



ESSEX FIRE AUTHORITY

Business Continuity - Operational Response

FINAL

Internal Audit Report: 10.16/17

14 November 2017

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

1 Executive summary	2
2 Action plan.....	4
3 Detailed findings.....	7
APPENDIX A: SCOPE	11
APPENDIX B: FURTHER INFORMATION	12
For further information contact	13

Debrief held	3 April 2017	Internal Audit team	Dan Harris, Head of Internal Audit Suzanne Rowlett, Senior Manager Anand Mistry, Assistant Manager Matt Wright, Senior Auditor Aidon Ford, Internal Auditor
Draft report issued	5 May 2017 20 June 2017 & 10 July 2017		
Revised draft issued			
Responses received	14 November 2017		
Final report issued	14 November 2017	Client sponsor	Charles Thomas, Corporate Risk and Business Continuity Manager
		Distribution	Charles Thomas, Corporate Risk and Business Continuity Manager Mike Clayton, Director of Finance and Treasurer

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at <http://www.icaew.com/en/members/regulations-standards-and-guidance>.

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. Recommendations for improvements should be assessed by you for their full impact before they are implemented. 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.

This report is solely for the use of the persons to whom it is addressed and 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

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Business Continuity - Operational Response was undertaken as part of the approved internal audit plan for 2016/17. The audit was designed to provide assurance over the Authority's controls to ensure it can continue to operate and respond effectively in the event of any serious incident.

As a Category 1 Responder, Essex Fire Authority is bound by the requirements of the Civil Contingencies Act 2004 (CCA 2004). The CCA 2004 requires that the Authority assess the risk of emergencies occurring and use the results to inform contingency planning; to put in place emergency and business continuity plans, to share information and cooperate with local responders to enhance coordination.

Senior leadership responsibility for the business continuity management function rests with the Director of Finance and Treasurer. Day to day oversight of the business continuity management process is the responsibility of the Corporate Risk and Business Continuity Manager, who is assisted in his duties by a Risk Officer and a Business Continuity Officer.

A survey conducted by the Risk and Business Continuity Team in Autumn 2016 identified a number of significant deficiencies, including the absence of processes at department level for identifying hazards, a lack of exercising activity, the majority of respondents expressing serious concerns about the existence or visibility of Business Continuity Plans, and a lack of understanding of the Civil Contingencies Act.

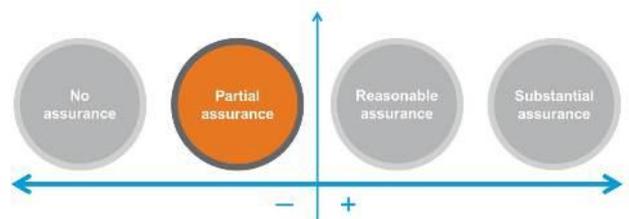
1.2 Conclusion

During the course of our audit, it was apparent that key operational business continuity plans were significantly out of date and were not being subjected to regular and rigorous testing. Work undertaken by the Risk and Business Continuity Team had highlighted significant process and knowledge gaps regarding business continuity management at the departmental level. We were not sufficiently assured from review of Senior Leadership Team meeting minutes that business continuity was given adequate attention, although this was a key part of the Team's documented remit. Due to a number of high priority findings, action is required to strengthen the control framework; as such, we can provide only partial assurance.

Internal Audit Opinion:

Taking account of the issues identified, whilst the Authority can take partial assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied.

Action is needed to strengthen the control framework to ensure this area is effectively managed.



1.3 Key findings

The findings from this review have resulted in five **high** and one **medium** priority management actions being agreed. The key findings from this review are as follows:

Business Continuity Plans

We reviewed the Business Continuity Plans for Fleet Management, Industrial Action, and Control as well as the overall Strategic Business Continuity and Recovery Plan. Through review we noted that these plans did not identify the key activities or objectives along with a clear plan of action to ensure that these objectives are delivered during an adverse event.

In addition, we noted that the plans did not adequately identify Maximum Tolerable Periods of Disruption (MTPD) or Recovery Time Objectives (RTO) nor were they subject to testing with subsequent review and updates made to ensure that the plans remain fit for purpose.

Without robust business continuity arrangements in place, and regular, rigorous exercising of plans, there is a combined risk of financial, operational and reputational impacts to the Authority in the event of serious operational disruption.

Management of Business Continuity Arrangements

We reviewed the terms of reference for Service Leadership Team (SLT) as well as the minutes for 15 SLT meetings dated between November 2016 and February 2017. We noted that the terms of reference documented the SLT's responsibility for reviewing, monitoring and ensuring effective management of business continuity arrangements. However, from review of the 15 SLT meeting minutes, we were unable to verify that business continuity arrangements had been discussed and challenged by the SLT at any point.

We also identified that there is no organisation-wide process for reviewing third-party BCPs or gaining assurance that they are working effectively.

We were advised that this had not historically been carried out by the Procurement Department. We were also advised that there was an intention to receive assurances from strategic suppliers regarding their business continuity arrangements however a formal programme regarding this was a work in progress.

Additional information to support our conclusion

Area	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
Business Continuity – Operational Response	4 (9)	1 (9)	0	1	5
Total			0	1	5

* 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.

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: Business Continuity					
1.1	We were unable to establish any reference within the Strategic Business Continuity and Recovery Plan to the activities or programme that would be required to deliver these objectives.	Medium	The Authority will ensure that the activities required to deliver the objectives are explicitly documented within the Strategic Business Continuity Plan. This includes setting out what level of business continuity planning required to be completed by Department Heads and Managers, and how these feed into wider service plans.	March 2018	Risk & Business Continuity Manager
1.2	We noted through review of our sample of six Business Continuity Plans, that only the Fleet Management plan had identified Maximum Tolerable periods of disruption and Recovery Time Objectives.	High	The Authority will identify Maximum Tolerable Periods of Disruption as well as Recovery Time Objectives and the resources required to achieve these for critical activities and incorporate these into Business Continuity Plans where appropriate.	March 2018	Department Managers/ Plan owners

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
1.3	We noted that the Business Continuity Plans were out of date and did not include clear actions and timescales for completion.	High	<p>All Business Continuity Plans will be reviewed and updated annually by the plan owners. This will include input and review by the Risk and Business Continuity Team to ensure that the level of detail and the transparency of plans are consistent across the organisations.</p> <p>Plans will include clear actions and timescales for completion, including details of those responsible for completing the actions.</p>	March 2018	Department Managers/ Plan owners
1.4	We noted that there is no formal programme in place for exercising and testing business continuity arrangements.	High	<p>Once adequate BCPs are in place, a formal testing programme will be established for testing the plans at appropriate intervals.</p> <p>Plans will be tested annually at a minimum. Lessons learned reports will be produced following each exercise and used to inform any necessary updates to BCPs.</p>	March 2018	Risk & Business Continuity Manager/Department Managers
1.5	<p>The SLT is responsible for reviewing, monitoring and ensuring effective management of business continuity arrangements.</p> <p>We reviewed a total of 15 SLT meeting minutes and could not verify that business continuity arrangements had been discussed by the SLT at any point.</p>	High	The Service Leadership Team, as the owners of business continuity arrangements, will regularly consider business continuity arrangements, and ensure that the robustness and completeness of business continuity plans is monitored. The SLT will receive regular, clear and evidence-based assurances from the Business Continuity Team that robust business continuity arrangements are in place.	March 2018	SLT

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
1.6	There is currently no clear and formal process for considering and approving the Business Continuity Plans adopted by partners or suppliers	High	ECFRS will evaluate supplier BCP's to establish their resilience on a case by case basis as considered appropriate, dependent upon the nature and value of the business being conducted. Where appropriate the requirement to have a suitable BCP will become a condition of contract.	March 2018	Risk & Business Continuity Manager/Head of Purchasing

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)	Audit findings and implications	Priority	Actions for management
Area: Business Continuity						
1.1	<p>The Authority has a Strategic Business Continuity and Recovery Plan in place. However, this is out of date and is currently undergoing review.</p> <p>The Plan includes an overview of business continuity principles, a schedule of service sites, general strategic considerations in the event of a service disruption, and command and control communication arrangements.</p>	Yes	No	<p>We were provided with the Strategic Business Continuity and Recovery Plan and through review we noted that the document stated its purpose as to provide a strategic response to a major business interruption.</p> <p>In addition, we identified that the aim of the plan had been documented as to provide a framework in which to manage the responses of the Service in order to mitigate the effects of a major business continuity interruption and following this, the seven objectives of the plan had also been documented.</p> <p>However, we were unable to transparently establish the activities or programme required to deliver these objectives. This includes the roles, responsibilities and requirements of Department Heads and Managers in supporting the Corporate Risk and Business Continuity Department in operationally delivering the strategy.</p> <p>We were informed that the Corporate Risk and Business Continuity Manager is developing a revised Business Continuity framework that places the onus of responsibility on Department Heads and Managers to operate effectively in the event of continuity issues, however, this does not in itself address the lack of a clear programme of activities.</p> <p>If the Plan does not transparently set out the activities required to deliver the objectives, there is a risk that the Authority may fail to achieve their objectives and effectively plan for the a business continuity event.</p>	Medium	<p>The Authority will ensure that the activities required to deliver the objectives are explicitly documented within the Strategic Business Continuity Plan.</p> <p>This includes setting out what level of business continuity planning required to be completed by Department Heads and Managers, and how these feed into wider service plans.</p>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
1.2	<p>Business Impact Assessments (BIAs) are incorporated within the Business Continuity Plans for industrial action, fleet and control.</p> <p>These list the critical activities for each area, as well as the Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objectives (RTOs) and the resources for achieving the RTOs.</p>	No	N/A	<p>We reviewed of the Industrial Action, Fleet Management, and Control plans and identified that only the fleet management plan had identified a Maximum Tolerable Period of Disruption (MTPD). Furthermore, only two plans identified an RTO with the fleet management plan also quantifying the resources required to achieve RTO's. The Control BIA did not include an MTPD or RTO, or quantify the resources required to achieve the RTO.</p> <p>We accept that there is a clear imperative to restore all activities as soon as possible however without MTPDs and RTOs, the Authority will be unable to prioritise resources to ensure that they are used most effectively to adequately maintain critical activities at an acceptable level during an adverse event.</p>	High	The Authority will identify Maximum Tolerable Periods of Disruption, Recovery Time Objectives, and the resources required to achieve these for critical activities and incorporate these into Business Continuity Plans where appropriate.
1.3	<p>Business Continuity Plans are in place No relating to industrial action, fleet management, and control. Stations have prepared basic contingency documents, but no formal continuity plans.</p>	No	N/A	<p>We reviewed three key operational business continuity plans (industrial action, fleet and control) to assess whether their design and content were fit for purpose.</p> <p>Our testing found that the industrial action BCP had not been updated since 2013 and the control BCP was last reviewed in 2012. It was noted that the industrial action BCP had been used multiple times since 2013 and we were informed that these had resulted in the evolution of these plans however these changes had not yet been reflected.</p> <p>Review of the industrial action contingency plan (known as Operation Gian) found that it was excessively large with excess verbiage, this creates the risk that it is unwieldy to use in practice. Furthermore, although a communication plan and strategy were included, no key contact details were listed in the plan And there was no clear analysis of critical activities or corresponding recovery timescales.</p> <p>Both the Fleet and Control BCPs included the resources for the recovery of critical activities however no clear</p>	High	<p>All Business Continuity Plans will be reviewed and updated annually by the plan owners. This will include input and review by the Risk and Business Continuity Team to ensure that the level of detail and the transparency of plans are consistent across the organisations.</p> <p>Plans will include clear actions and timescales for completion, including details of those responsible for completing the actions.</p>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				<p>processes were captured for their mobilisation. The Fleet and Control BCPs were largely at the level of a Business Impact Assessment, rather than a specific plan of actions to be undertaken following invocation. The Control BCP had more detail in this respect.</p> <p>We confirmed in discussion with the Control Room Manager that the Control BCP was not usable in its current form and that work was being undertaken with the Risk and Business Continuity Department to revise it.</p> <p>Ultimately, our testing found that there was significant inconsistency in the design and review of the business continuity plans. If Business Continuity Plans are not up to date, and do not include adequate detail with respect to specific actions and responsible owners, there is a risk that a materialising incident is will not be managed effectively and this could have an adverse impact on the safety of service users.</p>		
1.4	<p>There is no formal programme in place for exercising and testing business continuity arrangements. No exercising or scenario planning activity is currently taking place with respect to operational Business Continuity Plans.</p> <p>As a consequence, there is no process in place for formally identifying, recording and actioning lessons learned.</p>	No	N/A	<p>In discussion with the Corporate Risk and Business Continuity Manager, exercising of operational business continuity plans is the responsibility of the relevant departments.</p> <p>It was noted that there is no formal programme in place at the corporate or departmental levels for exercising business continuity plans.</p> <p>With respect to industrial action, it was noted that there was a limited requirement for exercising, as the Authority had had extensive experience of applying the relevant business continuity plan during industrial action in recent years. Similarly, we confirmed in discussion with the Control Room Manager that evacuation exercises had taken place in the past. We note however, that this was not testing of the plan as such, but a general resilience test.</p> <p>Without a formal programme of exercising business</p>	High	<p>Once adequate BCPs are in place, a formal testing programme will be established for testing the plans at appropriate intervals.</p> <p>Plans will be tested annually at a minimum. Lessons learned reports will be produced following each exercise and used to inform any necessary updates to BCPs.</p>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Actions for management
				continuity plans in place, there is a significant risk that they are not fit for purpose, that weak areas in the plans are not identified, and therefore to the continuity of operations.		
1.5	<p>The Service Leadership Team (SLT) assists Essex Fire Authority to meet their responsibilities to establish and oversee the corporate governance arrangements of the Service.</p> <p>The SLT is responsible for reviewing, monitoring and ensuring effective management of business continuity arrangements.</p> <p>A standing quarterly agenda item is documented in the Team's terms of reference for receiving updates on Corporate Risk and Business Continuity.</p>	Yes	N/A	<p>We reviewed the terms of reference for the SLT, confirming that they clearly documented the group's responsibility for reviewing, monitoring and ensuring effective management of business continuity arrangements. We also confirmed that they recorded a quarterly standing agenda update on corporate risk and business continuity.</p> <p>We reviewed a total of 15 SLT meeting minutes, covering the period November 2016 to February 2017. Although we noted that a quarterly Risk and Business Continuity Update was provided in February 2017, this included no information relating to business continuity, and throughout the entire period we could not verify that business continuity arrangements had been discussed by the SLT at any point.</p> <p>If there is insufficient oversight and direction of business continuity management from senior leadership, there is a risk that the process is not fit for purpose.</p>	High	The Service Leadership Team, as the owners of business continuity arrangements, will regularly consider business continuity arrangements, and ensure that the robustness and completeness of business continuity plans is monitored. The SLT will receive regular, clear and evidence-based assurances from the Business Continuity Team that robust business continuity arrangements are in place.
1.6	There is currently no clear and formal process for considering the Business Continuity Plans adopted by partners or suppliers acting on behalf of the service, or for receiving assurances that their plans are working effectively.	No	N/A	<p>In discussion with the Corporate Risk and Business Continuity Manager, it was noted there is no organisation-wide process for reviewing third-party BCPs or gaining assurance that they are working effectively. It was noted that this would be the responsibility of the relevant head of department.</p> <p>We noted in discussion with the new Head of Procurement that there was an intention to receive assurances from strategic suppliers regarding their business continuity arrangements; however, there is currently no formal programme of work in place to progress this and this had not been done historically by the procurement department</p>	High	ECFRS will evaluate supplier BCP's to establish their resilience on a case by case basis as considered appropriate, dependent upon the nature and value of the business being conducted. Where appropriate the requirement to have a suitable BCP will become a condition of contract

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 the Service can continue to operate and respond effectively in the event of any serious incident

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

Areas for consideration:

- The development of business continuity plans for the operational aspects of the Fire Service (appliances, staff strikes, etc.).
- The inclusion of requirements provided by the Civil Contingencies Act within approved business continuity plans.
- The assurances received that the plans are compliant with the Civil Contingencies Act.
- The communication of operational plans throughout the Service and to any external suppliers/partners where applicable.
- The periodic testing of the operational business continuity plans to ensure that they are fit for purpose.
- The use of any scenario planning exercises to discuss and consider the existing plans in place and whether they are fit for purpose.
- How lessons are learnt from testing, shared with the Service and where necessary updated in to the Business Continuity Plans.
- The consideration and approval of Business Continuity Plans adopted by Partners/Suppliers acting on behalf of the Service and the assurances received that their Business Continuity processes are working effectively.

Limitations to the scope of the audit assignment:

- The audit did not consider all aspects of business continuity. This review focused on operational aspects and not business support functions.
- The audit does not provide assurance that the plans derived will be sufficient and have the capability to ensure continuity in the event of an incident.
- We have not provided assurances on areas not covered within the business continuity plans reviewed as part of this audit.
- The scope of the work was be limited to those areas examined and reported upon in the areas for consideration in the context of the objectives set out in for this review. It should not, therefore, be considered as a comprehensive review of all aspects of non-compliance that may exist now or in the future.

Any testing undertaken as part of this audit was compliance based and sample testing.

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:

- Mike Taylor – Director Finance and Treasurer
- Charles Thomas – Corporate Risk and Business Continuity Manager
- Steve Brant – Business Continuity Officer
- Peter Suarez – Control Room 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	39%	
Reasonable assurance	44%	
Partial assurance	11%	X
No assurance	6%	

Management actions	Average number in similar audits	Number in this audit
	5	6

FOR FURTHER INFORMATION CONTACT

Suzanne Rowlett – Senior Manager

Suzanne.Rowlett@rsmuk.com

07720 508148