BEDFORDSHIRE FIRE AND RESCUE AUTHORITY

Risk Management – Key Controls

FINAL

Internal Audit Report: 10.16/17

12 May 2017

RSM

CONTENTS

Debrief held	5 April 2017	**Internal Audit team**	Dan Harris, Head of Internal Audit Suzanne Rowlett, Senior Manager Anand Mistry, Assistant Manager Farjad Shah, Senior Auditor
Draft report issued	5 May 2017		
Responses received	12 May 2017		
Final report issued	12 May 2017	**Client sponsor**	Darren Cook - Group Commander
		Distribution	Darren Cook - Group Commander

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Risk Management, focussing on the key controls, has been undertaken at Bedfordshire Fire & Rescue 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 was a total of 33 risks on the Corporate Risk Register.

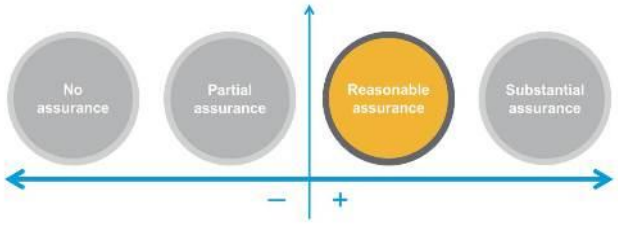
Three Policy and Challenge Groups were in place with responsibility for reviewing risks on a quarterly basis, as follows:

- Corporate Services (CSPCG);
- Human Resources (HRPCG); and
- Service Delivery (SDPCG).

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 Management Team (SDMT) are also provided with an update on the Corporate Risk Register on a monthly basis.

1.2 Conclusion

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:

Corporate Risk Register

Details relating to each individual risks on the Corporate Risk Register are recorded on the Abriska system such as a description of the risk, risk score, responsible owners for risks and controls and actions to mitigate risks.

Policy and Challenge Groups

We reviewed Corporate Risk Register reports to the three Policy and Challenge Groups for the last two quarters and confirmed they were in a consistent format, highlighting changes to risk scores and providing updates against risks as relevant. We noted a lack of challenge around the scoring of risks and this has been expanded below.

Reporting to Audit and Standards Committee

We confirmed through review that the Corporate Risk Register is reported to the Audit and Standards Committee and that they included updates from all three Policy and Challenge Groups, detailing changes to the risks for each. We also confirmed through review of the corresponding meeting minutes for September and December 2016 that changes to the risks were subject to regular oversight and review, including discussion around the treatment of risks.

Reporting to the CMT and SDMT

Although the Corporate Risk Register had not been subject to regular review at CMT and SDMT meetings, this had been identified as an action during meetings and the Corporate Risk Register was subsequently subject to review in the March 2017 meetings.

We found, however, the following issues, resulting in four **medium** priority management actions:

We noted key areas that had not been detailed within risk management policies and procedures, such as risk definitions, roles and responsibilities of key individuals, forums, and all staff in general, and the risk appetite of the organisation. This can result in the overall ineffective management of risks, potentially leading to risks being realised. **(Medium)**

Key fields had not been included in the Corporate Risk Register, such as mitigating controls, assurances against controls and gaps in controls / assurances. This may result in risk-related controls not being effectively monitored and gaps not being identified in controls and assurances to militate against. **(Medium)**

We noted instances where potential implications had not been identified for certain risks, such as risk CRR38, relating to the hacking of business critical or vital computer systems, which did not identify reputational damage as a consequence. In respect of actions, we found a number of cases where these were not sufficiently detailed, did not have responsible owners or due dates assigned, or were significantly overdue, with some actions having due dates in 2013. In other cases, actions were not actually reflective of actions, such as 'Trade Dispute Plan' which had been stated as an action for CRR4.

We also found various cases where risks had not been reviewed in line with their due dates, with some risks dating back to October 2016, such as risk CRR19. All of the above can increase the likelihood of risks materialising, especially where mitigating actions are not put in place in a timely manner to reduce the risk. **(Medium)**

With regards to risk review by the Policy and Challenge Groups, we noted a few cases where positive assurances and updates were received on the management of risks, yet there had been no subsequent revision of risk scores. An example of this is in the September 2016 CSPCG Corporate Risk Register report whereby the following update had been provided against risk CRR27: ‘The Authority has approved the receipt of the four year Government settlement offer. This provides some certainty over the medium term of the Authority's income streams’, however, the report stated that there were no changes to risk scores.

We also noted that there was a lack of discussion around the scoring of risks despite updates being provided against risks at Policy and Challenge Group meetings. This could be partly due to the fact that risk scores are not included in the Corporate Risk Register Reports or alternatively that minutes did not fully record the level of challenge. If risk scores are not actively revised in line with assurances and updates against risks, this can lead to risks not being prioritised appropriately. **(Medium)**

1.4 Additional information to support our conclusion

Area	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
Risk Management – Key Controls	2 (6)	2 (6)	0	4	0
Total			**0**	**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 Additional feedback

We have identified innovation or good practice at similar organisations that Bedfordshire Fire Authority may wish to consider:

Good practice for further consideration

In terms of key definitions and examples to demonstrate aspects of risk management for inclusion within risk management policies and procedures, we have included examples below which could be used to aid this (this is not a comprehensive list):

Definitions:

Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk should be defined along with the subsequent cause and effect.

Controls: Systematic measures (such as reviews, checks and balances, methods and procedures) instituted by an organisation to conduct its business in an orderly and efficient manner, safeguard its assets and resources, deter and detect errors, fraud, and theft, ensure accuracy and completeness of its accounting data, produce reliable and timely financial and management information, and ensure adherence to its policies and plans.

Assurances: An assurance is an outcome, such as an internal audit report, which verifies the operating effectiveness of a control(s)

Residual Risk: The level of risk remaining after the inherent risk has been mitigated by the internal controls and assurances of an organisation.

Example of a risk, control and assurance:

Risk / Cause / Effect	Controls	Recent assurance (Positive or Negative)
Inability to recover from a loss of IT systems, caused by insufficient data recovery arrangements, resulting in the organisation not being able to continue its operations.	*A Disaster Recovery Plan is in place which is tested on an annual basis (and whenever there is a significant change in disaster recovery arrangements).* *A daily, weekly and monthly backup of all systems is undertaken. Test recoveries are undertaken of backups on a quarterly basis (and whenever there is a major hardware or software change to the backup system)*	*Disaster Recovery exercise in January 2017 proved successful and all systems were recovered within 24 hours. (Positive).* *A test recovery was carried out on backup media in December 2016; however the IT team were unable to fully restore all data from backups. (Negative)*

2 ACTION PLAN

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 table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
Area: Risk Management					
1.1	The Corporate RM Policy and RM Service Order did not cover key areas, such as the roles and responsibilities of key staff.	Medium	The Service will review its risk management related policies and procedures to ensure they reflect current practice, and encompass the following information: • Key risk definitions; • Roles and responsibilities of staff and relevant forums; • Risk appetite; and • The escalation process for risks identified by staff.	31 December 2017	Darren Cook – Group Commander / Head of Projects, Safety and Business Support
1.2	Key fields had not been included in the Corporate Risk Register, such as mitigating controls.	Medium	The Corporate Risk Register will be updated to encompass the following fields: • Mitigating controls; • Assurances against controls; and • Gaps in controls / assurances.	31 December 2017	Darren Cook – Group Commander / Head of Projects, Safety and Business Support

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
1.3	A number of issues were found with the content of the Corporate Risk Register, for instance, a number of actions did not have responsible owners or due dates, and others were found to be significantly overdue.	Medium	A Risk Champion will be assigned to review the Corporate Risk Register on a periodic basis to check that: • All fields are complete and sufficiently detailed for each risk; • All potential implications of risks are identified; • Actions have responsible owners and due dates assigned; • Actions are completed in line with their due date. and • Risks are reviewed in line with their review date. Where there is non-compliance with the above, this will be escalated by the Risk Champion accordingly.	30 September 2017	Darren Cook – Group Commander / Head of Projects, Safety and Business Support
1.4	Risk scores were not being actively revised in line with assurances and updates against risks.	Medium	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.	30 September 2017	Darren Cook – Group Commander / Head of Projects, Safety and Business Support

3 DETAILED FINDINGS

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	Actions for management
Area: Risk Management						
1.1	The Service have in place a Corporate Risk Management Policy (RM Policy) which is supported by a Risk Management Service Order (RM SO) which details the various processes in place for risk management. Both documents are available to all staff on the intranet. There are, however, certain key aspects not included in the policy, such as the risk appetite of the organisation.	No	N/A	Through review of the RM SO, we confirmed that it had been last reviewed in January 2017. We found, however, that the Corporate RM Policy had not been reviewed since November 2014. Without regular review, this can result in the policy not remaining reflective of current practice. We found through review of the RM SO that it stated the following: "Existing controls are noted in the column 'Existing Risk Controls' of the Corporate Risk Register." We noted, however, that controls are not identified in the Corporate Risk Register, and a management action has been raised below in section 1.2. We also noted other issues with the RM SO: • Key risk definitions had not been detailed; • The RM SO implied that the Corporate Risk Register is reviewed by the Strategic Command Team, which is no longer the case; • The roles and responsibilities of key individuals, forums, and all staff in general, had not been detailed; and • No mechanism had been included for centrally escalating risks for review and	Medium	The Service will review its risk management related policies and procedures to ensure they reflect current practice, and encompass the following information: • Key risk definitions; • Roles and responsibilities of staff and relevant forums; • Risk appetite; and • The escalation process for risks identified by staff.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Actions for management
				potential inclusion on the risk register. We also noted that the RM SO referred to the risk appetite of the organisation being detailed in the Corporate RM Policy; however, we found that this had not been included. The above can result in the overall ineffective management of risks, potentially leading to risks being realised. We confirmed through review that the Policy and Service Order were available to all staff on the intranet.		
1.2	Individual risks are recorded on and managed using the Abriska system. The Service has a Corporate Risk Register in place 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	Through review of the latest Corporate Risk Register, we found that although it covered certain details in relation to risks, such as the risk score, we noted that certain key fields had not been included: • Mitigating controls; • Assurances against controls; and • Gaps in controls / assurances. This may result in the risk not being effectively monitored and gaps not being identified in controls and assurances to mitigate against.	Medium	The Corporate Risk Register will be updated to encompass the following fields: • Mitigating controls; • Assurances against controls; and • Gaps in controls / assurances.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Actions for management
1.3	Each of the Service's risks are described using the cause-effect model. Risk treatment actions are identified for each risk. This is to include details of the action along with the action owner and a proposed date for the completion of the action.	Yes	No	We confirmed through review that for all 33 risks identified in the Corporate Risk Register, the cause and effect had been detailed for each risk. We noted instances, however, where potential implications had not been identified for certain risks. An example of this is where risk CRR38, relating to the hacking of business critical or vital computer systems, did not identify reputational damage as a consequence. If all implications of risks are not identified, risks may not be scored appropriately, resulting in the risk not being prioritised accordingly. With regards to actions, we found a number of cases where these were not sufficiently detailed, did not have responsible owners or due dates assigned, or were significantly overdue, with some actions having due dates in 2013. In other cases, actions were not actually reflective of actions, such as 'Trade Dispute Plan' which had been stated as an action for CRR4, however it was not clear whether the action was for a plan to be produced, or updated, or reviewed etc. All of the above can result in the appropriate actions not being implemented promptly to mitigate risks, increasing the likelihood of risks materialising. Through further review of the Corporate Risk	Medium	A Risk Champion will be assigned to review the Corporate Risk Register on a periodic basis to check that: • All fields are complete and sufficiently detailed for each risk; • All potential implications of risks are identified; • Actions have responsible owners and due dates assigned; • Actions are completed in line with their due date. and • Risks are reviewed in line with their review date. Where there is non-compliance with the above, this will be 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	Actions for management
				Register, we found various cases where risks had not been reviewed in line with their due dates, with some risks dating back to October 2016, such as risk CRR19. Without regular review, changes in circumstances may not be identified in a timely manner, resulting in risks not being prioritised appropriately.		
1.4	Three Policy and Challenge Groups are in place as follows: • Corporate Services (CSPCG); • Human Resources (HRPCG); and • Service Delivery (SDPCG). A Corporate Risk Register Report is produced on a quarterly basis for review by each Policy and Challenge Group for risks impacting on their areas of responsibility, including changes to risk ratings and any updates in relation to risks.	Yes	No	Through review of the Corporate Risk Register reports to the three Policy and Challenge Groups for the last two quarters (September 2016 to January 2017), we confirmed that they were in a consistent format, highlighting changes to risk scores and providing updates against risks as relevant. We noted a few cases, however, where positive updates and assurances were received against risks, yet there had been no subsequent revision of risk scores. An example of this is in the September 2016 CSPCG Corporate Risk Register report whereby the following update had been provided against risk CRR27: "The Authority has approved the receipt of the four year Government settlement offer. This provides some certainty over the medium term of the Authority's income streams.", however, the report stated that there were no 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	Medium	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.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no/ N/A)	Audit findings and implications	Priority	Actions for management
				being subject to regular review with discussion taking place around updated risks. We noted, however, that there was a lack of discussion around the scoring of risk despite updates being provided against risks. This could be partly due to the fact that risk scores are not included in the Corporate Risk Register reports. If risk scores are not actively revised in line with assurances and updates against risks, this can lead to risks not being prioritised appropriately.		

APPENDIX A: SCOPE

Scope of the review

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. The scope was planned to provide assurance on the controls and mitigations in place relating to the following areas:

Objective of the area under review
To ensure that the risks to the achievement of the Authority's objectives are identified and mitigated

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

Areas for consideration:

A key controls review designed to provide assurances that the risk management arrangements have been established, deemed to be effective and subject to regular monitoring, review and reporting to management and through the Service and Authority governance structure at the appropriate level.

Our review covered the following:

- Risk Policy / Strategy in place, periodically reviewed and approved at appropriate level. To include:
    - Risk assessment criteria / process clearly defined.
    - Responsibilities clearly defined.
- Completion of Risk Registers including:
    - Risk description.
    - Risk score – inherent and residual.
    - Controls in place.
    - Action to further mitigate risk.
    - Risk Owners defined.
- Regular review and reporting of Risk Register at appropriate level within the Service and Authority.

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 have not conducted 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 the Authority and senior management to agree and manage their 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:

- Darren Cook - Group Commander
- Karen Daniels - Service Assurance Manager
- Lesley Girt - Principal Officers' Personal Assistant

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
Green (substantial assurance)	28.57%	
Amber Green (reasonable assurance)	28.57%	X
Amber Red (partial assurance)	42.86%	
Red (no assurance)	0	
Management actions	**Average number in similar audits**	**Number in this audit**
	6	4

FOR FURTHER INFORMATION CONTACT

Suzanne Rowlett, Senior Manager

Suzanne.Rowlett@rsmuk.com

(+44)7720 508 148