BUCKINGHAMSHIRE COUNTY COUNCIL
INTERNAL AUDIT AND RISK MANAGEMENT

FINAL INTERNAL AUDIT REPORT

Information Security 2018/19

Date Issued: 05-11-2018

CONTENTS

Audit Control:

Closing meeting:	21 September 2018
Draft report:	15 October 2018
Management responses:	24 October 2018
Final report:	5 November 2018
Audit Ref:	19/46

Auditors:	Maggie Gibb	Head of Business Assurance (and Chief Internal Auditor)
	Selina Harlock	Audit Manager, Business Assurance Resources
	William Ockendon	IT Audit Manager
	Mabona Khoza	IT Audit Senior
Report Distribution:		
Draft Report	Gerry Barry	Information Governance and Compliance Manager
	Graham Britten	Director of Legal and Governance
	Dave Thexton	ICT Manager
Final Report as above plus:	Mark Hemming	Director of Finance and Assets
	Jason Thelwell	Chief Fire Officer

Management Summary

Introduction

This audit of Information Security at Buckinghamshire and Milton Keynes Fire Authority (the Authority) was undertaken as part of the 2018/19 Internal Audit plan as approved by the Overview and Audit Committee. The audit was undertaken during the third quarter of 2018/19.

The prime purpose of the Authority is to provide Fire & Rescue Services to the South East of England, the area stretches from the outskirts of London to the South Midlands. It comprises the four districts of Buckinghamshire – Aylesbury Vale, Chiltern, South Bucks and Wycombe – and Milton Keynes.

The Authority receives around 16,000 calls for assistance every year, of which about 7,000 are emergency incidents. It has 42 frontline and specialist fire and rescue vehicles and four Urban Search and Rescue vehicles.

Information at the Authority is mainly electronic and is held within the corporate network. Staff access is managed through the Microsoft Active Directory Operating System, where users are required to logon through a username and a complex password.

All staff members are responsible for Information Security within the Authority. Management has been delegated to the Information Governance and Compliance Manager, who reports to the Director of Legal and Governance, whist the Information Communication Technology (ICT) team provide technical support and administration and the implementation of IT security controls within the Authority.

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 Information Security with 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.

Scope of work

The audit activity focussed on the following key controls areas identified in the processes relating to Information Security:

Data Classification and Sharing

- Data has been appropriately identified and classified. Adequate controls such as data sharing protocols and security policies are in place.

Data Management and Policies and Procedures

- Security policies have been documented, and include such considerations of data classification, storage and transmission. Responsibility for data security has been clearly designated to a senior staff member.

Training and Awareness

- Staff receive appropriate and periodic training in relation to security awareness, including data security.

Logical Access Controls

- Logical access controls are in place across IT systems, such as controls related to remote access, encryption, application passwords and permissions for access (to files/folders/records/CCTV).

Physical Access Controls

- Physical controls are in place to mitigate and manage the risk of theft and compromise of IT equipment, documentation and data by means of unauthorized physical access to premises.

Backup Strategy

- Backup arrangements are in place to mitigate the risk of loss of data and lack of availability. Such arrangements should include a detailed back up strategy and testing of backups.

Disposal Procedures

- Procedures are in place to securely dispose of data after its retention can no longer be justified, as well ensuring that data is removed from obsolete equipment.

Legislation Compliance

- Relevant Data Protection legislation is being complied with across the Buckinghamshire Fire and Rescue Service, with appropriate planning being undertaken to ensure compliance with the General Data Protection Regulation (GDPR) which came into effect on 25th May 2018.

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
Data Classification and Sharing	Substantial	-	-
Data Management and Policies and Procedures	Substantial	-	-
Training and Awareness	Substantial	-	-
Logical Access Controls	Substantial	-	-
Physical Access Controls	Reasonable	-	1
Backup Strategy	Substantial	-	-
Disposal Procedures	Substantial	-	-
Legislation Compliance	Reasonable	-	1
		-	2

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

The overall conclusion of **Reasonable** Assurance for the Information 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 implementation of Close Circuit Television system (CCTV) at all fire stations, the development

of a formal IT assets disposal agreement and a review of the Network password settings (password reset counter in minutes). The implementation of our recommendations should help to strengthen the Information Security controls within the Authority.

Data Classification and Sharing

There is a Protective Marking and Harm Testing Classification Procedure that was recently reviewed by the Information Governance and Compliance Manager and has been approved by the Strategic Management Board. The procedure provides an overarching guidance and direction regarding data classification. The Authority has adopted the Government Security Classifications (GSC) framework, which has three classification markings 'OFFICIAL', 'SECRET' and 'TOP SECRET'. Based on the GSC framework, the Authority has classified its information as Official Sensitive.

A Personal Data Mapping Exercise has been carried out in accordance with GDPR by the Human Resources Development Manager. The Exercise include action to be taken for each of the GDPR 12 Steps, Personal Data Held, Personal Data Shared, Issues and Actions and HR Systems access.

There is a Dealing with Request for Information Procedure for 2018-19, that was approved by the Performance Management Board. The purpose of this procedure is to raise awareness of, and improve compliance with, legislation for the management of information including personally identifiable information and how requests for information are dealt with by the Authority. We carried out a sample reviewed of Information Sharing Protocols and noted that they were effectively approved.

Data Management and Policies and Procedures

There is an Information Security Policy Statement for the Authority, which highlight how the Authority processes information which includes personal and sensitive information, about individuals and other organisations in order to carry out its business.

An Acceptable Use of Information and Information and Communications Systems and Equipment Procedure approved by the Director of Legal and Governance in June 2018 is in place. The procedure provide guidelines to staff members on areas such as; access to information and information and communications systems, use of personal devices, hardware and software installations, password policy and Remote access, etc.

All staff members are responsible for Information Security within the Authority and management of Information Security has been delegated to the Information Governance and Compliance Manager, who reports to the Director of Legal and Governance. The Information Communication Technology (ICT) team provide technical support and administration.

Training and Awareness

Staff completed a mandatory e-Learning security training for 2018-19. This training is completed on an annual basis and new joiners are also required to complete the training during induction. GDPR training has been provided to relevant staff (staff members who deal with personal data) during 2018.

Ongoing Information Security awareness is provided to staff through email and security alters and changes to Security Policies and Procedures is communicated via the intranet.

Logical Access Controls

Logical access controls are in place across IT systems, such as controls related to remote access, encryption, application passwords and permissions for access (to files/folders/records/CCTV). Initial access to information is controlled through the Network Operating System - Active Directory (AD). All staff members are provided with unique usernames and passwords to logon to the Authority's Network.

Password controls identified are fairly configured, meeting key requirements of password length, complexity, history size, expiry and lockout threshold. However, password reset counter is set to 30 minutes, which mean that users are allowed to try logon every 30 minutes after they are locked out. **Refer to Management Action 3**

Physical Access Controls

Physical access controls are in place to mitigate and manage the risk of theft and compromise of IT equipment, documentation and data. Staff members are provided with an access tag (forb). Visitors are required to sign in at reception and are escorted by a member of staff.

Access to the data centre is limited to ICT and Facilities staff, whilst visitors are escorted by an authorised members of staff and are required to sign a register. Close Circuit Television system (CCTV) are installed in the data centre and are monitored by Facilities.

CCTV is implemented at head office and on all fire trucks. However, we noted that there is no CCTV at all Fire Stations within the Authority. Management confirmed that a risk assessment was conducted and a business decision was taken to not install CCTV Cameras at all fire stations as it would be too expensive. **Refer to Management Action 1.**

Backup Strategy

Backup procedures are in place, outlining the backup process, tape rotation procedure and restoration process. Backup is performed on a daily basis through Backup Exec, backup tapes are stored off-site and backup can be restored from the offsite facility.

Disposal Procedures

An IT assets disposal arrangement is in place with a third party (Dynamic). The Authority contacts Dynamic as and when they need to dispose of IT assets. Dynamic provide disposal certificates to the Authority after completion of the process.

However, we noted that there is no formalised agreement with Dynamic outlining the procedures for disposing off the IT assets. **Refer to Management Action 2.**

Legislation Compliance

The organisation is currently registered with the Information Communication Office, the registration is due to expired in December 2018. As the registration is not due for renewal there is no need to registration under GDPR as yet.

Table 2 Detailed Audit Findings and Action Plan

Management actions have been agreed to address control weakness identified during the closing meeting and agreement of the draft Internal Audit report. All management actions will be entered on the Council's Performance Management Software and progress in implementing these actions will be tracked and reported to the Regulatory & Audit Committee.

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

Priority High (H)	Major issue or exposure to a significant risk that requires immediate action or the attention of Senior Management.
Priority Medium (M)	Significant issue that requires prompt action and improvement by the local manager.
Priority Low (L)	Minor issues requiring action to improve performance or overall system of control.

	Audit Finding, risk exposure and potential impact	Priority	Management Action
1.	**CCTV cameras at all Fire Stations** The Authority should re-consider implementing CCTV Cameras at all Fire Stations to monitor the interior and exterior, so as to detect and deter theft and compromise of IT equipment which may result in exposure of sensitive information. Audit identified that there is no CCTV Cameras at all Fire Stations within the Authority. Management confirmed that a risk assessment was conducted and a business decision was taken to not install CCTV Cameras at all fire stations as it would be too expensive. Lack of CCTV Cameras at Fire Stations may lead to theft and compromise of IT equipment not being detected or deterred and may result in exposure of sensitive information.	M	**Action:** The Premises Security Group will meet to undertake a further review and risk assessment of the CCTV system to consider if the use of CCTV on more Stations is likely to be a deterrent to intruders. The review to include other potential deterrents such as lighting with motion sensors. **Officer responsible:** Gerry Barry, Information Governance & Compliance Manager. **Date to be implemented by:** end of January 2019

	Audit Finding, risk exposure and potential impact	Priority	Management Action
2.	**IT Assets Disposal Agreement** A formal disposal agreement should be developed and agreed with Dynamic. The agreement should clearly outline the process to be followed by the third party when disposing IT assets. An IT assets disposal arrangement is in place with the third party (Dynamic), where the Authority contacts Dynamic as and when they need to dispose of IT assets. However, we noted that there is no formalised agreement with Dynamic, outlining the procedures for disposing of IT assets. If a formal agreement which outline the disposal procedure is not in place, there is a risk that personal and/or sensitive information may be made available to unauthorised individuals due to the service provider no following appropriate disposal procedure.	M	**Action** Draft contract is in the process of being finalised. In the meantime Dynamic deliver services to us under WEEE regulations, they are certified by the Environment Agency and our data remaining on devices is destroyed above and beyond DoD 5200.22M standard. **Officer responsible:** Dave Thexton, ICT Manager **Date to be implemented by:** 01/01/2019

Table 3 Low Priority Issues

Minor issues to be noted or requiring action to improve performance or overall system of control, which do not present a material risk to the system of control.

	Audit Finding, risk exposure and potential impact	Management Action
3.	**Network Password Settings (Password Reset Counter)** Management should consider increasing the password reset counter to 1440 minutes (24 hours), to be in line with Microsoft best practice. The Authority may also consider implementing a self-service password reset to ease call volumes. Our review of the Network Password Settings identified that Password controls are fairly configured, meeting key requirements of password length, complexity, history size, expiry and lockout threshold. User accounts are locked out after 3 unsuccessful attempts. However, password reset counter is set to 30 minutes, which mean that users are allowed to try logon every 30 minutes after they are locked out. Failure to enforce strong password controls increases the risk of unauthorised access to the Authority's Network and therefore access to sensitive data and impacting on its confidentiality.	**Action:** We have consulted a Police Cyber Security Advisor from the South East Regional Organised Crime Unit) who suggests that if used in conjunction with a long, complex password policy a lockout of 30 minutes is sufficiently disruptive to deter anyone but the most persistent of brute force attacks. We agree with the audit findings that a 30 minute timer might not prevent a determined attacker if weak, common passwords are a possibility. We will consider further guidance from the National Cyber Security Centre and investigate a number of options to ensure the use of strong passwords (to include training users in the selection of passwords) and "smart lockout' options, where the system analyses the context of the logins before locking out. **Officer responsible:** Dave Thexton, ICT Manager **Date to be implemented by:** This will be reviewed by year end.

Appendix 1 Definition of Conclusions

Grading:	Substantial	Reasonable	Limited
Overall conclusion on the system of internal control being maintained	There is a strong system of internal control in place and risks are being effectively managed. Some minor action may be required to improve controls.	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.	The system of internal control is weak and risks are not being effectively managed. The system is open to the risk of significant error or abuse. Significant action is required to improve controls.

Appendix 2 Officers Interviewed

The following staff contributed to the outcome of the audit:

- Gerry Barry Information, Governance and Compliance Manager
- Graham Britten, Director of Legal and Governance
- Dave Thexton, ICT Manager
- Daniel Shaw, ICT Server Specialist
- Faye Mansfield, Human Resources Development Manager
- Dean Elliott, Station Commander Amersham and Beaconsfield

The Closing Meeting was attended by:

- Gerry Barry , Information, Governance and Compliance Manager
- Graham Britten, Director of Legal and Governance

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.

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

Selina Harlock, Audit Manager, Business Assurance (Resources)

Phone: 01296 383717

Email: sharlock@buckscc.gov.uk

William Ockendon , IT Audit Manager (Mazars LLP)

Phone:07500 571942

Email William.Ockendon@Mazars.co.uk

Mabona Khoza , IT Audit Senior (Mazars LLP)

Phone: 078812 84022

Email: Mabona.khoza@Mazars.co.uk