Appendix C

Bolsover, Chesterfield and North East Derbyshire District Councils'

Internal Audit Consortium

Internal Audit Report

Authority:	**Chesterfield Borough Council**
Subject:	**ICT Network Security**
Date of Issue:	**15th November 2017**

Report Distribution:	**Customers commissioning and change Manager (CBC)** **Information Assurance Manager (CBC)** **Client Officer (CBC)** **ICT Projects Manager (Arvato)** **Site Director (Arvato)**

INTERNAL AUDIT REPORT
ICT and E-Government Service

Introduction

A routine review of the Council's IT security and disaster recovery procedures has recently been carried out. It should be noted that this is inclusive of CBC and Arvato responsibilities and hence the recommendations made may require liaison between both parties or may be the sole responsibility of a single party as highlighted in the report and implementation schedules.

Scope and Objectives

The scope and objectives of the audit were to review the controls in place in respect of:

- Action taken on previously agreed recommendations
- Framework and procedures
- Network access controls and security
- Security testing and incident management
- Data transfer
- Protection against malicious software
- Physical security
- Training
- Disaster Recovery
- Insurance
- Public Services Network

Incorporated within the above scope and objectives were compliance with the CESG 10 steps to cyber security publication, these are:

- Information Risk Management Regime
- User Education and Awareness
- Home and Mobile Working
- Secure Configuration
- Removable Media Controls
- Managing User Privileges
- Incident Management
- Monitoring
- Malware Protection
- Network Security

The scope of the audit was restricted to the above areas and reflects the current practises and procedures. It does not incorporate network structure, hardware or the impact of business continuity (which are vulnerabilities that the Council are aware of).

An external review of the ICT network is being undertaken and aims to make further recommendations to address these issues. It may be prudent once this is concluded to utilise specialist consultants to periodically assess the IT infrastructure and associated elements.

Conclusion

It is considered that the current ICT system and procedures provide **Limited Assurance** in respect of network security (Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed). A summary of the assurance levels used from April 2017 are included at Appendix 1

Findings and Recommendations

<u>Previous Audit Recommendations</u>

1. A review of the previous audit recommendations revealed that 9 out of 12 have been completed to a satisfactory level.

2. 2 out of the 3 remaining audit recommendations have been progressed as below:
    - It was recommended that new ICT policies are approved and implemented as the current policies are outdated. New policies have been drafted by the Information Assurance Manager however the new policies have not yet been approved.
    - It was recommended that the new ICT policies include the risks of using personal devices for council data. A review of the draft policies (currently not approved) established that requirements for using your own device (BYOD) are listed in the new policies.

3. 1 out of the 3 remaining audit recommendations had not been progressed
    - It was recommended that a system be brought into place to monitor the transfer of data to unsecure email accounts. The original agreed implementation date was October 2017. So far no progress has been made however this is now to be reviewed as part of the ICT Transformation Project.

Recommendations		
R1	**CBC**	As recommended in the previous audit it is essential that the new draft ICT policies are approved and made available to employees and members as the current policies are outdated, this should include the risks of using personal devices ***(Priority: High)***
R2	**CBC & Arvato**	A system should be implemented to monitor the transfer of data to unsecure email addresses. ***(Priority: Medium)***

4. During the Accounts Payable Audit it was identified that the micro fax system used to fax remittance advice slips out to suppliers was running on an outdated machine (running windows XP, not PSN compliant). It was recommended that this system be replaced. A replacement system, provided by bottomline technologies has been bought and is planned to be implemented by the end of November 2017.

Framework and Policies

5. During the 2014 audit it was recommended that the council's current "use of ICT by employees" policy is reviewed to determine it is still fit for purpose, if it was deemed unfit for purpose a new ICT policy should have been devised.

6. The Council's Policy on the use of ICT by employees and the responsibility for the review and update was not included in the Corporate Services specification for ICT therefore this is responsibility of CBC.

7. It was evidenced during the audit that new ICT policies have been drafted and are waiting to be submitted for approval. **See R1**

Network Access Controls and Security

8. The Council's network can only be accessed by a corporate log on which requires a username and password. Network access is arranged by the ICT department upon completion of a new starters form confirming that they have read and accepted the ICT Policies. Users are only given access to limited areas of the network dependant on their role.

9. User accounts are controlled by secure passwords that are required to be changed on a 60 day cycle. The previous 20 passwords cannot be used and all passwords require specific formats. It was noted in the IT Health check that even though passwords comply with this policy they can still be considered weak passwords (e.g. Orange11 contains Upper case, lower case and numbers however is still a very weak password and is used by 22 user accounts (2.87%))

10. The council have recently received a password checking tool from the NCSC (national Cyber Security Centre). It has been agreed that the council network will be scanned on a monthly basis. This will allow the ICT department to identify weak passwords and contact the user to ensure it is updated with a more secure password. The first scan has been completed on this and the results have been discussed with the Information Assurance Manager.

11. It was established that recently the council has received a grant of £25,000 from NCSC (National Cyber Security Centre) to conduct a case study with the aim of reducing the requirements around passwords including changing passwords on a regular basis and allowing single sign on systems. This case study is being completed by the Information Assurance Manager with aim to be presented to the NCSC in March 2018.

12. Any change of access rights needs to be actioned by the ICT department. For new starters, leavers, movers, and long term absences, there is a form to complete so that access to all the relevant applications can be corrected too. This is the responsibility of the line manager.

13. Individual applications are managed by their respective system administrators. As these are not managed by the ICT department there is no central log to confirm what applications employees have access to. Records of access levels for each system can be obtained by the individual system administrators.

14. Remote Access to the network requires 2 factor authentication as well as requiring specific network certificates (can only be provided by ICT) before access to CBCs Virtual Private Network is granted.

15. Remote log on for anyone other than CBC employees requires the user to contact ICT department to be granted access to the system and given a single use Pass code to enable one off access to the network from a remote location. Remote locations are always checked to ensure they are within the European Economic Area.

16. It is required under data protection to ensure there are measures to prevent unlawful or unauthorised access to personal data. Within the council there are periodical reviews of users with access to the network. Discussions during the audit have identified that these get completed on a monthly basis. Any users that have not accessed the network for over one month have their access placed on hold until the user contacts the ICT department to unlock the account or the ICT department are made aware that the employee has left.

17. When a staff member leaves and their email account is still required the manager can request that the account stays open. Where this is the case the ICT department cannot remove this account without the manager's approval. Reminders are sent annually to managers to check whether the email accounts are still required.

18. Currently the council are in the process of ensuring all unnecessary user accounts are removed with the aim to reduce the number of Microsoft licences being paid for by the council (£21 per year per user account) for staff who do not work for the council but still have open accounts, this is part of the work being completed before Microsoft conduct an audit on the council systems.

19. During the audit it was evidenced that a review of users with administration rights within the council's windows domain system (Initial windows logon for council devices) had been completed on a regular basis

20. It was confirmed during the previous audit that encryption on all of the councils laptops has been completed using the Bitlocker application. Encryption ensures at all data stored within device is not accessible without entering a username and password.

Data Transfer

21. When a user wishes to use data from an external CD or USB memory stick the policy states that user is required to contact ICT to ensure the media is safe to use. This is checked by using a "Sheep Dip" terminal which is not connected to the network. When any media gets tested it is logged within ICTs records. Examination of the "sheep dip" record shows that 32 tests have been completed in 2017.

22. Secure Data Transfer solutions are in place within CBC. A new web form provided by Egress has been created to allow employees and external users to “drop off” documents for collection by the recipient, while the information is held in situe it is securely held by egress. It is not possible to ensure that all data is transferred securely, this is the responsibility of the employee transferring the data however if sensitive data is lost the council could be fined by the ICO for the data breach. It was identified that encryption of emails can be established by configuration of the exchange servers to allow all emails to be secure this is currently in the process of being updated by the ICT department after a change request was submitted in April 2017.

23. It was identified that currently there is no monitoring of emails sent to/recieved from external sources. This means that employees could create sensitive council documentation on a personal device without the security measures needed to protect the data. It also means that employees could send data from corporate email to personal email addresses to allow them to edit council property on personal devices. Even if this data was sent securely there are multiple ways that sensitive data could be lost (E.g. Personal email address gets hacked, personal device is stolen with council data on, personal device gets ransomware). If the data was lost through an attack on the personal account/device the employee would not be required to report this as it is not council property. In November 2017 a charity worker received a conditional discharge for 2 years and a monetary fine for sending sensitive data from his work email account to his personal email account. ICO fines are set to increase as part of the GDPR guidelines from May 2018. **See R1 and R2**

Protection against Malicious Software

24. Sophos End Point Protection is the main protection for the council computers used by employees. This is installed on all computers within the council. A policy is created on Sophos to ensure all versions of Sophos protect the same areas:
    - Anti-virus and Anti-malware protection
    - Adware and Potentially unwanted application protection
    - Application control blocks specific unwanted application from running
    - Device Control blocks the use external devices and allows specific devices (CD drives and USB devices)
    - The end point software is managed centrally by the Sophos Enterprise Console from within the ICT Department
    - The software automatically checks and install updates

25. During the audit it was identified that a computer within the audit office did not have a working version of Sophos Endpoint Protection, this was corrected during the audit and a further review of the Sophos Enterprise Console was completed, the following was established:
    - 15 out 15 computers sampled were running a version of Sophos which had been updated within the last 5 days.

- It was identified that the majority of versions of Sophos were running application control. The machines which were not running the application control scans still stated that Sophos was “up to date with the policy”.
- It was evidenced that there were 244 machines with errors on the Sophos software, these have not been reviewed.
- At the time of the audit there was a total of 96 machines without protection from Sophos across the council, these include printers, scanners and incompatible servers (e.g. Linux). it was established that a review of this list had not been completed recently to ensure that no computers were on the list.
- The only way to establish that a machine is not protected is by a reconciliation of current machines to protected machines. It was established that a reconciliation does not take place
- The management software keeps a record of machines that have missed updates however it was established that a machine that had not been updated since June 2017 was not recorded on this list.

At the time this was discovered the ICT Support Officer raised a help desk call to establish the cause of the issues.

Recommendation		
R3	**Arvato**	A review of the Sophos monitoring procedures should be completed with the aim of ensuring the following are completed on a regular basis • Errors and warnings reviewed and cleared from system • Reconciliation of devices protected to full list of current devices • Ensuring all Sophos protection policies are active and correct ***(Priority: High)***

26. The authority uses Barracuda email filter to act as a gateway between the email server and the internet, This scans for malicious software or code within emails being sent or received.

27. The authority uses Bloxx web filter (which is due to go out of service) and has recently installed Smoothwall web filter as a physical device that acts as gateway between the internet and our PCs and the internet to protect them against malicious software and code.

28. Checkpoint Firewalls were installed in April 2015. This includes an IPS system which provides an extra layer of protection. These are managed by Imerja, who update the software, patches, proactively monitor and fix any issues with the system.

29. Mobile devices such as Smart phones, iPads and tablets do not directly connect to the network. Only to the E-Mail server. These devices are managed by an application called MobileIron, which in case of loss/theft, can remotely erase all data and lock the devices.

30. A sample of 10 computers from across the council was tested to ensure that the systems were updating the window operating system. All 10 were appropriately up to date.

31. A review of the Agresso, Resource link and IDOX servers established that these server's operating systems (windows) had not been updated with security updates since June 2017. It was evidenced that some servers had not been updated with security updates since 2014 prior to June 2017.

32. It was established that the council has recently come to an agreement where Arvato will update all of the server's operating systems, software and databases with security updates on a monthly basis. This has been agreed at a cost of £30,000 per annum.

Security Testing and Incident Management

33. A monthly vulnerability scan of the Council's external internet facing Internet Protocol (IP) addresses is carried out by Trustwave. The ICT department receive a report that details vulnerabilities identified and classify them as high, medium, low or info.

34. It was evidenced that these reports get reviewed and vulnerabilities get logged on the ICT service desk however these are logged as part of KPI ICT 9 (Responding to Incidents of security threats). The indicator is intended to measure the response in carrying out a risk assessment on information received about potential security threats; this includes the monthly network scans however it was established that the KPI only relates to the recording and assessment of incidents, not the fixing of the incidents

35. A new version of the KPI has been drafted by the information assurance manager. The Customers, Commissioning and Change Manager has agreed that this will be reviewed as part of the ICT review.

36. A review of the vulnerabilities reported on the trustwave scans was completed. The following table illustrates vulnerabilities compared over a 4 month period.

Comparison of 4 months vulnerability scans

	June	**September**			
	Vulnerabilities identified	Vulnerabilities outstanding	vulnerabilities identified since June	Fixed since June	% Change
High	0	0	0	0	0%
Medium	23	20	0	3	-13%
Low	14	17	4	1	21%

Although the above table indicates that 3 out of 23 medium risk vulnerabilities have been mitigated the 20 remaining vulnerabilities relate to server encryption:

- 13 of the remaining 20 vulnerabilities are required to be corrected before June 2018 as recommended by the PCI SSC. If these are not completed the PCI SSC will request risk mitigation and migration plans to ensure that this is going to be updated.
- 7 of the remaining 20 vulnerabilities are specific to the encryption methods. When this vulnerability was initially identified a test was conducted on the most popular websites around the world, this vulnerability was only accessible in 0.6% of instances.

37. On an annual Basis CBC receives an “ICT Health check” This is used to confirm compliance with PSN guidelines. The company SEC-1 completed the previous health check. The next health check will be procured after the council has gained PSN compliance which is to be submitted in December 2017. This will enable the next ICT health check to be completed in January or February 2018. Results of the health check will be discussed with the Information Assurance Manager to enable any risks identified to be reviewed and corrected to ensure PSN compliance.

38. The council has purchased licences for Nessus scanning software. This is an internal vulnerability scanner to allow the ICT department to intermittently scan in between the ICT Health Checks. It was agreed that these scans would be completed monthly to assess the progress fixing the network vulnerabilities. After a conversation with the ICT service lead and projects manager it was established that the first full scan has been completed in November 2017, this shows that some servers had vulnerabilities where the software updates had not been completed. These will be reviewed and updated with the aim to reduce the vulnerabilities that are detected.

<u>Physical Security</u>

39. It was identified that as part of PSN compliance the server rooms under ICT control were inspected to ensure compliance with PSN requirements.

40. Physical Server room audits are being completed on a 6 monthly basis, during the audit it was evidenced that these are being completed however have not been sent to the Information Assurance Manager for review since August 2016.

Recommendation		
R4	**Arvato**	Where server room audits are completed it should be ensured that the results are sent to the Information Assurance Manager for further review ***(Priority: Low)***

41. Recently the ICT Board have agreed to an additional meeting, ICT Security Meeting. This will allow for operation discussions to take place and be taken for approval at the ICT Board Meeting.

42. A review of the previous 2 server room audits identified that recommendations are generally being completed however it was identified that the server room door codes have not been changed since November 2015 despite recommendation in the previous 2 server room audits.

Recommendation		
R5	**Arvato**	It should be ensured that the server room door codes are changed annually as a minimum standard ***(Priority: Medium)***

43. The main server room at the town hall has prevention against fire and power surges. Temperatures in the room are also controlled by an independent air conditioning unit

44. With the increase of home working availability the home working policy states security measures to be taken when working remotely.

45. When an employee leaves, they are required to return all devices provided by the council. There is a central list of all devices held by ICT Dept.

46. During the audit a review of the record of issued devices was completed. It evidenced that the records from business transformation and the ICT department have been amalgamated and the record was up to date. It was identified that there were council devices that had been reported lost or stolen within the year. Not all of these losses were reported to the internal audit department.

47. A review of the lost and stolen guidance provided to Arvato revealed that Internal audit were not listed on the guidance to be made aware of lost or stolen devices.

Recommendation		
R6	**Arvato & CBC**	It should be ensured that the lost and stolen device guidance is updated so that internal audit is made aware of any lost or stolen devices and that this guidance is adhered to. ***(Priority: Low)***

48. During the audit it was evidenced that all unused ICT equipment is locked away when not in use.

49. When devices are disposed of they should be disposed of correctly. CBC Requires all disposal companies to be appropriately approved. The most recent collection was by TES-AMM Europe Ltd, who is certified to the standard required by CBC.

50. Since the previous audit the council has purchased a licence for data erasure software (Blancco). This is currently being used to erase remaining data on redundant servers prior to being sent for disposal. This is to further reduce the risk of a data breach.

Training

51. New starters must read, accept and sign a copy of the ICT Policy before they are given access to the ICT systems.

52. Training was identified and a recommendation made to ensure that the mandatory training is completed was included in the Data Protection Audit.

53. Since the previous audit the introduction of the Aspire learning system now means that the training is delivered in an online course. The mandatory course which included Data Protection, Freedom of Information and Information Security was released in March 2017.

Recommendation

R7	**CBC**	Action should be taken to ensure all council employees and members complete the mandatory training courses ***(Priority: Medium)***

54. The course was issued to 921 users, it was established that only 43.60% of council employees have completed the Information Security part of the course.

<u>Disaster Recovery</u>

55. It was established that since the previous audit all of the council servers have been migrated to the virtual server infrastructure. This now means that no tape backups are required and that all backups are now completed using the Commvault and Nimble Systems.

56. The ICT Projects Manager confirmed that operational requests have required information to be restored from the new virtual servers and no issues have been encountered.

57. A previous audit recommendation was to produce an updated and revised disaster recovery plan; a new plan was introduced in September 2016.

58. A recent ICT outage (caused by the core network switch failing and the failover system not activating) brought to light that the ICT disaster recovery plan does not cover the failure of certain parts of the ICT infrastructure.

59. A review of the current plan established that a clearly defined scope is included and where it states the following key phrases.

    "It must be understood that there are currently no 'hot standby' servers to replace the Town Hall server infrastructure should there be a disaster affecting these servers and the associated infrastructure (core network switches and firewalls controlling internet access)"

    "Given the exceptional nature of certain situations with which Arvato could be faced, it is likely that certain contractual commitments become impossible to meet, in full or in part, for reasons beyond Arvato's control"

    Overall the disaster recovery plan provided by Arvato only covers the areas of infrastructure and support that Arvato are responsible for. This plan was approved by the council in September 2016.

60. During the audit it was established that key ICT staff were aware of the ICT disaster recovery plan however other ICT employees were not aware of it.

Recommendation		
R8	**Arvato**	It should be ensured that all ICT staff are aware of the disaster recovery plan and that it is available at all times ***(Priority: Low)***

61. The Council Business Continuity Strategy and Plan is reviewed in the Business continuity audit.

Insurance

62. Since the commencement of the contract CBC only has an insurable interest in the hardware used by CBC employees and members.

63. All devices owned by the council are covered by Insurance. For devices to be covered by insurance they need to be registered with the insurance company. A review of the ICT asset list was completed and established that it was up to date

64. When the laptops were purchased by Arvato for CBC the first 120 laptops were purchased with a 5 year accidental cover and extended warranty. It was decided by Great Place Great Service that further laptops purchased did not require the accidental cover and were only purchased with the extended warranties.

Public Services Network

65. The Public Services Network allows for greater access to information and additional security for sharing information. It is currently run as part of the Government Digital Service.

66. To have access to the network each council is required to undergo an ICT Health Check, show that any issues that arise are being/have been fixed. The Council solicitor in his role as SIRO is required to sign information assurance documents. If all of these are completed correctly then the council will be granted a PSN compliance certificate, and access to the network.

67. The current PSN certificate for Chesterfield Borough Council was obtained in January 2017 and expires in January 2018. The application for next year's PSN compliance certificate will be started in December 2017.

68. It was established that the council also applied for the cyber essentials plus certification. This certification is similar to PSN compliance however this is assessed by an auditor where the PSN compliance is self-assessed.

69. Cyber essentials plus certifications are currently being promoted by the UK government. It was established that the DWP now accept either PSN Compliance or Cyber Essentials plus certifications to access the DWP service also that some government departments (MOD) require cyber essentials plus before any data transfers can take place.

70. The council failed to accomplish this certification this year. The main vulnerabilities are listed below:
    - Vulnerabilities were identified in the initial configuration of the machines tested.
    - Security patches that were released over 30 days prior to the testing were not installed on the machine tested.

    A conversation with the Information Assurance Manager established that he will continue to seek the cyber essentials plus certification for CBC.

Acknowledgement

71. The Auditors would like to thank the Officers within ICT Service and the Information Assurance Manager for their helpful assistance during this audit.

Appendix 1.

Internal Audit Consortium Report opinion classifications from April 17

Assurance Level	Definition
Substantial Assurance	There is a sound system of controls in place, designed to achieve the system objectives. Controls are being consistently applied and risks well managed.
Reasonable Assurance	The majority of controls are in place and operating effectively, although some control improvements are required. The system should achieve its objectives. Risks are generally well managed.
Limited Assurance	Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed.
Inadequate Assurance	There are fundamental control weaknesses, leaving the system/service open to material errors or abuse and exposes the Council to significant risk. There is little assurance of achieving the desired objectives.

Internal Audit Report – Implementation Schedule – CBC

Report Title:	ICT Network Security	**Report Date:**	15th November 2017
		Response Due By Date:	6th December 2017

Recommendations		Priority (High, Medium, Low)	Agreed	To be Implemented By:		Disagreed	Further Discussion Required	Comments
				Officer	Date			
R1	As recommended in the previous audit it is essential that the new draft ICT policies are approved and made available to employees and members as the current policies are outdated.	**High**	**Y**	**Rachel O Neil**	**March 18**			
R2	A system should be implemented to monitor the transfer of data to unsecure email addresses.	**Medium**	**Y**	**Rachel O Neil**	**Oct 18**			This is a piece of work which has been included in the ICT improvement roadmap which is currently being discussed with members. It is expected to be implemented by October 2018
R6	It should be ensured that the lost and stolen device guidance is updated so that internal audit is made aware of any lost or stolen devices and that this guidance is adhered to.	**Low**	**Y**	**Mick Blythe**	**Jan 18**			This has been completed.

Recommendations		Priority (High, Medium, Low)	Agreed	To be Implemented By:		Disagreed	Further Discussion Required	Comments
				Officer	**Date**			
R7	Action should be taken to ensure all council employees and members complete the mandatory training courses	**Medium**	**Y**	**Rachel O Neil / CMT**	**May 18**			CMT are responsible to driving up completion rates for staff in their individual service areas.

______ - Joint recommendation between CBC and Arvato (on both implementation schedules)

Please tick the appropriate response (✓) and give comments for all recommendations not agreed.

Signed Head of Service:	Rachel O Neil	Date:	16th January 2018

Note: In respect of any High priority recommendations please forward evidence of their implementation to Internal Audit as soon as possible.

Internal Audit Report – Implementation Schedule - Arvato

Report Title:	ICT Network Security	**Report Date:**	15th November 2017
		Response Due By Date:	6th December 2017

	Recommendations	**Priority (High, Medium, Low)**	**Agreed**	**To be Implemented By:**		**Disagreed**	**Further Discussion Required**	**Comments**
				Officer	**Date**			
R2	A system should be implemented to monitor the transfer of data to unsecure email addresses.	**Medium**	Yes	CBC IAM/ Arvato ICT	TBA		Date to be agreed once the specification is developed	A secure email system specification is being developed and Arvato will be asked to quote for this change following completion of the contractual review of the ICT service.
R3	A review of the Sophos monitoring procedures should be completed with the aim of ensuring the following are completed on a regular basis • Errors and warnings reviewed and cleared from system • Reconciliation of devices protected to full list of current devices • Ensuring all Sophos protection policies are active and correct	**High**	Yes	Jon Alsop	31st Dec 2017			ICT will undertake an initial tidy up of the Sophos management console to remove obsolete devices. A new Group Policy has been implemented to identify devices

Recommendations		Priority (High, Medium, Low)	Agreed	To be Implemented By:		Disagreed	Further Discussion Required	Comments
				Officer	Date			
								that do not have Sophos installed and to install it. A weekly task will be added to the Service Desk to review the Sophos update progress report and investigate the devices that are not receiving Sophos updates.
R4	Where server room audits are completed it should be ensured that the results are sent to the Information Assurance Manager for further review	**Low**	Yes	Jon Alsop	Next server room audit due 27th Nov 2017			The next server room audit will be sent to the Information Assurance Manager for further review.
R5	It should be ensured that the server room door codes are changed annually as a minimum standard	**Medium**	Yes	Jon Alsop	24th Nov 2017			The codes were changed on the server room doors in the Town Hall and Customer Services Centre on 24th

Recommendations		Priority (High, Medium, Low)	Agreed	To be Implemented By:		Disagreed	Further Discussion Required	Comments
				Officer	Date			
								November 2017. An annual task has been added to the ICT Wiki to prompt annual changes to these codes.
R6	It should be ensured that the lost and stolen device guidance is updated so that internal audit is made aware of any lost or stolen devices and that this guidance is adhered to.	**Low**	Yes	Jon Alsop	TBA			A request has been sent to the Information Assurance Manager to amend the guidance around lost or stolen devices to include the requirement to inform Internal Audit. Previous guidance did not include this requirement
R8	It should be ensured that all ICT staff are aware of the disaster recovery plan and that it is available at all times ***(Priority: Low)***	**Low**	Yes	Jon Alsop	30th Nov 2017			At the next ICT Team Meeting the location of the disaster recovery plan will be discussed and

Recommendations		Priority (High, Medium, Low)	Agreed	To be Implemented By:		Disagreed	Further Discussion Required	Comments
				Officer	Date			
								will then become a standing reference on all future monthly ICT Team Meetings.

Please tick the appropriate response (✓) and give comments for all recommendations not agreed.

Signed Head of Service:	Jonathan Alsop	Date:	1st December 2017

Note: In respect of any High priority recommendations please forward evidence of their implementation to Internal Audit as soon as possible.