

|  |
| --- |
| **The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police** |
| **Assurance Review of ICT Business Continuity**  **2017/18** |

|  |
| --- |
| **Executive Summary** |

|  |  |
| --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** | **OVERALL CONCLUSION** |
|  | **Cleveland Police were found to demonstrate a good level of awareness and understanding of ICT Business Continuity risk and issues, and this was supported by detailed ICT continuity plans and supporting documentation.**  **It was also noted that there were several exercises ongoing at time of audit to further strengthen the Forces ICT Business Continuity controls.**  **Two key issues identified were as follows;**   * **There is no regularly scheduled/ annual testing of the ability to recover key ICT systems and services currently undertaken;** * **There are currently no test plans currently in place describing the detailed processes and procedures to be followed when testing the ability to recover key ICT systems and services.**   **These risks are mitigated to some extent by the fact ICT have been able to test the ability to recover some systems and services in BAU.** |
| **SCOPE** | **ACTION POINTS** |
| The objective of the audit was to assess the adequacy and effectiveness of the internal controls in place for managing the ICT business continuity (BC) process and ensuring that the Force’s systems and services are resilient to disruptive events that may impact upon the organisation. | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **0** | **2** | **0** | **3** | |

|  |
| --- |
| **Management Action Plan – Priority 1, 2 and 3 Recommendations** |

| **Rec.** | **Risk Area** | **Finding** | **Recommendation** | **Priority** | **Management**  **Comments** | **Implementation**  **Timetable**  **(dd/mm/yy)** | **Responsible**  **Officer**  **(Job Title)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | Compliance | There is no regularly scheduled/ annual testing of the ability to recover key ICT systems and services currently undertaken.  As a result there is limited assurance around the timescales within which key systems and services can be restored in the event of a DR scenario. | ICT to liaise with key business stakeholders within the Force to agree an approach to the regular testing of key ICT systems and services. | 2 | *A meeting has been arranged for June 6th to discuss the actions and timescales for implementation. A further update to how this finding will be remediated will be issued after this meeting.* | *TBC* | *TBC* |
| 3 | Compliance | As there is no scheduled testing for key ICT systems and services, there are currently no test plans currently in place describing the detailed processes and procedures to be followed when testing the ability to recover key ICT systems and services. | Test plans for key systems be produced detailing the approach to testing. Test results be documented as part of a formal test report which details test objectives, outcomes, and lessons learned. This can then be used in updating the associated DR plans and supporting documents. | 2 | *A meeting has been arranged for June 6th to discuss the actions and timescales for implementation. A further update to how this finding will be remediated will be issued after this meeting.* | *TBC* | *TBC* |

|  |
| --- |
| **Operational Effectiveness Action Plan** |

| **Ref** | **Risk Area** | **Item** | **Management**  **Comments** |
| --- | --- | --- | --- |
| 1 | Compliance | ICT management to consider whether there is a need for Business Continuity training within ICT following the exercise to document and perform regular DR testing exercises. | *A meeting has been arranged for June 6th to discuss the actions and timescales for implementation. A further update to how this finding will be remediated will be issued after this meeting.* |
| 2 | Operational | ICT to liaise with BCP management in order to share knowledge about systems where necessary and ensure the completion of the ICT Service Catalogue. | *A meeting has been arranged for June 6th to discuss the actions and timescales for implementation. A further update to how this finding will be remediated will be issued after this meeting.* |
| 3 | Operational | Management to consider updating BC documentation to show both Force and ICT recovery targets for each key system to provide improved visibility and assurance that these are appropriately aligned. | *A meeting has been arranged for June 6th to discuss the actions and timescales for implementation. A further update to how this finding will be remediated will be issued after this meeting.* |

|  |
| --- |
| **Detailed Findings** |

**INTRODUCTION**

1. This review was completed in March 2018 as part of the planned internal audit work for 2017/18. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

**KEY FINDINGS & ACTION POINTS**

1. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

**SCOPE AND LIMITATIONS OF THE REVIEW**

1. The objective of the audit was to assess the adequacy and effectiveness of the internal controls in place for managing the ICT business continuity (BC) process and ensuring that the Force’s systems and services are resilient to disruptive events that may impact upon the organisation.

The audit focussed on the following key areas:

* Business continuity risks are documented and have action plans to mitigate risk;
* Appropriate ICT business continuity plans are in place, regularly reviewed and readily accessible to staff;
* Business impact assessments are completed on a regular basis;
* Critical systems recovery (priorities, dependencies etc.) are known, documented and reasonable;
* Business continuity plans are periodically tested to ensure their effectiveness, with lessons learned being integrated into the planning process;
* Disaster recovery plans are in place, appropriately documented and subject to regular periodic testing.
* Adequate training is provided to staff to ensure they are fully aware and understand their responsibilities in the event of an incident occurring.

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

**MATERIALITY**

1. Business continuity is a key risk for the Force and appropriate plans should be in place and regularly exercised in order to provide assurance business disruptions can be appropriately managed. Business continuity planning is a fundamental requirement for a Category 1 responder under the Civil Contingencies Act 2004.

**DISCLAIMER**

1. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

**RISK AREA ASSURANCE ASSESSMENTS**

1. The definitions of the assurance assessments are:

|  |  |
| --- | --- |
| **Substantial Assurance** | There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved. |
| **Reasonable Assurance** | The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved. |
| **Limited Assurance** | The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved. |
| **No Assurance** | There is a fundamental breakdown or absence of core internal controls requiring immediate action. |

**ACKNOWLEDGEMENT**

1. We would like to thank staff for their co-operation and assistance during the course of our work.

**RELEASE OF REPORT**

1. The table below sets out the history of this report.

|  |  |
| --- | --- |
| **Date draft report issued:** | 29th March 2018 |
| **Date management responses received:** | 9th May 2018 |
| **Date final report issued:** | 10th May 2018 |

1. The following matters were identified in reviewing the Key Risk Control Objective:

|  |
| --- |
| **Directed Risk: Failure to direct the process through approved policy & procedures.** |

* 1. Key ICT policies and procedures relating to ICT business continuity (BC) were identified and obtained during the course of the audit. These were used in the process of reviewing the suitability of the controls in place around ICT business continuity. The policies identified as being of particular relevance in this review are the; ‘Business Continuity Management Force Plan and Guidance’, ‘ICT Disaster Recovery Plan’, ‘Business Continuity Plan Network and Telecoms’, and the ‘Business Continuity Plan Mobile Devices and Radio’ documents.
  2. The ‘Business Continuity Management Force Plan and Guidance’ describes the Force’s high level approach to ensuring compliance with the statutory duties required by the Civil Contingencies Act 2004, assuring the maintenance of critical services and activities during periods of major disruption and organisational change. It was noted that this plan was in draft stage at the time of review as there was some work still required on the classification and prioritisation of particular key services and systems.
  3. ICT BC plans are invoked in the event of a significant disruption that results in the total or partial loss of the workplace, personnel or power. Review of the two key BC plans relating to ICT services found that they followed the standard format used for BC plans across the Force and contained the expected level of detail including;
* Definition of key roles and responsibilities;
* Invocation procedures;
* Actions and short term mitigating plans required to ensure the continuity of services;
* Prioritisation of services and the required recovery timescales, and;
* Associated templates and documents to be used in the event of an invocation.
  1. Policies and procedures are made available to staff via the Force Sharepoint site, including BCP and DR documentation ensuring that the documentation is available from multiple locations and channels in the event it is required.
  2. A partnership risk forum meeting is held on quarterly basis to review and consider ICT risks including disruptions to services, and business continuity risks. Risks are managed via the use of strategic and operation risk registers with business continuity management reporting risks to the Audit Committee. Regular reports are made to the Operations Board of the Force to update on and approve business continuity plans.

|  |
| --- |
| **Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.** |

* 1. It was noted during the review that due to the fact that ICT services are provided via the partnership with Sopra Steria there are differences in approach between the management and documentation of ICT BCP activities and business BCP activities managed by the Force. It is the intention of the partnership to move towards a more standardised approach over time.
  2. It was also noted that, while there are documented recovery timescales in place for all key services, there was an exercise ongoing at the time of audit to review these in order to ensure they are appropriate and that key services are appropriately classified and prioritised according to risk.
  3. The ‘ICT Disaster Recovery Plan’ document describes the high level approach to the recovery systems and services and details all key IT systems, linking to more detailed DR procedures for each key system where necessary. Systems are categorised according to the priority to be used when recovering the system. Categories and recovery timescales are as follows; Core Critical = 0-2 hours, Category 1 = 0 – 6 hours, Category 2 = within 24 hours, Category 3 = within 5 business days.
  4. There is no regularly scheduled/ annual testing of the ability to recover key ICT systems and services currently undertaken by ICT. As a result there is limited assurance around the timescales within which key systems and services can be restored in the event of a DR scenario, other than that provided when there is a need to restore data as a result of an actual failure/ issue.

|  |  |
| --- | --- |
| **Recommendation: 2** | **Priority: 2** |
| **ICT to liaise with key business stakeholders within the Force to agree an approach to the regular testing of key ICT systems and services.** | |

* 1. As there is no scheduled testing for key ICT systems and services, there are currently no test plans currently in place describing the detailed processes and procedures to be followed when testing the ability to recover key ICT systems and services.

|  |  |
| --- | --- |
| **Recommendation: 3** | **Priority: 2** |
| **Test plans for key systems be produced detailing the approach to testing. Test results be documented as part of a formal test report which details test objectives, outcomes, and lessons learned. This can then be used in updating the associated DR plans and supporting documents.** | |

* 1. It was reported that that there has been no recent training of ICT staff specifically in Business Continuity issues, though it was noted that if regular test exercises were undertaken (as recommended in Recommendation 1) this would provide the opportunity for staff to familiarise themselves with the required processes and procedures.
  2. It is understood the Business Continuity team has recently arranged training exercises for Business Continuity Champions and Authorisers within the Force. It is suggested that as and when further training sessions are held, management consider if there are any ICT representatives that would benefit from the training.

|  |
| --- |
| **Operational Effectiveness Matter: 1** |
| **ICT management to consider whether there is a need for Business Continuity training within ICT following the exercise to document and perform regular DR testing exercises.** |

|  |
| --- |
| **Operational Risk: Failure to identify opportunities to operate more efficiently or to be prepared for forthcoming changes.** |

* 1. It was noted in discussion with ICT management that there was some further work required on the ICT Service Catalogue to ensure that it is comprehensive and that it fully documents the required relationships and interdependencies between systems and that work to address this was ongoing at the time of audit.

|  |
| --- |
| **Operational Effectiveness Matter: 2** |
| **ICT to liaise with BCP management in order to share knowledge about systems where necessary and ensure the completion of the ICT Service Catalogue.** |

* 1. It was noted during review of ‘Business Continuity Management Force Plan and Guidance’ document and supporting documents that, though the documents detail the timescale the Force considers services should be recovered within, it does not cross reference or refer to the service recovery timescales that ICT report they are able to recover systems within. It is suggested that management considers including this information to the plan in order to provide improved assurance and visibility that the Force targets and ICT recovery timescales are aligned.

|  |
| --- |
| **Operational Effectiveness Matter: 3** |
| **Management to consider updating documentation to show both Force and ICT recovery targets for each key system to provide improved visibility and assurance that these are appropriately aligned.** |