in order to meet its objectives. The above can result in the overall ineffective management of risks, potentially leading to risks being realised. We have therefore agreed a new management action to address this issue.		risk the Service are willing to tolerate).		
3	The Abriska system is utilised for the documenting and subsequent management of Service risks. The system encompasses the Corporate Risk Register which details the following key information for each risk: • Risk owner; • Risk scores and treatment; • Risk review date; and • Actions. There are certain key fields, however, not included in the Corporate Risk Register, such as mitigating controls.	No	N/A	A management action had been agreed during our 2016/17 Risk Management review in regard to the updating of the Corporate Risk Register with key columns: • Mitigating controls; • Assurances against controls; and • Gaps in controls and assurances. We found, however, that the Corporate Risk Register had not been updated to reflect these requirements. This may result in risks not being effectively monitored and gaps not being identified in controls and assurances to mitigate against. We have therefore reiterated this management action.	Medium	The Corporate Risk Register will be updated to encompass the following fields: • Mitigating controls; • Assurances against controls; and • Gaps in controls / assurances.	31st August 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
4	Each of the Service's risks are described using the cause-effect model, and each risk is assigned an inherent risk score and residual risk score using a 5x5 matrix. The scoring method is detailed in the Service Assurance Framework.	Yes	No	Through review of the Corporate Risk Register, we noted that there were a total of 38 risks. In all cases, we confirmed that risks had been described using the cause-effect model. We also confirmed that all risks were assigned an inherent and residual risk score using the scoring matrix in line with the Service Assurance Framework, with the total risk score being correctly calculated in all instances. As the Service do not document mitigating controls, we discussed the rationale behind the inherent and residual risk scoring with the Head of Organisational Assurance. We identified through our discussion that the Service assign the inherent risk score based on existing measures in place surrounding the risk, as opposed to a score based on the risk if no controls or other mitigating factors were in place. Moreover, we were advised that the residual risk score is based according to mitigating actions being undertaken to address the risk, as opposed to existing controls in place. Inappropriate risk scoring can lead to the ineffective prioritisation of risks, potentially leading to the Service not focusing their efforts on the most key risks.	Medium	A review of all risk scores will be undertaken in line with the following definitions: • Inherent risk - the risk that an activity would pose if no controls or other mitigating factors were in place; and • Residual risk - the risk that remains after controls and other mitigating factors are taken into account	31st August 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				A management action has been agreed around including key risk definitions in the Service Assurance Framework, above.				
5	As per the Service Assurance Framework, the Corporate Management Team is responsible for the risk management programme with aid of the Head of Organisational Assurance. The Head of Organisational Assurance and the Service Assurance Manager are due to undertake training on the risk management system in March 2018. There is, however, no general risk management training for key staff.	No	N/A	We confirmed through review of the Service Assurance Framework that responsibility had been clearly assigned for the Service's risk management programme. We also confirmed during our review that operationally, the Corporate Risk Register was being maintained by the Head of Organisational Assurance, as identified in the Service Assurance Framework. In terms of training with respect to the Abriska system, the Head of Organisational Assurance advised that they had not yet received system training since being assigned responsibility for the maintenance of Abriska (the previously trained staff member had left the Service). We were provided with email correspondence confirming that relevant system training had been booked in March 2018 for both the Head of Organisational Assurance and the Service Assurance Manager (who will assist with the administration of the system). We are therefore satisfied that this is receiving adequate management attention. We were advised by the Head of Organisational Assurance, however, that	Low	The Service will introduce formal risk management training for risk owners and other key staff.	31st August 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				the Service does not have any formal training on general risk management for key staff. Without appropriate training, this can result in an inconsistent approach being undertaken to managing risk, or risks not being dealt with effectively, increasing the likelihood of risks being realised.				
6	Each Service risk is assigned a risk owner who is responsible for reviewing their risks. There is currently, however, no defined minimum frequency for risk reviews. Risk treatment actions are identified for each of the Service's corporate risks. This is to include details of the action along with the action owner and a proposed date for the completion of the action.	No	N/A	We reviewed the Corporate Risk Register and noted that for all 38 risks, a risk owner had been assigned. We found three instances, however, where risks had not been reviewed in line with their review dates as follows: • CRR27 was due for review on 8th February 2018; • CRR38 was due for review on 11th January 2018; and • CRR42 was due for review on 31st December 2017. We also noted that the Service had not defined a minimum frequency for risk review by risk owners and a management action has been agreed accordingly above. Without regular review of risks, this could lead to changes in the impact, likelihood or direction of the risk not being identified in a timely manner, thereby leading the risk not being managed appropriately.	Low	The Risk Champion review of the Corporate Risk Register will be undertaken on at least a quarterly basis to check key areas, including: • Whether actions have responsible owners and due dates assigned; • Whether actions are completed in line with their due date (or reasoning has been provided where they are overdue); and • Whether risks are reviewed in line with their review date. Where there is non-compliance with the above, this will be	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				In terms of actions, we noted that a total of 61 actions had been included against the Service's 38 risks. We noted an instance, however, where an action had not been assigned a responsible owner or due date. We also found five cases where actions were overdue (due dates were 1st June 2013, 1st January 2018, 1st February 2018 for three of the actions and 8th February 2018 for the remaining two actions. In four of these cases, we were provided with sufficient reasoning as to why the action had not been closed, for instance, the Service were awaiting release of meeting minutes before closing the action. This should therefore be detailed on the system to enable sufficient monitoring. In the remaining case (CRR8), the action did not have an update or justification as to why the action was overdue and whether progress was being made against it. Without sufficient monitoring of actions, this could lead to mitigating measures not being implemented against risks in a timely manner, increasing the likelihood of risks materialising. A management action had been agreed in the 2016/17 Risk Management review for the assigning of a risk champion to regularly review the Corporate Risk		escalated by the Risk Champion accordingly.		

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				Register and escalate any issues, such as overdue actions and risks. We were advised by the Head of Organisational Assurance that they were the Services 'Risk Champion' and that an overall review of the Corporate Risk Register is undertaken on a six monthly basis. In light of the issues above, the overall Corporate Risk Register review should be undertaken more frequently.				
7	New / emerging risks are to be reported to the Head of Organisational Assurance for initial screening prior to the risk being reported to the Corporate Management Team (CMT). The process, however, has not been defined in the Service's risk management policies/procedures.	No	N/A	We noted during our review that the process of escalating newly identified risks has not been defined in the Service's risk management policies/procedures, and a management action has been agreed above. Through review of the last three meeting minutes of the Corporate Management Team (CMT) for October 2017, November 2017 and January 2018, we noted that two new risks had been reported to the CMT relating to data protection and the SharePoint system. We found, however, that where new risks had been reported, this was not accompanied by the proposed scoring of the risk.	Low	Where new risks are reported to the Corporate Management Team (CMT), the proposed risk scoring will also be reported to ensure appropriate oversight prior to the risk being added to the Corporate Risk Register.	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				As a result, the priority of the risk may not receive sufficient oversight by the Committee to ensure it is appropriate.				
8	The Corporate Management Team (CMT) and Service Delivery Leadership Team (SDLT, formerly the Service Delivery Management Team) are provided with an update on the Corporate Risk Register on a monthly and quarterly basis, respectively. A Terms of Reference is in place to define the remit of both forums, however, these do not include key areas, such as accountability lines and quorum.	No	N/A	Through review of the Terms of Reference (ToR) for the Corporate Management Team (CMT), we noted that it had not been reviewed since April 2015, and did not state a next review date/review frequency. In terms of content, although the ToR covered responsibilities, membership and meeting frequency, key areas had not been included, such as: • Accountability lines; • Reporting requirements; and • Quorum. We also reviewed the Service Delivery Leadership Team (SDLT) (this was in draft format due to a change in name from 'Service Delivery Management Team') and noted similar issues, whereby the following had not been detailed: • Accountability lines; • Quorum; • Review frequency of the ToR; • Meeting arrangements; and • Membership. Without an appropriate Terms of Reference in place which is subject to regular review, this can result in a lack of accountability, an	Low	The Terms of References of the Corporate Management Team and Service Delivery Leadership Team will be updated to include the following information: • Accountability lines; • Reporting lines (both up and down); • Quorum; • Review frequency of the ToR; • Meeting arrangements; and • Membership.	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				unclear remit, or the ToR not being reflective of current practice. We confirmed that both ToRs encompassed risk management responsibilities.				
9a	Three Policy and Challenge Groups are in place as follows: • Corporate Services (CSPCG); • Human Resources (HRPCG); and • Service Delivery (SDPCG). A Terms of Reference (ToR) is in place detailing the remit of the Groups, although these do not include a next review date or review frequency.	No	N/A	Through review of the Terms of References (ToRs) for the Corporate Services, Human Resources and Service Delivery Policy and Challenge Groups, we confirmed that all were in a consistent format and had been last reviewed in the last 12 months. In terms of content, we confirmed all included key areas such as responsibilities, membership, quorum, reporting requirements and meeting arrangements. We found, however, that the ToRs did not include a next review date or review frequency. This can result in the ToRs not being subject to regular review to ensure they remain reflective of current practice and remit. The same issue was also noted for the ToR of the Audit and Standards Committee.	Low	The Terms of References of the Policy and Challenge Groups and the Audit and Standards Committee will be updated to include a next review date/review frequency.	31st May 2018	Karen Daniels – Service Assurance Manager
9b	A Corporate Risk Register Report is produced on a quarterly basis for review by each Policy and Challenge Group (for risks relating specifically to them) detailing	Yes	No	The following management action has been agreed in the 2016/17 Risk Management review: "Where updates and assurances against risks are reported as part of Corporate Risk Register reports,	Medium	Where updates and assurances against risks are reported as part of Corporate Risk Register reports to the Policy and Challenge Groups and	31st May 2018	Darren Cook – Head of Organisational Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	changes to risk ratings and any updates in relation to risks.			risk scores will also be included for review as to whether they require revising." Through review of the last two quarterly Corporate Risk Register Reports for the three Policy and Challenge Groups (between September 2017 and January 2018), we confirmed that they were in a consistent format, highlighting whether there were any changes to risk scores and providing updates against risks as relevant. We found, however, that risk scores had not been included where updates were being provided for risks. Moreover, despite there being updates against 10 risks (positive assurances etc.), there had been no changes to risk scores. An example of this is where an update had been provided against CRR15 (Corporate Services Corporate Risk Register Report for September 2017) whereby it was confirmed that mobile terminals had gone live which completes the resilience benefits required by the Home Office, however, there was no evidence of consideration of changes to risk scores. Through review of the corresponding meeting minutes of the three Policy and Challenge Groups, we confirmed that the Corporate Risk Register was being subject to regular review with discussion taking place around updated risks.		the Audit and Standards Committee, risk scores will also be included for review as to whether they require revising.		

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				We noted, however, that there was a lack of discussion around the scoring of risk despite updates being provided against risks (only one meeting discussed changes to risk scoring, the Human Resources Policy and Challenge Group meeting in September 2017). This could be partly due to the fact that risk scores are not included in the Corporate Risk Register reports. This issue was also found to be the case during our review of risk reporting to the Audit and Standards Committee, with minimal discussion being noted around the scoring of risks. If risk scores are not actively considered and revised in line with assurances and updates against risks, this can lead to risks not being prioritised appropriately.				

APPENDIX A: 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 areas:

Objectives of the area under review
To ensure that the risk management framework and processes are firmly embedded

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

The Authority has recently undertaken an internal review of their risk management systems and processes. This audit will seek to provide assurance that a robust risk management framework has been established and embedded throughout the organisation. This will include ensuring that:

- There is an agreed Risk Management, Information Security and Business Continuity Strategy which has been made available to all relevant staff. This includes clear risk assessment procedures and a defined escalation process. The Information Security and Business Continuity Strategy clearly link to the Risk Management arrangements;
- Appropriate corporate and operational risk registers have been established;
- Responsibility for the review and maintenance of the Risk Registers has been formally delegated to appropriate groups and/or persons. Training has been provided where necessary;
- Responsibility for each risk has been assigned to an accountable person with the appropriate delegated authority to manage the risk;
- The cause and effect of each risk is evident. Each risk has a pre- and post- mitigating control risk score. Risk scoring takes into account the characteristics of the risk;
- Controls and assurances are identified for each risk. Gaps in the control and assurance frameworks have been identified and appropriate action plans have been developed;
- Processes are in place to identify and assess new or emerging risks at a team / department / project level and then escalate them appropriately; and
- Processes have been established to ensure that common operational level risks are identified through a comparison of operational risk registers.

Limitations to the scope of the audit assignment:

- 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 will not include compliance with the Information Security and Business Continuity Strategy;
- We will not comment on the appropriateness of any risk scores given;
- We will not confirm that the actions taken and controls implemented will mitigate the risk from being realised;
- We do not endorse a particular means of risk management;

- It remains the responsibility of the Authority and senior management to agree and manage information needs and to determine what works most effectively for the organisation;
- All testing will be compliance based sample testing only; and
- Our work will not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Darren Cook – Head of Organisational Assurance
- Karen Daniels – Service Assurance Manager
- Lisa Langley – Corporate Management Team Secretary
- Alberdina Jenkins – Secretary to CMT

Benchmarking

We have included some comparative data to benchmark the number of management actions agreed, as shown in the table below. In the past year, we have undertaken a number of audits of a similar nature in the sector.

Level of assurance	Percentage of reviews	Results of the audit
Substantial assurance	25%	
Reasonable assurance	37.5%	X
Partial assurance	37.5%	
No assurance	0%	
Management actions	**Average number in similar audits**	**Number in this audit**
Total	5.63	10

FOR FURTHER INFORMATION CONTACT

Louise Davies, Client Manager

Louise.Davies@rsmuk.com

+44 (0)7720 508146