# ESSEX FIRE AUTHORITY

## Business Continuity - Operational Response

### DRAFT

### Internal Audit Report: 10.16/17

### 5 May 2017



RSM

# CONTENTS



| | | | |
|---|---|---|---|
| **Debrief held** | 3 April 2017 | **Internal Audit team** | Dan Harris - Head of Internal Audit<br>Suzanne Rowlett - Senior Manager<br>Matt Wright - Senior Auditor<br>Aidon Ford – Internal Auditor |
| **Draft report issued** | 5 May 2017 | | |
| **Responses received** | | | |
| **Final report issued** | | **Client sponsor** | Charles Thomas – Corporate Risk and Business Continuity Manager |
| | | **Distribution** | Charles Thomas – Corporate Risk and Business Continuity Manager<br>Mike Clayton – Director of Finance and Treasurer |

# 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.

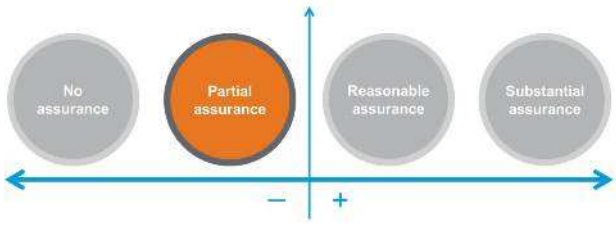
A survey conducted by the Risk and Business Continuity Team in Autumn 2016 identified a number of significant deficiencies, including the absence of processes at department level for identifying hazards, a lack of exercising activity, the majority of respondents expressing serious concerns about the 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, 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 two **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.

Furthermore Business Impact Assessments (BIAs) were not taking place at the individual fire stations that were tested as part of our sample.

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 | 2 | 5 |
| **Total** | | | **0** | **2** | **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. | | |
| 1.2a | We noted that no Business Impact Assessments had been completed for the fire stations under review. | Medium | Business Impact Assessments will form an integral part of station business continuity planning. | | |
| 1.2b | 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 all Business Continuity Plans. | | |

| 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 | All business continuity plans will be updated annually by the plan owners. This will include input from the Risk and Business Continuity Team where appropriate, who will perform a secondary review to ensure plans are fit for purpose.<br><br>Plans will include clear actions and timescales for completion, including details of those responsible for completing the actions. | | |
| 1.4 | We noted that there is no formal programme in place for exercising and testing business continuity arrangements. | High | Once adequate BCPs are in place, a formal testing programme will be established for testing the plans at appropriate intervals.<br><br>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. | | |
| 1.5 | The SLT is responsible for reviewing, monitoring and ensuring effective management of business continuity arrangements.<br><br>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. | High | The Service Leadership Team will challenge the Risk and Business Continuity Team regarding the status of and progress against business continuity management, raising appropriate actions to address weak areas, and following these through to completion.<br><br>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 and approving the Business Continuity Plans adopted by partners or suppliers | High | The Authority will implement a clear and formal process for the review of third-party BCPs, and gain frequent assurance regarding their effectiveness. | | |

# 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 | The Authority has a Strategic Business Continuity and Recovery Plan in place. However, this is out of date and is currently undergoing review.<br><br>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.<br><br>The Strategy includes a set of business continuity strategic objectives. | Yes | No | 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 for Business Continuity Management and Recovery.<br><br>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 seven objectives had also been documented.<br><br>However, we were unable to establish any reference within the document to the activities or programme that would be required to deliver these objectives.<br><br>If the Business Continuity Plan does not address the activities that are required to deliver the objectives there is a risk that the authority may fail to achieve their objectives. | Medium | The Authority will ensure that the activities required to deliver the objectives are explicitly documented within the Strategic Business Continuity Plan. |
| 1.2 | Business Impact Assessments (BIAs) are incorporated within the Business Continuity Plans for industrial action, fleet and control.<br><br>These list the critical activities for each area, as well as the Maximum Tolerable Period of Disruption and Recovery Time Objectives (RTOs). Resources for achieving the RTOs are | No | N/A | We noted that no BIAs had been completed for the stations under review (Basildon, Colchester and Southend).<br><br>Without robust business impact assessments, there is a risk that the stations have not adequately identified their critical activities or the size and nature of disruption to the activity, leading to an increased likelihood that there will be an intolerable level of disruption.<br><br>Similarly, without an appropriate assessment of the Maximum Tolerable Period of Disruption or Recovery Time | Medium<br><br>High | Business Impact Assessments will form an integral part of station business continuity planning.<br><br>The Authority will identify Maximum Tolerable Periods of Disruption as well as Recovery |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Actions for management |
|---|---|---|---|---|---|---|
| | documented.<br><br>BIAs are not completed, however, at the station level. | | | Objectives, there is a risk that actual disruption will not be manageable within agreed timeframes.<br><br>In addition, we identified that although the industrial action plan detailed the actions for short duration (up to 24 hours) and duration of up to 8 days, no assessment had been made regarding the impact to the authority in the first 24 and 48 hours.<br><br>This creates the risk that the Authority may not undertake actions with an appropriate level of mitigation to minimise the effects caused as a result of an adverse event.<br><br>We also noted that only the fleet management plan had identified a Maximum Tolerable Period of Disruption (MTPD) and there were only two plans that had identified a Recovery Time Objective (RTO) with the fleet management plan also quantifying the resources required to achieve RTO's. The Control BIA did not include and MTPD or RTO, and did not quantify the resources required to achieve the RTO.<br><br>If a maximum tolerable period of disruption and recovery time objectives with resources required to achieve these are not identified, there is a risk that the authority will be unable to adequately maintain critical activities at an acceptable level during an adverse event. | | Time Objectives and the resources required to achieve these for critical activities and incorporate these into all Business Continuity Plans. |
| 1.3 | Business Continuity Plans are in place relating to industrial action, fleet management, and control. Stations have prepared basic contingency documents, but no formal continuity plans. | No | N/A | We reviewed three key operational business continuity plans (industrial action, fleet and control) and three station plans to assess whether the design and content were fit for purpose. We noted that the industrial action contingency plan (known as Operation Gian) was an excessively large document with excess verbiage, creating a risk that it is unwieldy to use in practice.<br><br>We noted the plan had not been updated since 2013, and that responsibility for updating the plan had not been clearly documented. Although a communication plan and | High | All Business Continuity Plans will be updated annually by the plan owners. This will include input from the Risk and Business Continuity Team where appropriate, who will perform a secondary review to ensure Plans are fit for purpose. Plans will include clear actions and timescales for completion, |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Actions for management |
|---|---|---|---|---|---|---|
| | | | | strategy were included, no key contact details were listed in the plan.<br><br>The implementation plan was in a heavily narrative form and it was unclear precisely what actions should be undertaken, or who was formally responsible for undertaking them.<br><br>The plan included no clear analysis of critical activities or corresponding recovery timescales, and hence it was not clear that resources had been appropriately aligned to recovery activities.<br><br>For both the Fleet and Control BCPs, we noted the document authors were identified, but no clear protocols for reviewing and updating the document.<br><br>There was no clear schedule of roles and responsibilities following plan invocation, and although authority for invoking the plan was documented, the circumstances under which invocation should occur were not.<br><br>Resources for the recovery of critical activities were listed out, but no clear process 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.<br><br>The Fleet BCP also included a high-level communication strategy, but had a lack of specific communication activities to be undertaken.<br><br>We noted the Control BCP was heavily out of date, being last reviewed in 2012.<br><br>We confirmed in discussion with the Control Room Manager that it was not usable in its current form and that work was being undertaken with the Risk and Business Continuity Team to revise it. | | including details of those responsible for completing the actions. |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Actions for management |
|---|---|---|---|---|---|---|
| | | | | We confirmed that the industrial action, Control and Fleet BCPs were all explicitly aligned to the Civil Contingencies Act 2004.<br><br>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 not managed effectively. | | |
| 1.4 | 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.<br><br>As a consequence, there is no process in place for formally identifying, recording and actioning lessons learned. | No | N/A | In discussion with the Corporate Risk and Business Continuity Manager, exercising of operational business continuity plans is the responsibility of the relevant departments.<br><br>It was noted that there is no formal programme in place at the corporate or departmental levels for exercising business continuity plans.<br><br>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.<br><br>Without a formal programme of exercising business 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. | High | Once adequate BCPs are in place, a formal testing programme will be established for testing the plans at appropriate intervals.<br><br>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. |
| 1.5 | The Service Leadership Team (SLT) assists Essex Fire Authority to meet their responsibilities to establish and oversee the corporate governance arrangements of the Service. | Yes | N/A | 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.<br><br>We also confirmed that they recorded a quarterly standing | High | The Service Leadership Team will challenge the Risk and Business Continuity Team regarding the status of and progress against business continuity management, raising |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Actions for management |
|---|---|---|---|---|---|---|
| | The SLT is responsible for reviewing, monitoring and ensuring effective management of business continuity arrangements.<br><br>A standing quarterly agenda item is documented in the Team's terms of reference for receiving updates on Corporate Risk and Business Continuity. | | | agenda update on corporate risk and business continuity.<br><br>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.<br><br>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. | | appropriate actions to address weak areas, and following these through to completion. 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 and approving 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 | 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.<br><br>It was noted that this would be the responsibility of the relevant head of department.<br><br>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 | High | The Authority will implement a clear and formal process for the review of third-party BCPs, and gain frequent assurance regarding their effectiveness. |

# 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 | 100% | |
| Reasonable assurance | - | |
| Partial assurance | - | X |
| No assurance | - | |
| **Management actions** | **Average number in similar audits** | **Number in this audit** |
| | 2 | 7 |

# FOR FURTHER INFORMATION CONTACT

Suzanne Rowlett – Senior Manager

Suzanne.Rowlett@rsmuk.com

07720 508148