



**Police and Crime Commissioners for Norfolk and Suffolk and Chief Constables of Norfolk and Suffolk Constabularies**

**Suffolk Internal Audit Progress Report**

**September 2016**

**INTRODUCTION**

1. This summary report provides an update on the progress of our work at the Police and Crime Commissioners for Norfolk and Suffolk and Chief Constables of Norfolk and Suffolk Constabularies as at 13<sup>th</sup> September 2016. The report is based on internal audit work carried out by TIAA and management representations that have been received during the period since our last progress report.

**PROGRESS AGAINST THE 2016/17 ANNUAL PLAN**

2. Our progress against the Annual Plans for 2016/17 is set out in Appendix A. The results of these reviews are summarised at Appendix B.

**AUDITS CARRIED OUT SINCE THE PREVIOUS PROGRESS REPORT**

3. The table below sets out details of audits carried out since the previous meeting of the Audit Committee.

| Review                       | Evaluation  | Key Dates    |                    |              | Number of Recommendations |   |   |     |
|------------------------------|-------------|--------------|--------------------|--------------|---------------------------|---|---|-----|
|                              |             | Draft issued | Responses Received | Final issued | 1                         | 2 | 3 | OEM |
| Transport                    | Reasonable  | 21/06/2016   | 26/06/2016         | 27/06/2016   | 0                         | 4 | 2 | 0   |
| Corporate Communications     | Reasonable  | 14/06/2016   | 31/08/2016         | 02/09/2016   | 0                         | 4 | 3 | 5   |
| FoI / DP / Document Security | Reasonable  | 26/07/2016   | 23/08/2016         | 31/08/2016   | 0                         | 0 | 8 | 2   |
| Firewalls                    | Substantial | 09/06/2016   | 09/08/2016         | 09/08/2016   | 0                         | 0 | 0 | 0   |
| ICT – Disaster Recovery      | Reasonable  | 26/07/2016   | 10/08/2016         | 10/08/2016   | 0                         | 4 | 1 | 1   |

OEM = Operational Effectiveness Matters

Summaries of the finalised reports are attached at Appendix B. Full reports are available to Audit Committee Members on request. The details for Norfolk only reports will not be included in the Suffolk progress report.

#### **CHANGES TO THE ANNUAL PLAN 2016/17**

4. There have been the following changes made to the annual plan:

- The risk management and governance audits have been brought together to be undertaken as one audit with the assurance framework. This will provide some efficiencies in days, to be transferred to contingency.
- Timing of audits across the year have changed, to coincide with operational requirements.
- The network element of the network and social media audit has been combined with corporate communications, with the social media elements not being undertaken. This is due to the level of IT coverage within this element between both audits being combined with the systems audit and changes within the department.

#### **FRAUDS/IRREGULARITIES**

5. We have not been advised of any frauds or irregularities in the period since the last summary report was issued.

#### **LIAISON**

6. Liaison with external audit: We have liaised with EY during the year and kept them informed of our work and will make available to them all final audit reports. Liaison with the Chief Finance Officers: Regular progress meetings are held with the Chief Finance Officers.

#### **PROGRESS ACTIONING URGENT and NOT APPROVED RECOMMENDATIONS**

7. We have made no urgent recommendation (i.e. fundamental control issues on which action should be taken immediately) since the previous Progress Report.

8. We have made no recommendations which have not been approved by management since the previous Progress Report.

**RESPONSIBILITY/DISCLAIMER**

9. 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. The matters raised in this report not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. 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.

## Progress against the Annual Plan for 2016/17

| System   | Planned Quarter | Planned Days | Actual Days | Current Status                                      | Expected Audit Committee | Comments  |
|--|-----------------|--------------|-------------|---|--------------------------|---|
| Transport Services   | 1               | 15           | 15          | Final report issued                                 | September 2016           |   |
| Corporate Communications / Network   | 1               | 12           | 16          | Final report issued                                 | September 2016           | Network aspects covered within Corporate Communications, 4 days moved from ICT Network / Social Media             |
| HR Recruitment   | 1               | 12           | 12          | Draft report issued 13 <sup>th</sup> September 2016 | December 2016            |   |
| Duty Management System   | 1               | 15           | 15          | Draft report issued 13 <sup>th</sup> September 2016 | December 2016            |   |
| FoI / DP / Document Security   | 1               | 15           | 15          | Final report issued                                 | September 2016           | Audit commencing 27 <sup>th</sup> June 2016   |
| ICT – Firewall   | 1               | 12           | 12          | Final report issued                                 | September 2016           |   |
| ICT – Network / Social Media   | 2               | 12           | -           | Complete  | n/a                      | Social Media aspects within Corporate Communications due to areas now within the same management responsibilities |
| Assurance Framework / Risk Strategy and Policy / Mitigating Controls Verification / Strategic Control and Corporate Governance | 2               | 35           |             | Scheduled   | March 2017               | Combined areas into one audit   |
| Overtime, Expenses and Additional Payments   | 2               | 16           | 6           | Scheduled   | March 2017               | Scheduled for November 2016   |
| Firearms Management  | 2               | 12           | 11          | In progress   | December 2016            |   |
| Estates – Duty of Care / Cost Allocations  | 2               | 12           |             | Scheduled   | December 2016            | Scheduled for October 2016  |
| Estates – Facilities (Catering – Suffolk)  | 2               | 6            |             | Draft report issued 12 <sup>th</sup> September 2016 | December 2016            |   |
| ICT – Disaster Recovery  | 2               | 12           |             | Final report issued                                 | September 2016           |   |
| Performance Management   | 3               | 15           |             | Scheduled   | March 2017               | Scheduled for November 2016   |

| System                                | Planned Quarter | Planned Days | Actual Days | Current Status  | Expected Audit Committee | Comments  |
|---------------------------------------|-----------------|--------------|-------------|-----------------|--------------------------|---|
| Purchase Cards                        | 2               | 12           | 2           | In progress     | December 2016            |   |
| Budgetary Control                     | 3               | 12           |             | Scheduled       | December 2016            | Scheduled for October 2016  |
| Pensions Administration               | 3               | 10           |             | Scheduled       | March 2017               | Scheduled for October 2016  |
| HR – Strategy & Workforce Planning    | 3               | 10           |             | Scheduled       | December 2016            | Scheduled for October 2016  |
| Complaints                            | 4               | 10           |             | To be scheduled | June 2017                | Moved from Q1 due to timing of the change in rules in November 2016 |
| Collaborations                        | 4               | 10           |             | To be scheduled | March 2017               |   |
| ICT – Exchange 2010 / Email Archiving | 4               | 12           |             | Scheduled       | June 2017                | Scheduled for February 2017   |
| ICT – ERP Second / Third Line Support | 4               | 12           |             | Scheduled       | March 2017               | Scheduled for January 2017  |
| Key Financial Controls                | 4               | 30           |             | To be scheduled | March 2017               |   |
| Payroll                               | 4               | 10           |             | Scheduled       | March 2017               |   |
| Estates – Maintenance and Repair      | 4               | 12           |             | To be scheduled | June 2017                |   |
| Commissioners Grants (Norfolk)        | 4               | 10           |             | To be scheduled | June 2017                |   |
| Follow Up Work                        | 2 / 4           | 10           | 5           | Ongoing         |                          | Year-end reporting June 2016 / mid-year reporting                   |
| Contingency                           | 1-4             | 18           |             | As required     |                          | Possibility bring forward Lone Working or Safeguarding from 2018/19 |
| Audit Management                      | 1-4             | 20           | 10          | Ongoing         |                          |   |
| <b>Total Days</b>                     | -               | <b>399</b>   | <b>119</b>  |                 |                          |   |


KEY:

|  |   |                     |
|--|---|---------------------|
|  | = | To be commenced     |
|  | = | Site work commenced |
|  | = | Draft report issued |
|  | = | Final report issued |

## Summaries of Finalised Audit Reports issued since the last report

### Audit Report: NSC1703 Transport Services

Report Issued: 27<sup>th</sup> June 2016

| <p><b>SCOPE</b></p> <p>The review considered the systems, controls and processes around the maintenance and repair of vehicles and the usage of fuel.</p> <p><b>MATERIALITY</b></p> <p>Total spend in 2015/16 was £2.4m. Budget information provided by the Head of Transport confirmed that the department was overall £66,323 underspent.</p> <p>There are 1021 cars within the fleet. In 2015/16 128 vehicles were disposed of, with a value of £145,317.47. Currently in 2016/17, seven have been disposed of, to a value of £8,312.50.</p> | <p><b>KEY FINDINGS</b></p> <ul style="list-style-type: none"> <li>• A Joint Transport Strategy has been produced and approved. A Joint Transport Policy supports this document. Standard operating procedures are in the process of being updated following staffing changes.</li> <li>• Testing of disposal, servicing and maintenance proved satisfactory.</li> <li>• Testing of issuing of fuel cards proved satisfactory.</li> <li>• Fuel Card usage is monitored and reported on a monthly basis by Allstar.</li> <li>• Recommendations made relate to the publication of strategy on both websites, the document approval process, vehicles exceeding maximum mileage/age, de-commissioning forms, standardising weekly vehicle checks forms and process for monitoring completion.</li> </ul> |         |             |         |             |   |   |   |   |
|---|--|---------|-------------|---------|-------------|---|---|---|---|
| <p><b>OVERALL ASSURANCE ASSESSMENT</b></p>   | <p><b>ACTION POINTS</b></p> <table border="1" data-bbox="1131 1077 2011 1236"> <thead> <tr> <th>Urgent</th> <th>Important</th> <th>Routine</th> <th>Operational</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>4</td> <td>2</td> <td>0</td> </tr> </tbody> </table>   | Urgent  | Important   | Routine | Operational | 0 | 4 | 2 | 0 |
| Urgent  | Important  | Routine | Operational |         |             |   |   |   |   |
| 0   | 4  | 2       | 0           |         |             |   |   |   |   |

**Recommendations – Urgent (Priority 1), Important (Priority 2) and Not Approved**

| Report Ref | Risk Area | Finding   | Recommendation  | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|-----------|---|---|----------|--|-------------------------------------|---------------------------------|
| 2          | Directed  | The Joint Transport Strategy is supported by the Joint Transport Policy, including security of Constabulary vehicles V6. This was reviewed as part of the audit and it can be confirmed that there is no date for the document or approval process recorded within it. There is an index of operating procedures which has recently been prepared as a result of the reorganisation of the department. At the time of the audit these had not been fully completed. | The Joint Transport Policy be subject to document control and approval process and current operating procedures should be updated and maintained. | 2        | <p><i>Joint Transport Policy Force Policy Officer, Corporate Development and Change to be consulted regarding document control and approval process. It should be noted this is a Transport Services only Policy as it was determined the Policy was more aligned to a standard operating procedure.</i></p> <p><i>The standard operating procedures are in the process of being updated to reflect T13 restructure and process changes.</i></p> | 31/10/16                            | Head of Transport               |



| Report Ref | Risk Area  | Finding  | Recommendation   | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|------------|--|--|----------|--|-------------------------------------|---------------------------------|
| 3          | Compliance | A download from the Tranman database provided details of both the current mileage of the vehicle and its age. A review of this data confirmed that there are 1021 cars within the fleet. Of these, 55 are above the replacement mileage as stated in the Joint Transport Strategy and a further 183 are over their maximum age. The Head of Transport Services confirmed that each vehicle is reviewed once it reaches either the maximum mileage or age and a decision is made on whether to retain the vehicle or dispose of it. Evidence of this decision and the approval of the Head of Transport Services is not recorded in these cases on Tranman and therefore no record is held to support the vehicles not complying with the Joint Transport Strategy. | Decisions made on vehicles that have exceeded the maximum mileage or age as detailed in the Joint Transport Strategy be noted on Tranman and approved by the Head of Transport Services. | 2        | <i>The Head of Transport determines whether a vehicle will be retained over and above the vehicle replacement criteria for the role. This is determined by a number of factors such as condition, use, and available budget. Vehicles are considered on an individual basis. Vehicles are retained following replacement for specific operations etc. on a temporary basis. Vehicles highlighted for replacement by Tranman are exported to a replacement report where this information is detailed. A field will be created on Tranman that details this information.</i> | 31/07/16                            | Head of Transport               |

| Report Ref | Risk Area  | Finding  | Recommendation  | Priority | Management Comments   | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|------------|--|---|----------|---|-------------------------------------|---------------------------------|
| 5          | Compliance | Weekly vehicle checks were discussed with the Head of Transport, who confirmed that there are different systems operating within Suffolk and Norfolk. Within Suffolk there are currently four different vehicle inventory forms in use. Within Norfolk there is one form in use. Whilst the forms are broadly similar it doesn't provide a consistent approach across that two counties. | The weekly vehicle check form be standardised across both counties. | 2        | <i>Within Norfolk weekly check sheets fall under the remit of the Driver of Police Vehicles Force Policy Document, with the Policy owner being Specialist Operations. Within Suffolk the remit is with the County Policing Command. Norfolk and Suffolk Constabularies are aligning their equipment levels and types. This will then allow the use of one form across both Counties. This is already in progress and will be managed through the Transport Strategic Group.</i> | 31/12/16                            | <i>Head of Transport</i>        |

| Report Ref | Risk Area  | Finding   | Recommendation  | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|------------|---|---|----------|--|-------------------------------------|---------------------------------|
| 6          | Compliance | Drivers are required to provide copies of the weekly checklist to their local station. These are usually completed on a Sunday. Records of checks completed are maintained within the local station, although the system is different depending upon the local station. Evidence was provided from staff across both Suffolk and Norfolk, which illustrated that weekly checks are being undertaken and results are being recorded and monitored within local stations, however the system isn't standardised and there is no central reporting to ensure that there is an overview of the process, in order to identify any areas that are not meeting expectations. | The system for recording and monitoring the completion of the weekly vehicle checks be standardised and a system for central oversight of the results of the checks be implemented. | 2        | <i>There is scope for the central reporting hub to be Transport services. This will be progressed through the Transport Strategic Group.</i> | 31/12/16                            | <i>Head of Transport</i>        |

**Audit Report: NSC1704 Corporate Communications**

**Report Issued: 2<sup>nd</sup> September 2016**

**SCOPE**

The review considered the handling of internal and external communications, including social media. The constabulary websites were excluded from the scope as these are under review and will be covered by a subsequent internal audit review.

**MATERIALITY**

Communications are essential for the purposes of keeping staff and the public informed of crimes, operations and initiatives.

**KEY FINDINGS**

- There is a Digital Strategy 2015-18 which sets out the importance of social media and an objective to expand the use of this.
- There is currently no formal Corporate Communications Strategy or Policy.
- The Corporate Communications Teams carry the risk of reliance on the experience of key individuals, with a lack of written protocols.
- Internal and external communications are undertaken through a variety of channels, including wide use of social media.
- Social media usage is monitored and reported, although the effectiveness of communication is an area for development.

**OVERALL ASSURANCE ASSESSMENT**



**ACTION POINTS**

| Urgent | Important | Routine | Operational |
|--------|-----------|---------|-------------|
| 0      | 4         | 3       | 5           |

**Recommendations – Urgent (Priority 1), Important (Priority 2) and Not Approved**

| Report Ref | Risk Area | Finding  | Recommendation  | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title)                           |
|------------|-----------|--|---|----------|--|-------------------------------------|---|
| 1          | Directed  | There is currently no corporate communications strategy.   | A corporate communications strategy be developed and embedded, aligned with the visions of the Norfolk and Suffolk Constabularies.  | 2        | <i>A communications strategy will emerge over the next six months. Revised Police and Crime Plans for both forces are awaited: these will form a central element of an effective strategy.</i> | 31/03/17                            | Head of Corporate Communications                          |
| 2          | Directed  | There are currently no formal communications policies.   | Corporate communications policies be developed and embedded. Appropriate review periods be set for each policy.   | 2        | <i>Formal policies on specific areas (for example Social Media) are being developed on an ad hoc basis. This will be ongoing, with a date of 31/03/17 set for review.</i>                      | 31/03/17                            | Head of Corporate Communications                          |
| 3          | Directed  | The audit identified a lack of written protocols in the communications teams. This is especially a risk given the reliance on the experience of key individuals. | Written protocols be prepared to cover the roles within the Corporate Communications teams, with appropriate references to College of Policing guidance, media law and best practice. | 2        | <i>A series of communications protocols are being developed covering the core areas of the department's activities.</i>  | 31/03/17                            | Head of Corporate Communications, Communications Managers |

| Report Ref | Risk Area  | Finding   | Recommendation   | Priority | Management Comments   | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title)  |
|------------|------------|---|--|----------|---|-------------------------------------|--|
| 4          | Compliance | In addition to the corporate Twitter accounts, there are a large number of district, department / unit and individual Twitter accounts. Staff are encouraged to arrange for individual accounts to be set up and to access to existing accounts. The audit was unable to identify whether a risk assessment had taken place in respect of this. | A risk assessment be undertaken in respect of the wide access granted to Twitter accounts. | 2        | <i>A policy decision was made at Chief Officer level to offer accounts to individual officers and staff, and it seems unlikely that this decision will or should be revisited. The value of a formal risk assessment is therefore limited, but a constant overview of social media is maintained to identify and mitigate risk and to promote good practice via training. This will be ongoing, with a date of 31/12/16 set for review.</i> | 31/12/16                            | <i>Head of Corporate Communications, Digital Media Team, Communications Managers</i> |

**Audit Report: NSC1708 FoI, Data Protection, Document Security**

**Report Issued: 2<sup>nd</sup> September 2016**

**SCOPE**

The review considered the effectiveness of managing freedom of information requests, data protection and document security. The scope did not include incident management, cyber security or records management compliance, as these are subject to separate reviews.

**MATERIALITY**

It is crucial to protect information in order to provide effective policing. It is a legal requirement to comply with the Data Protection Act 1998 and the Freedom of Information Act 2000.

**KEY FINDINGS**

- There is a sound governance and risk management structure in place, overseen by the Information Management Steering Group (IMSG).
- There is a suite of information management policies in place. Many are under review and this is being overseen by the IMSG.
- Subject access requests and Freedom of Information disclosures are well documented, authorised and generally timely.
- Testing of Information Sharing Agreements found some issues around central recording, authorisation and review.
- System access audit is documented, although recent Police National Database (PND) audit had not been carried out at the time of this audit.

**OVERALL ASSURANCE ASSESSMENT**



**ACTION POINTS**

| Urgent | Important | Routine | Operational |
|--------|-----------|---------|-------------|
| 0      | 0         | 8       | 2           |

**Audit Report: NSC1704 Corporate Communications**

**Report Issued: 2<sup>nd</sup> September 2016**

**SCOPE**

The review has considered the effectiveness of the controls in place around the management of firewall appliances. The firewall appliances are all CISCO appliances and are currently undergoing a tech refresh to replace older appliances in Mission Critical and Business Critical order. The CISCO ASA 5505 devices are being replaced with ASA 5506X and the ASA 5510s are being replaced with ASA5512x appliances.

**MATERIALITY**

Robust management of firewall appliances is critical to helping to ensure the security of the ICT network and the data hosted therein.

**KEY FINDINGS**

- Example testing indicated that the firewall infrastructure is being managed adequately and effectively.
- Older firewall appliances are currently being replaced to remain compliant with PSNP requirements.
- The Intrusion Prevention system is being replaced by FireSIGHT, with related business procedures being updated to take account of the change.
- Mission-critical and certain business-critical systems are protected by a resilient firewall infrastructure.

**OVERALL ASSURANCE ASSESSMENT**




**ACTION POINTS**

| Urgent | Important | Routine | Operational |
|--------|-----------|---------|-------------|
| 0      | 0         | 0       | 0           |



**Audit Report: NSC1712 Disaster Recovery**

**Report Issued: 10<sup>th</sup> August 2016**

| <p><b>SCOPE</b></p> <p>The review considered the effectiveness of the controls in place around ICT Disaster Recovery.</p> <p><b>MATERIALITY</b></p> <p>Norfolk and Suffolk Constabularies provide an emergency service to the public in the region and elsewhere on a 24 hour basis, which requires a resilient Mission-critical IT infrastructure to support.</p> | <p><b>KEY FINDINGS</b></p> <ul style="list-style-type: none"> <li>• The Physical and Environmental security of the equipment rooms at the Operations &amp; Communications Centre and Dereham Police Station were generally found to be adequate, with some suggestions for minor enhancements having been made.</li> <li>• Mission-Critical services are being adequately targeted for priority IT support.</li> <li>• Testing of the Backup processes proved adequate.</li> <li>• Recommendations made relate to the need to review the document set that makes up the Disaster Recovery readiness plans, conducting physical Disaster Recovery tests, servicing the manual fire extinguisher in Dereham, changing door lock key codes and installing webcams in the Dereham equipment rooms.</li> </ul> |         |             |         |             |   |   |   |   |
|--|---|---------|-------------|---------|-------------|---|---|---|---|
| <p><b>OVERALL ASSURANCE ASSESSMENT</b></p>    | <p><b>ACTION POINTS</b></p> <table border="1" data-bbox="1131 778 2011 938"> <thead> <tr> <th>Urgent</th> <th>Important</th> <th>Routine</th> <th>Operational</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>4</td> <td>1</td> <td>1</td> </tr> </tbody> </table>  | Urgent  | Important   | Routine | Operational | 0 | 4 | 1 | 1 |
| Urgent   | Important   | Routine | Operational |         |             |   |   |   |   |
| 0  | 4   | 1       | 1           |         |             |   |   |   |   |

**Recommendations – Urgent (Priority 1), Important (Priority 2) and Not Approved**

| Report Ref | Risk Area | Finding | Recommendation | Priority | Management Comments | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|-----------|---------|----------------|----------|---------------------|-------------------------------------|---------------------------------|
|------------|-----------|---------|----------------|----------|---------------------|-------------------------------------|---------------------------------|

| Report Ref | Risk Area | Finding  | Recommendation  | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title)          |
|------------|-----------|--|---|----------|--|-------------------------------------|--|
| 1          | Directed  | <p>Disaster Recovery plans are comprised of a range of separate procedure documents that cover different aspects of Disaster Recovery in place. For example, there is an Emergency 24x7 Support process, ICT Substantial Loss of Staff procedure and an ICT Major Incident procedure. The documents have all received relatively recent review, although there are discrepancies between review dates recorded in version histories and within the headers of the documents.</p> <p>The audit also noted that there are duplications across the document set. An example of this is roles &amp; responsibilities.</p> <p>The document set requires review to rationalise the document set to remove duplications and to take account of a recent major restructure within the department that may affect roles and responsibilities.</p> | <p>Documents making up the IT Disaster Recovery response all require review to ensure that they are all aligned and that review dates match where required. Review also required to take account of a recent major restructure within the IT department and include 3rd party vendor contact details and key SLA requirements for each. The framework of documents also overlap in terms of content. Hence the review should also attempt to rationalise the number of documents. Once the review is completed, ensure that all offline copies are updated. For example, copies issued to senior managers and the hard copies contained within the red folders at both ends of the IT department.</p> | 2        | <p><i>Documentation to be reviewed, rationalised and re worked to address the recommendations.</i></p> | 30/11/16                            | <p><i>Process and Policy Manager</i></p> |

| Report Ref | Risk Area  | Finding  | Recommendation   | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|------------|--|--|----------|--|-------------------------------------|---------------------------------|
| 2          | Compliance | Mission critical systems are in scope for annual Business Continuity testing. The exercises have been theoretical desktop exercises to date and the IT department have taken part. Physical Disaster Recovery testing has not taken place. An example of a small scale physical Disaster Recovery test could be the removal of an email cluster from the network to understand the ability of the remaining two clusters to continue providing email services with no disruptions. Subsequent physical testing would likely comprise larger scale testing of mission- and Business-critical services as confidence increases. A recommendation to look into the feasibility of planning and conducting physical Disaster Recovery tests and feeding the results back into relevant Disaster Recovery plans, where required, has been raised. Such tests to help provide tangible assurance over the ability of the IT infrastructure to provide seamless support to mission-critical and Business-critical services. | IT Management to work with the business areas to look into the feasibility of conducting regular physical Disaster Recovery Tests, planning these in over time and feeding the results back to the business and relevant Business Continuity and Disaster Recovery Plans as appropriate. | 2        | <i>ICT have previously engaged with the CCR to conduct physical testing but due to the nature of the criticality of the systems the appetite to conduct the testing has been low, however ICT will work with the Business leads to look into the feasibility of the recommendations with a view to planning physical tests should approval by the business be given.</i> | 31/12/16                            | Head of ICT Infrastructure      |

| Report Ref | Risk Area   | Finding  | Recommendation  | Priority | Management Comments  | Implementation Timetable (dd/mm/yy) | Responsible Officer (Job Title) |
|------------|-------------|--|---|----------|--|-------------------------------------|---------------------------------|
| 3          | Operational | Keycodes are used for 2 of the rooms in Dereham. Codes are not changed frequently, although it is acknowledged that there are restrictions on the number of staff with access to the codes and that the Dereham Police Station is staffed 24 hours a day. However, it is considered good practice to change the codes on a regular basis and always after staff with knowledge of the codes have left. | Equipment rooms that are locked using keypad codes should have their codes changed periodically and always after staff with knowledge of the codes have left. Appropriate recordkeeping to log the changes, dates, and signatures should be kept. | 2        | <i>To be implemented in conjunction with Facilities Dept.</i>                                      | 30/09/16                            | Head of ICT Infrastructure      |
| 5          | Operational | All of the built-in fire systems were found to have been serviced within the last year. However, the manual fire extinguisher service log suggests that its last service was undertaken in 2013. A recommendation to look into this has been raised.   | IT Management to work with relevant estates colleagues to understand and resolve the service status of the manual fire extinguisher located in Equipment Room 1 at Dereham Police Station.  | 2        | <i>This has been highlighted to the Head of Estates and will be addressed as soon as possible.</i> | 31/08/16                            | Head of ICT Infrastructure      |