BUCKINGHAMSHIRE COUNTY COUNCIL

Business Assurance and Risk Management

Final BMKFA Cyber Security Audit Report (Ref-20/21)

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

William Ockendon, IT Manager

Sue Bressington, IT Audit Senior

CONTENTS

Management Summary 3

Table 1: Overall Conclusion 5

Table 2: Detailed Audit Findings and Management Action Plan 8

Appendix 1: Definition of Conclusions 11

Appendix 2: Officers Interviewed 13

Appendix 3: Report Distribution List 14

Management Summary

Introduction

This audit of Cyber Security at Buckinghamshire and Milton Keynes Fire Authority (the Authority) was undertaken as part of the 2019/20 Internal Audit plan as approved by the Overview and Audit Committee. The audit was undertaken during the second quarter of 2019/20.

The prime purpose of the Authority is to provide Fire & Rescue Services in the South East Region of England. The area covered reaches the outskirts of London to the South Midlands, which is split into the following districts within the Buckinghamshire geographical area – Aylesbury Vale, Chiltern, South Bucks, Wycombe and Milton Keynes.

The Authority connects to the Bucks County Council infrastructure for its Wide Area Network (WAN) via a Virtual Local Area Network (VLAN), as a stakeholder of the Council's Public Sector Network. The network infrastructure is managed by Updata (part of the Capita Group), who provide a fully managed network service, as well as maintaining the current WAN, LAN and associated ICT services. This is supplemented by a small team of Fire Authority Officers who provide a service desk and non-network management related tasks, as well as monitoring the network's health and status. Although the monitoring is officially completed by Updata, the Authority monitors this to ensure that all issues are identified and remediated by Updata as soon as possible

Audit Objective

Internal Audit's objectives for this audit are to provide an evaluation of, and an opinion on, the adequacy and effectiveness of the system of internal controls that are in place to manage and mitigate risks associated with Cyber Security within the Authority.

This will serve as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually to the Fire Authority, and also as an assurance to the Section 112 officer that financial affairs are being properly administered.

Scope of work

The audit activity focussed on the following key control areas as defined by the Cyber Essentials Scheme (a Government backed and industry supported scheme to help organisations who become accredited, to protect themselves against common cyber-attacks; Cyber Essentials It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats):

Boundary firewalls and internet gateways

- Information, applications and PCs within the Group's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure configuration

- PCs and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User access control

- User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

Malware protection

- Devices that are exposed to the internet should be protected against malware infection through the use of malware protection software.

Patch management

- Software running on PCs and other network devices should be kept up-to-date and have the latest security patches installed.

The audit considered the controls in place at the time of the audit only. Where appropriate testing was undertaken using samples of activities that occurred within the last 12 months.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Reasonable**

RISK AREAS	AREA CONCLUSION	No of High Priority Management Actions	No of Medium Priority Management Actions	No of Low Priority Management Actions
Boundary firewalls and internet gateways	Substantial	0	0	1
Secure configuration	Reasonable	0	1	0
User access control	Reasonable	0	1	0
Malware protection	Substantial	0	0	0
Patch management	Substantial	0	0	0
		0	2	1

Appendix 1 provides a definition of the grading for each of the conclusions given.

The overall opinion of **Reasonable** Assurance for the Cyber Security audit was concluded as there were no significant weaknesses in the control framework for the areas reviewed as part of this audit. There is generally a good system of internal control in place and the majority of risks are being effectively managed. However, some action is required to improve controls in relation to user access protocols, cyber security training and contract management with Updata. The implementation of our recommendations should help to strengthen the Cyber Security controls within the Authority.

Boundary firewalls and internet gateways

The Authority's network perimeter is protected by firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the Authority. The firewall rules are set to deny traffic by default and only allow access for authorised protocols, ports and applications to exchange data across the boundary. Any required changes are subject to a change management process where proposed changes are reviewed and approved prior to configuration. All changes are supported by a business case to explain why they are required. Firewall rules are reviewed annually by Updata and any changes are notified to the Authority's ICT Manager, who is responsible for approving or rejecting the change to go ahead.

Wireless access points are secured to only allow known devices to connect to corporate Wi-Fi services.

Administrator access to any network component is authenticated and authorised, and default administrative passwords for network equipment are routinely changed upon implementation of the application.

The network is managed by Updata with support from the Authority. The Operational Process document agreed with Updata sets out target response times, and states that monthly service performance reports will be sent to the Authority on 10th working day of the calendar month. The reports should include incidents raised, analysis of resolution categories, time to fix, performance to SLA and service availability. These reports are not provided by Updata *(see Finding 3 below)*.

Secure configuration

Solarwinds is in use to regularly monitor network vulnerabilities, the status of corporate devices and ensure that all required actions are identified. Actions are to be completed by Updata, therefore if the Authority identifies an action to be taken before Updata, they raise a service desk ticket to start the process. Conversely, if Updata identify one, they raise a ticket and notify the Authority.

System Center Operations Manager (SCOM) is used to monitor servers, which provides a monitoring solution for operating systems and hypervisors (virtual machine manager). SCOM uses a single interface that shows state, health and performance information of systems. It also provides alerts generated according to some availability, performance, configuration or security situation being identified. It works with Microsoft Windows Server and Unix-based hosts.

System administrators are the only officers able to install software. This is controlled by a group policy setting which is configured to not allow execution files to run for standard users. Therefore software can only be downloaded if it has been pre-approved and made available for users to install by ICT, in Microsoft System Center Configuration Manager (SCCM). Group policy settings allow USB devices to install documents to PC's but not PC to USB unless the USB is encrypted. All PC's are encrypted by BitLocker and users are not permitted to connect with their own device.

External penetration tests are completed bi-annually, with a targeted test in between. Required actions identified in the last test (2016) were monitored and recorded in a remediation plan and no actions are outstanding. The next full test which was due in 2018 is scheduled for completion this month; this was delayed due to resourcing and staffing issues, however we note that there are monitoring tools in use to help identify any vulnerabilities, and the vulnerabilities identified in the last penetration test have been addressed.

User access control

A walk-through review of the process for notifying starters and leavers to ICT was completed. We noted that automatic emails are created as part of a workflow process, which are then diarised in a central diary by ICT to ensure that all relevant staff have access and are able to act upon the email requests.

During the last 12 months, there were 38 new starters and 62 leavers. Walk-through testing of three starters and one leaver confirmed that these had been processed in accordance with local procedure. The local procedure permits standard users the same level of access by department. Access permissions for applications are managed by ICT within the relevant application. Role profiles have not been identified and are therefore not in use. We note that access rights have been created and some privileges granted are added after the initial user permissions have been created. There is therefore a need to review all profiles to ensure that users do not have access to data and systems not needed to perform their job duties, and this has not been completed *(see Finding 1 below)*.

The Authority's active directory has seven ICT users with enhanced privileges, 22 external users with enhanced privileges (including one network manager and 3rd party software suppliers). In total there are 430 active accounts.

At the time of the audit, 92.3% of all staff had completed mandatory e-Learning security training "Protecting Information". This training is part of the user induction process. All training materials and relevant topic updates are added to the Intranet, however there is not a standard cyber security refresher course, and no mock phishing attacks are completed to test the effectiveness of induction training and user awareness *(see Finding 2 below)*.

Malware protection

Microsoft System Center Configuration Manager (SCCM) is utilised to manage the Authority's Anti Malware and Antivirus solution. Updates are configured to automatically roll out when they are available, the next time a device connects to the network. The SCCM Endpoint Protection Status is checked on a daily basis to make sure the Endpoints are reporting in and have installed correctly on client devices and servers. At the time of the audit, a total of 30 from 356 active devices with endpoint protection had not connected to the network to receive the latest update. This was monitored and reviewed on an on-going basis throughout the day.

Patch management

SCCM enables administrators to manage the deployment and security of devices and applications across an enterprise. One of the features in use at the Authority is the remote control of patch management, operating system deployment, network protection and other various services. The SCCM endpoint protection of windows servers is managed by WSUS (Windows Server Update Services) which downloads the updates from the Microsoft Update website and then distributes them to devices connected to the network. This has been configured to download updates and for the products installed on clients and servers.

Updates are pushed out to client devices 14 days after "Microsoft Patch Tuesday". User devices are configured to have the update installed within two days of ICT releasing it. 14 days are passed before deploying these updates to make sure that all issues with the updates have been identified and resolved by Microsoft, therefore this negates the need for pre-release testing. Patch management for all applications are controlled by the relevant software provider.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Role profiles and tidying up of current access permissions	Risk Rating	Agreed Management Actions
Role profiles have not been identified and are therefore not in use. We note that access rights have been created and some users have additional privileges granted after the initial user permissions have been created. User profiles therefore need to be reviewed to ensure that there is a business need for all users to access the systems and date they have been granted, however this has not been completed. This increases the risk of unauthorised access being granted as there is no set profile structure, which could result in users having access to data they are not entitled to view. We recommend, as has been identified by the ICT Manager and Service Desk Manager that current access permissions are reviewed and removed where appropriate, and role profiles are created and implemented to allow a standard configuration by function.	**M**	We currently use a retention schedule with each department Information Asset Owner owning their own schedule worksheets within it. When a new starter (or new to role) is notified they can only be given access as advised by the Information Steward to be listed as an access rights holder in relevant schedule. If an existing employee transfers to another department their access rights are stripped and rebuilt as advised in the relevant schedule. **Officer responsible:** ICT Manager, DT **Date to be implemented by:** 31 March 2020

Finding 2: Training and the measurement of its effectiveness	Risk Rating	Agreed Management Actions
At the time of the audit, 92.3% of all staff had completed mandatory e-Learning security training "Protecting Information". This training is provided as part of the user induction process. All training materials and relevant topic updates are added to the Intranet, however there is not a standard cyber security refresher course, and no mock phishing attacks are completed to test the effectiveness of induction training and user awareness. This increases the risk of users not being aware of, or accountable for inappropriate use of the Authority's devices, which could result in a cyber-attack or data breach occurring. We recommend that an annual refresher training course/package is completed and rolled out to all users to ensure that they are kept up to date with the most recent guidance. Mock phishing attacks should be scheduled on a rotational basis to establish the effectiveness of training and user awareness.	**M**	The "Responsible for Information" general user is completed by all new starters and bi-annually by all employees via the HEAT package (an online training facility). It replaced the "Protecting Information" training. HEAT sends out reminders when the refresher training is due. It is proposed to maintain the refresher training as bi-annual (rather than annually as suggested). We are in discussion with BCC Audit for suggested mock phishing providers. We have identified a free cyber training package from the National Cyber Security Centre https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html It is proposed to roll this out via HEAT with refreshers on a bi-annual basis by 31 March 2020 After the free training session provided by the South East Regional Organised Crime Unit to SMB on 1 October 2018 it was agreed that its free training offer for lower tier would be rolled out. **Officer responsible:** Information Governance & Compliance Manager. GB **Date to be implemented by:** 31 March 2020

Finding 3: Contract management with Updata	Risk Rating	Agreed Management Actions
The network is managed by Updata with support from the Authority. The Operational Process document agreed with Updata sets out target response times, and states that monthly service performance reports will be sent to the Authority on the 10th working day of the calendar month. The reports should include incidents raised, analysis of resolution categories, time to fix, performance to SLA and service availability. These reports are not provided by Updata. There is an increased risk that Updata are not effectively delivering against their SLA targets, and this may not be identified. There is also a risk that the overall high level monitoring of network issues is not identified. The Authority should, in conjunction with Bucks CC, discuss and agree the process for contract monitoring and reporting with Updata, to ensure that a full overview of the network stability and performance is available and repeat issues identified and resolved.	**L**	The Authority has signed a two-year extension to the Updata contract. Whilst we have not previously found regular reports and meetings necessary due to the small level of issues, we will insist that these are prepared and formally delivered in the future. **Officer responsible:** ICT Manager, DT **Date to be implemented by:** 1 November 2019

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

Definition		Rating Reason
Substantial	There is a sound system of internal control designed to achieve objectives and minimise risk.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a good system of internal control in place which should ensure objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority but some high priority actions may be present.
Partial	The system of internal control designed to achieve objectives is inadequate. There are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
Limited	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actions. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the draft Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Dave Thexton	ICT Manager
Lewis Higgins	Service Desk Manager
Daniel Shaw	ICT Server Specialist
Dylan Bettles-Hill	ICT Operations Specialist

The Exit Meeting was attended by:

Name:	Title:
Dave Thexton	ICT Manager

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report:

Dave Thexton	ICT Manager
Gerry Barry	Information Governance and Compliance Manager
Graham Britten	Director of Legal and Governance

Final Report as above plus:

Mark Hemming	Director of Finance and Assets
Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	10 July 2019
Draft Report	27 August 2019
Management Responses	22 October 2019
Final Report	24 October 2019
Audit File Ref	20-21

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance Manger

Phone: 01296 387327

Email: mgibb@buckscc.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: sharlock@buckscc.gov.uk