BEDFORDSHIRE FIRE & RESCUE AUTHORITY

Risk Management

FINAL

Internal audit report 4.18/19

13 February 2019

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.

CONTENTS

Debrief held	22 January 2018	**Internal audit team**	Daniel Harris - Head of Internal Audit Suzanne Rowlett - Senior Manager Satnam Parmar - Senior Auditor Jordan Williamson - Internal Auditor
Draft report issued	31 January 2019		
Revised draft report issued	13 February 2019		
Responses received	13 February 2019		
Final report issued	13 February 2019	**Client sponsor**	Andy Peckham - Head of Service Development and Organisational Assurance
		Distribution	Andy Peckham - Head of Service Development and Organisational Assurance

1 EXECUTIVE SUMMARY

1.1 Background

A review of Risk Management was undertaken at Bedfordshire Fire and Rescue Authority as part of the approved Internal Audit Plan for 2018/19. The objective of the review was to provide assurance over the effectiveness of the risk management framework in place.

As of January 2019, 39 risks had been recorded on the Corporate Risk Register. The Authority has in place a risk management system, Abriska, which is used to record risks, risk responses and actions which can be accessed by risk owners. Abriska details the full history of risks identified by the Corporate Management Team (CMT) which includes a breakdown of how risk scores, based upon the risk matrix, have evolved over time.

Three Policy and Challenge Groups are in place which are responsible for the review of risks on a quarterly basis. The Group consists of the following teams:

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

Oversight of risk management resides with the Audit and Standards Committee which receives a Corporate Risk Register Report on a quarterly basis. The CMT and Service Delivery Leadership Team (SDLT) are also provided with the Corporate Risk Register, however, the CMT are responsible for updating and maintaining the risks identified.

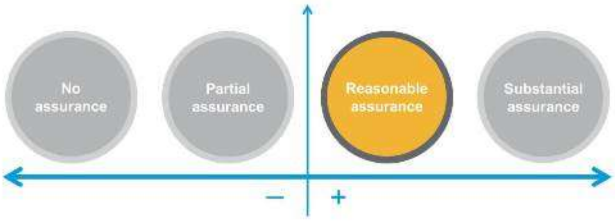
1.2 Conclusion

Our review found that a risk management control framework was in place to mitigate risks identified by the CMT and the wider organisation as appropriate. We found a detailed Risk Management procedure was in place in addition to Abriska User Guides for recording risks. However, we noted that the Service used different risk management terminology compared to that of widely accepted terms. Additionally, we found that whilst there was regular review of organisational risks by CMT, risks overdue for review had not been discussed within CMT meetings and there was no formal escalation process in place to address this. We noted that training on key risk management principles was in place as part of leadership and management development units and training on the use of system was evident through the provision of Abriska user guides. We did note, however, that formal training on key elements of practical organisational risk management such as the quality of risk descriptions, the level of information required for risk reviews and management of risk actions has not been provided to risk owners.

Overall, we noted that there had been improvement in the management of this area since our last review in April 2018. This can be demonstrated by the introduction of the functionality for the recording of mitigating controls, assurances and gaps in controls within Abriska, indicating a positive move towards a more integrated, evidence-based approach to risk management. However, further work was now required to populate the increased functionality.

Internal audit opinion:
Taking account of the issues identified, the Authority can take reasonable assurance that the controls in place to manage this risk 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 risk(s).



1.3 Key findings

The key findings from this review are as follows:

Service Assurance Framework and Procedures

- We confirmed the Service has in place a Service Assurance Framework which was approved in August 2018 by the Chief Fire Officer. We noted the framework detailed key information on business continuity, information security and risk management.

- Additionally, we found the Service had in place a Corporate Risk Management Policy and Risk Management Service Order. We were advised by the Organisational Assurance Manager that both documents were in the process of being combined to form an up to date Risk Management Service Order.

Risk Management Training

- Review of the Service Assurance Framework revealed the Head of Service Development and Assurance was responsible for ensuring Risk Management arrangements were embedded into the Service's culture. Whilst we found training guides for the use of Abriska were in place, formal training on risk management had not been provided to risk owners. Failure to have in place formal training increases the risk of risk owners not having sufficient practical knowledge of risk management to enable effective management of the organisation's risks. **(Medium)**

Corporate Risk Register

- Through review of the October, November and December 2018 CMT minutes, we found two new risks were identified by the CMT and discussed in relation to Sharepoint and Brexit.

- We found that, following an action raised in our 2017/18 Risk Management review, the Abriska system had been updated to include fields for mitigating controls, assurances and gaps in controls/assurances. We noted, however, that these fields had not been populated for the risks on the Corporate Risk Register. This may result in risks not being effectively monitored and gaps not being identified in controls and assurances to mitigate against. **(Medium)**

- Each of the Service's risks are described using the cause-effect model, and each risk is assigned an absolute risk score, an inherent risk score and a residual risk score using a 5x5 matrix. The risk scoring definitions are not in line with widely accepted risk management terminology (including the inherent risk score related to the current risk level, given the controls in place; and the residual risk score related to the target risk level for the

organisation. Whereas the generally accepted risk management terminology, where the untreated risk rating is the inherent risk, the risk rating with controls in place is the residual risk and the target risk level would be known as a target score.)
There may be a risk of confusion, particularly when engaging with external organisations in relation to risk management if generally accepted risk terminology is not used. If the organisation wishes to continue with its current terminology, there is a risk of risks being assigned inappropriate scores if the organisational definitions of absolute, inherent and residual risk are not defined within the Risk Management Service Order. **(Medium)**

Risk Management Governance

- We confirmed the Service had in place Terms of Reference for the CMT and Service Delivery Leadership Team (SDLT, formerly the Service Delivery Management Team). We noted the remit of both forums.

- Review of the July, September and December 2018 Audit and Standards Committee minutes revealed the Corporate Risk Register Report was consistently received which detailed changes to risks and scores.

- The CMT is provided with an update on the Corporate Risk Register on a monthly basis. Evidence of challenge of outstanding risk reviews and actions is not recorded within the CMT minutes and there is no formal escalation process in place for non-compliance with regards to risk reviews and outstanding actions. We noted of the 39 risks identified on the January 2019 risk register, 14 risks were overdue for review. Whilst we noted the residual risk scores of ten of the 14 overdue risks were below five, the remaining four overdue risks were scored eight and higher.   Failure to update risks in a timely manner increases the risk that such events identified within the risk register may materialise without frequent review and the introduction of risk mitigating controls. **(Medium)**

We have also agreed four ‘low’ priority management actions, detailed further in section two, below.

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	3	(10)	5	(10)	4	4	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	7	3	0

Number of actions implemented/ superseded	3	1	0
Actions not yet fully implemented:	4	2	0

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)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
1	The organisation has a Corporate Risk Management Policy and Risk Management Service Order in place. The policy and service order are due to be combined into a revised Risk Management Service Order which is currently in draft format. The Service Order is reviewed annually and is available to all relevant staff via the organisation's intranet site.	Yes	No	We were advised by the Organisational Assurance Manager that the Risk Management Policy and Risk Management Service Order were being combined, resulting in an up to date Risk Management Service Order. We reviewed the current policy and Service Order and confirmed that they provided details of the risk management processes in place, including risk identification, risk assessment and risk rating. We noted through review of the draft Service Order that the responsibility for CMT to review and update risks had been added.	Low	The revised Risk Management Service Order will be approved at the appropriate governance forum and made accessible to all relevant staff.	April 2019	Organisational Assurance Manager

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				We noted that there was no clear timeframe for when the revised Service Order would be approved and available to all relevant staff. There is a risk of the current service order not being reflective of organisational practice.				
2	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. Whilst fields for mitigating controls, assurances and gaps in control exist within the Abriska system, these have not been populated for any risks on the Corporate Risk Register.	No	NA	A management action had been agreed during our 2016/17 Risk Management review regarding 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 whilst the Abriska system had been updated to include the above fields, these fields had not been populated for the risks on the Corporate Risk Register. This may result in risks not being effectively monitored and gaps not being identified in controls and assurances to mitigate against.	Medium	Risks on the Corporate Risk Register will have the following fields populated: • Mitigating controls; • Assurances against controls; and • Gaps in controls / assurances.	May 2019	Head of Service Development & Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
3	Each of the Service's risks are described using the cause-effect model, and each risk is assigned an absolute risk score, an inherent risk score and a residual risk score using a 5x5 matrix. The risk scoring definitions are not in line with widely accepted risk management terminology.	No	NA	We were advised by the Head of Service Development and Organisational Assurance that: • the absolute risk score related to the impact of the risk untreated if no controls were in place; • the inherent risk score related to the current risk level, given the controls in place; and • the residual risk score related to the target risk level for the organisation. We noted that this differed from generally accepted risk management terminology, where the untreated risk rating is the inherent risk, the risk rating with controls in place is the residual risk and the target risk level would be known as a target score. There may be a risk of confusion, particularly when engaging with external organisations in relation to risk management if generally accepted risk terminology is not used. If the organisation wishes to continue with its current terminology, there is a risk of risks being assigned inappropriate scores if the organisational definitions of absolute, inherent and residual risk are not defined within the Risk Management Service Order.	Medium	The organisation will decide whether to utilise the standard risk management definitions for inherent, residual and target risk. If it decides to continue with its use of absolute, inherent and residual risks, the definitions of these will be documented within the Risk Management Service Order.	May 2019	Organisational Assurance Manager
4	The Service Assurance Framework states that it is the responsibility of the Head of Service	Yes	No	We were advised by the Head of Service Development and Organisational Assurance that risk owners are members of CMT and their appointment relies on a level of	Medium	Formal risk management training will be provided to risk	May 2019	Organisational Assurance Manager

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	Development and Assurance to ensure that Risk Management arrangements are embedded into the service culture. This includes training for all managers with respect to Risk Management.			management knowledge which will usually include training in the principles of risk management including qualifications in Business Management for two of the three CMT members. We noted that user guides were in place for the use of Abriska and held within the system to assist with use. Whilst training guides for the use of the system are in place and risk owners are expected have some knowledge of risk management principles, formal training on key elements of practical organisational risk management such as the quality of risk descriptions, the level of information required for risk reviews and management of risk actions has not been provided to risk owners. Additionally, with the organisation moving towards assigning mitigating controls, assurances and gaps in controls to all risks in the risk register for the first time, there is a risk of risk owners not having sufficient practical knowledge of risk management to enable effective management of the organisation's risks.		owners and other key staff. Areas to be covered could include: • the quality of risk descriptions • the level of information required for risk reviews • management of risk actions • mitigating controls • assurances gaps in control		
5	Each Service risk is assigned a risk owner who is responsible for reviewing their risks. Members of the CMT are responsible for updating and maintaining	Yes	No	Through review of the January 2019 Corporate Risk Register, we selected a sample of ten risks and reconciled the risks to the Abriska System.	Low	The Service will update the Risk Procedure to include the minimum frequency at which risks will be reviewed.	May 2019	Organisational Assurance Manager

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	those risks that fall within their area of responsibility. 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.			We confirmed in all instances, risks had been allocated to responsible owners and risk review dates. Of the ten risks reviewed, we noted actions were raised in five instances. In the remaining five instances, risks were accepted therefore actions were not required. We found of the ten risks reviewed, risks were overdue for review in five instances. We noted this included: • CR44 which was overdue by 110 days and had a residual score of 16; • CR23 which was overdue by 239 days and had a residual score of 3; • CR19 which was overdue by 139 days and had a residual score of 3; • CR14 which was overdue by 82 days and had a residual score of 3; and • CR20 which was overdue by 82 days and had a residual score of 2. Furthermore, we noted that justifications had not been recorded as to why risk reviews had not been completed. Through review of the Service's Risk Management Service Order, we noted that the minimum risk review frequency had not been stated. This was further substantiated through review of the Abriska system as a risk had been highlighted as in need of review,				

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				however, the review date set by the Service was in mid-2019. Failure to actively review risks as review dates fall due increases the risk of such events materialising. Additionally, mitigating actions may not be implemented in a timely manner which may further increase the risk of such events occurring. We have raised a management action below in relation to the overdue risk reviews.				
6	Updates to the register may take place as a result of horizon scanning by the Service Strategic Command Team or CMT. Alternatively, SCT / CMT members can make additions or updates to the Corporate Risk Registers and notify these changes by emailing the Head of Strategic Support	Yes	No	Through review of the October, November and December 2018 CMT minutes, we found two new risks were identified by the CMT in relation to: • Sharepoint becoming unusable; and • Brexit. Whilst we found discussions had taken place around the two risks identified, corresponding inherent risk scores had not been discussed by CMT. Failure to propose risk scores may present the risk of insufficient oversight by the CMT. This may result in inappropriate prioritisation of risks identified.	Low	Management will ensure that where new risks are identified by CMT, risk scores will be allocated to the identified risks prior to being added to the Corporate Risk Register.	May 2019	Organisation al Assurance Manager
7	The CMT Terms of Reference (ToR) is in place to define the group's remit.	Yes	No	Through review of the CMT ToR we noted it was last reviewed in August 2018. We noted the ToR detailed key responsibilities of the CMT which included the review, monitoring and effective management of corporate risk.	Low	Management will update the CMT ToR to include the quoracy requirements and state	May 2019	Head of Service Development

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				We also found both the accountability and reporting lines of the CMT had been stated. However, as per the management action raised in the 2017/18 review, we noted that neither the quoracy or frequency at which the ToR should be reviewed had been stated. Failure to state both the quoracy requirements and frequency the ToR should be reviewed may present the risk of the CMT Team being unreflective of current practice. Furthermore, this may be impeded by decisions taken place without individuals with required proficiency present.		how frequently the ToR is to be reviewed		and Assurance
8	The CMT is provided with an update on the Corporate Risk Register on a monthly basis. A formal report is not presented at the CMT meetings, instead, the Corporate Risk Register is viewed on the projector screen using the Abriska system with a verbal update being provided by the Head of Organisational Assurance. Evidence of challenge of outstanding risk reviews and actions is not recorded	No	NA	Through review of the Authority's Risk Management Procedure, we noted the CMT were responsible for updating and maintaining the risks identified within the corporate risk register. Review of the October, November and December 2018 minutes revealed that the registers were consistently presented. We noted discussion surrounding risks had occurred, however, challenge of risks could not be evidenced within the CMT minutes. We noted of the 39 risks identified on the January 2019 risk register, 14 risks were overdue for review. Whilst we noted the residual risk scores of ten of the 14 overdue	Medium	The CMT will actively discuss and challenge risks that have not been reviewed in line with documented timeframes or those with outstanding actions to be completed. An escalation process will be put in place for any regular non-compliance, with progress against risks (including regularity of review and progress against action plans) to be discussed as part of each risk owner's one	March 2019	Head of Service Development and Assurance

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	within the CMT minutes and there is no formal escalation process in place for non-compliance with regards to risk reviews and outstanding actions.			risks were below five, the remaining four overdue risks were scored eight and higher. Failure to update risks in a timely manner increases the risk that such events identified within the risk register may materialise without frequent review and the introduction of risk mitigating controls.		to one monthly meetings with Principal Officers.		

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
Annual Review of the Risk Management arrangements.

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

Areas for consideration:

- Risk Management Strategy and associated policies and procedures
- The provision of training and the assignment of roles and responsibilities for risk management
- Arrangements for identifying and assessing risks linked to strategic and operational objectives
- Processes for review and updating of the strategic/corporate/operational risk registers
- Processes at a departmental level for reviewing and reporting on risks in these areas
- The arrangements for escalating and reporting risks for the attention of senior management, via appropriate governance forums.
- How controls and assurances and captured on the relevant risk registers, and whether feedback on risks are fed back to committees and groups for assurance purposes.
- The operation and effectiveness of an assurance framework, and the process for escalation and review of risks for consideration and inclusion in relation to this document.

Limitations to the scope of the audit assignment:

- This review did not comment on whether individual risks are appropriately managed, or whether the organisation has identified all of the risks and opportunities facing it.
- 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.

Our work does not provide absolute assurance that material errors, loss or fraud do not exist

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Andy Peckham – Head of Service Development and Assurance
- Ian McLaren – Organisational Assurance Manager
- Karen Daniels – Service Assurance Manager

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	72%	
Reasonable assurance	14%	X
Partial assurance	14%	
No assurance	0%	
Management actions	**Average number in similar audits**	**Number in this audit**
	3	8

FOR FURTHER INFORMATION CONTACT

Suzanne Rowlett, Senior Manager

Suzanne.Rowlett@rsmuk.com

+44 (0)1908 687800

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Bedfordshire Fire & Rescue Authority, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.