London Borough of Hammersmith and Fulham

Internal Audit Report - Final

Cyber Security

July 2020

Contents

1 Introduction

As part of the internal audit plan, agreed by the Audit, Pensions and Standards Committee, we have undertaken a cyber security audit at the London Borough of Hammersmith and Fulham. The audit took place over the period August 2019 to November 2019.

The 2015 National Security Strategy confirmed that cyber remains a Tier 1 threat to the UK's economic and national security and there is a recognition that cyber-attacks are becoming more frequent and of greater sophistication. At the same time Government Departments have plans to dramatically increase the services that will be provided digitally. Users expect digital services to be user friendly and quick but also secure.

The overall objective of this internal audit is to provide reasonable assurance of the adequacy and effectiveness of the key controls relating to the cyber security control framework currently in place to minimise the risk of cyber security threats impacting on information confidentiality, integrity and availability within the London Borough of Hammersmith and Fulham.

This review is based on the National Cyber Security Centre (NCSC)'s "10 steps to security" framework. It will also form an opinion on the current level of compliance against the Cyber Essentials framework that LBHF is working towards.

2 Executive Summary

2.1 Assurance Opinion

	Nil	Limited	Satisfactory	Substantial
Audit Opinion		L		

2.2 Recommendations Summary

The following table highlights the number and categories of recommendations made.

Area of Scope	Adequacy	Effectiveness	Recommendations Raised		
			High	Medium	Low
Governance			0	1	0
Culture, Awareness and User Education			0	0	1
Secure Configuration			1	0	0
Network Security			0	1	0
Identity and Access management			0	1	0
Malware Prevention			0	0	1
Incident Management			1	0	0
Removable Media			0	0	1
		Total:	**2**	**3**	**3**

Please refer to the Appendix 2 for a definition of the audit opinions and recommendation priorities.

3 Summary of Findings

In Internal Audit's opinion, **Limited Assurance** can be given to Executive Members, the Chief Executive and other officers that the controls relied upon at the time of the audit were suitably designed, consistently applied and effective in their application.

Our findings indicated that weaknesses and/ or omissions in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk. Two high, three medium and three low priority findings were identified, which are detailed in Appendix 1.

Design of and compliance with controls to address the key risks identified

Governance

- LBHF has created and maintains a risk register and accompanying risk management strategy which comprises of a consideration of risks across LBHF, including cyber security related risks.
- Fortnightly meetings between relevant personnel are scheduled to ensure that information management risks and issues, including cyber security matters, are discussed and mitigations agreed. These meetings inform updates to LBHF's risk register so it is kept sufficiently up to date in order to appropriately determine the organisation's risk appetite. These meetings are attended by the IT Security Manager, Information Manager, the Data Protection Officer, and the Senior Information Risk Officer (currently the Chief Digital Officer).
- LBHF has developed six policies supporting technology and risk within the organisation. In addition to the internal Risk Management Strategy document, there is also a broader IT Strategy informational leaflet which provides knowledge on LBHF's approach to IT as part of its 5-year plan.

Culture, awareness and user education

- LBHF has a staff induction process, as part of which, new personnel must undertake and complete an induction training presentation (covering both information security and data privacy). The terms and conditions of employment are laid out in the staff handbook.
- Users throughout LBHF are expected to undertake and complete additional courses, as assigned to them by their managers (via SuccessFactors) to ensure that they maintain their awareness of corporate policies and practices. Completion of this training is mandatory for all personnel and a mechanism exists to ensure that the training is completed.

Secure Configuration

- The creation of baseline machine configurations and the deployment and management of those configurations is managed by a third party (BT) under a service contract.
- BT deploy and manage (including patch management) a set of supported software with the defined configurations. Supported hardware and software is agreed between BT and LBHF as part of the service contract. The supported software includes antivirus, web browsers, and Windows 10. Additionally, machines are deployed with Bitlocker encryption enabled (full disk encryption).
- Patches are implemented using SCCM and pushed to deployed machines according to the specific patches required (i.e. server vs client).

- Changes to the build configuration are agreed and subsequently result in the production of a new high-level design document; however, there has not been any such changes within the last year.
- LBHF also maintains an IT asset register, and company IT assets are assigned a unique tag. LBHF's asset register also includes software that is not managed as part of its service contract with BT. The Service Delivery team perform regular reviews of leavers to ensure that licenses are being deactivated when no longer required; as part of the leaver process, physical assets are also returned, and the list is amended.
- The Windows 10 high-level design document outlines the whitelisted applications that are installed as part of image deployment. A combination of Software Centre and AppLocker is used to deny installation and execution for any application that has not been preapproved.

Network Security

- Default administrative passwords are changed as part of the installation process.
- Regular penetration tests are performed against LBHF's systems by a third party and a report is prepared and reviewed by the IT Security Manager. Relevant findings are shared with senior management. Action points following on from the findings are tracked to ensure that potential vulnerabilities are remedied.

Identity and Access Management

- LBHF has established a process to manage starters and leavers through an online tool.
- Accounts that have not been used for over 75 days are queried manually and subsequently managers are informed and the account is disabled. Accounts disabled are added to a "daily report spreadsheet" which notes that leaver and dormant access has been manually inspected by IT/Service Desk and revoked.
- Users are provisioned with accounts that adhere to the principle of least privilege. Standard accounts are restricted in their ability to materially change the core system functionality and are limited to making user-level changes as part of their business roles.
- Administrative accounts are limited in number and assigned to authorised individuals as required by their business role. Administrative accounts are reviewed periodically by the IT Security Manager.
- The provisioning of privileged access is performed using the starters and leavers process, with the elevated access requests accompanying the new joiner ticket.
- For administrative accounts belonging to, and managed by, BT (under a service contract) these are assigned according to BTs requirements and are subject to their own internal controls.

Malware Prevention

- Microsoft System Centre Configuration Manager (SSCM) is used to deploy and update anti-malware protection across the infrastructure.
- Firewall rules are in place to filter traffic and are set to deny traffic by default.
- End user protection consists of Windows Defender in a Windows 10 environment deployed by BT as part of the standard image, in accordance with the service contract.

Incident Management

- LBHF has established an incident management policy to provide guidance on incident reporting and handling. Additionally, a third-party service provider (Agilisys) has been contracted to manage the incident reporting and handling process. Agilisys acts as first line triage for incident tickets submitted upon user request.
- Agilisys provides monthly service reports which are communicated to the Service Delivery Manager and contain key statistics for that month, including service desk KPIs and a performance breakdown including by type and by number.

Removeable Media

- User education and awareness on the proper use and handling of removable media is implemented as part of the induction process and is delivered via the webcast system.
- The use of removable media is limited. In consultation with the third-party contracted to deploy and maintain LBHF's secure baseline, BT restrict the use of removable media.

4 Acknowledgement

We would like to thank the following members of staff for their time and assistance during the audit:

- Quentin Brooks – Service Director
- Katrine Nowicki – Operations Manager
- Adrian Dewey – IT Security Manager
- Anthony King – Technical Architect
- Ed Crow - Head of information and data protection officer

Appendix 1: Management Action Plan

1. Governance

Priority	Issue	Risk	Recommendation
Medium	Within cyber security, risk management reporting lines and roles have not been clearly designated, neither in the Risk Management Strategy or another document. Additionally, whilst there is a semi-formal meeting established during which cyber security is discussed, the information presented at this meeting may not always be fully relevant or complete, as information does not flow through a designated process. We inquired with a number of teams, including Service Delivery and Networking and were unable to establish a process by which information is fed upstream, from the individual teams to this meeting. Moreover, LBHF has a series of organisation charts, but we could not identify a specific framework relating to the roles and responsibilities of individuals as pertained to cyber security. In our inquiries with the IT Security Manager for example, we noted that no specific job description exists and that responsibility for LBHF's cyber security landscape was his 'ad-hoc' responsibility.	Without effective governance processes the Board may have an incorrect understanding of the overall risk exposure of the organisation. Without effective risk management processes, the Board may not have confidence that its stated policies and risk appetite are being consistently applied across the business as a whole.	Formalise the reporting lines in the Risk Management Strategy. Formalise the terms of reference of the Cyber Security meeting. Update the job description of the IT Security manager to include responsibility for cyber security.

Management Response
1) More structured recording of SIRO / DPO briefings has now been established. See attached evidence – please clarify if anything further needed. 2) Establish more regular (quarterly) Digital Services DLT reviews of risk register, recognising cyber security issues and management as defined in the SIRO / DPO briefings. **Target end July 2020** 3) IMT job descriptions to be updates as applicable. **Target end June 2020**.

Responsible Officer	Deadline
Ed Crow	31st July 2020

2. Culture, awareness and user education

Priority	Issue	Risk	Recommendation
Low	We were unable to inspect an "acceptable use policy". Apart from high level information provided in the employee handbook and in the agreement signed by employee upon receipt of company assets, there is no detailed policy in place to govern, at a corporate level, the acceptable use of company assets on a per-system basis. In line with the NCSC's guidance, there should be a separate document which details management expectations from users across different business systems. The cyber security objective is that, whilst installations are restricted on laptops and sandboxed on mobiles, user education can step in where technically restrictive controls fall short.	The lack of an acceptable use policy may expose LBHF to virus attacks, compromise of network systems and services, and legal issues through misuse of assets.	Formalise an acceptable use policy that details the limitations and restrictions to be enforced by the users.

Management Response	
This will need to be coordinated through the re-constituted Corporate Information Management Board, with service areas requested to create to define acceptable use policies for their systems. For example, ASC and Children's services to define an acceptable use policy for Mosaic (per system basis). Digital Services and IMT can advise on the creation of these. **Target end August 2020** Personal Commitment statement to be reviewed by Head of Information. **Target end July 2020**.	
Responsible Officer	**Deadline**
Ed Crow	31st August 2020

3. Secure Configuration

Priority	Issue	Risk	Recommendation
High	A report of the latest patches installed is sent to the IT Security Manager on a monthly basis which includes out-of-band (i.e. critical) patches. However, due to resource constraints, this report is not reviewed by IT Security Manager. Additionally, the report does not cover the list of patches that have not been installed across the domain. Patching lists are only reviewed when an event occurs or if an issue is flagged in Nessus which could relate to patch management. Through inspection of the penetration test, we noted a significant number of vulnerabilities including critical risks such as outdated ActiveX controls related to Adobe Flash.	If patches are not deployed in a timely manner across all devices, attackers may attempt to exploit unpatched systems to gain unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patchhave been issued but not applied.	Management should liaise with BT to amend the content of the patch reports to focus on actionable information (e.g. list of patches including their criticality that have not been installed) and, then, review them on a monthly basis. Management should ensure updates are applied to all software installations, including non-Microsoft applications, on a regular basis.

Management Response
Subsequent to the audit H&F has documented a new security patching process with BT (Evidence attached 'patch-process-ms-security-hf-bt-01). The policy is owned by the Technical Design Authority. It includes monitoring for applicable patches, roll-out to devices, and reporting of compliant (successfully patched) and non-compliant (patches outstanding) devices. The document was completed on 29th July 2019, and the process is operated on a monthly cycle. We have a separate policy for application patching. It is still in draft, awaiting approval by the Technical Design Authority. It comprises of two documents currently named 'app-monitoring-process-a01.docx' and 'apps-installed-vs-supported-tda.xlsx'. The policy is expected to be approved by the end of July 2020, and in full operation by end of November 2020.

Responsible Officer	Deadline
Ed Crow (Representing TDA)	30th November 2020.

4. Network Security

Priority	Issue	Risk	Recommendation
Medium	Alerts are generated by the firewall and saved into a log file; however, this log file is not reviewed - either automatically or manually - except in the event of an incident. At the time of the audit we were not able to inspect any firewall logs reviews in order to obtain an analysis of the nature of the traffic.	In the case of incidents, the firewalls audit trail may be insufficient for a thorough investigation as they are not reviewed.	Management should consider implementing a pro-active process to review the network logs to identify possible security threats and incidents.
Management Response			
We will consider how network logs are reviewed, taking into account the impact of Covid-19 and other major projects such as the King Street Regeneration programme as they may influence the process.			
Responsible Officer			**Deadline**
Quentin Brooks			31st December 2020.

5. Identity and Access Management

Priority	Issue	Risk	Recommendation
Medium	Although a starter and leaver process has been designed, we noted that the document was still in draft and was neither reviewed nor approved by Management. Through inquiry with the Service Delivery Manager, we noted a lack of communication between HR and IT (e.g. no notification from HR informing of the next leavers). Furthermore, we noted that the online tool implemented to manage starters and leavers is not always used by managers. Through inquiry, we noted that the generic administrator account administrator.lbhf@lbhf.gov.uk was still active due to an artefact of previous environments, where the generic account was used to run automated admin jobs. However, this account is no longer in use and has a complex password.	Without policies and/or with outdated policies, the IT control framework may be weak, inconsistent or inefficient, especially on sensitive areas. The current process is exposed to human errors resulting potentially in accounts not being disabled in a timely manner.	The User Access Management policy should be reviewed and approved by Management to clarify and improve the link between HR and IT. The process should ensure leavers are pro-actively recorded in the online tool in order to allow IT to act upon accordingly. Management should consider to amend the process so that the notifications about new joiners/leavers/movers are issued by HR as it is often more efficient and reliable than line managers. Management should consider disabling the generic administrator account if no longer in use.

Management Response	
1) **User Access Management policy** – Agreed, the policy needs to be defined and documented. We already have monthly meetings with HR to address the problems identified above. **Target end December 2020**. 2) **Generic administrator account**. The generic administrator account referred to above administrator.lbhf@lbhf.gov.uk has now been disabled. We will review who has domain administrator accounts to ensure tighter control. **Target end July 2020**.	
Responsible Officer	**Deadline**
Quentin Brooks	31st December 2020

6. Malware Prevention

Priority	Issue	Risk	Recommendation
Low	Although anti-malware solutions are deployed across the infrastructure (firewall) and end user devices (laptops/ desktops), we noted that no documented policy was in place. Through inspection of the Intune policy configurations, we noted that neither anti malware nor application whitelisting was defined and configured on mobile devices.	Without policies the IT control framework may be weak, inconsistent or inefficient, especially on sensitive areas such as malware protection. The lack of application whitelisting or anti malware solution on mobile devices may facilitate their loss or compromise.	Management should define and approve an anti-malware protection policy. The policy should assign an owner and should be regularly updated to reflect the threat profile facing LBHF. It should stipulate the relevant roles both across entities (i.e. taking into account third parties) and across internal teams. For corporate mobiles, Management should consider implementing whitelisting to ensure only pre-authorised applications are installed and executed or install anti malware solutions.

Management Response
H&F has documented a new, anti-malware policy. (Evidence attached - 'anti-malware-policy-hf-1-1.docx') The policy is owned by the Technical Design Authority and is currently awaiting their review. The policy stipulates the required anti-malware protections for: end-user devices, servers, email services and internet gateway services in-use at H&F. It has recently been updated to make it explicit that H&F is using Google Play Protect rather than app white-listing to prevent malware being installed on corporate smartphones.

Responsible Officer	Deadline
Ed Crow (Representing TDA)	31st July 2020

7. Incident Management

Priority	Issue	Risk	Recommendation
High	The backup policy was not documented at the time of the audit. Furthermore, for a selected sample of months, we inspected the BT monthly report and could not find any information about the backups as the section was flagged as "N/A". But the audit has been informed that BT has started to add this information after our fieldwork. In addition, LBHF does not receive any evidence of successful restoration tests for the backups performed by third-parties. Through inspection of the H&F Service Continuity Plan, we noted that the document was last reviewed in September 2018. Furthermore, it was noted that the plan has not been tested in the last 12 months.	The backup policy currently implemented may either be insufficient, waste IT resources or not be aligned specifically to the business needs/ requirements. Furthermore, without testing the recoverability of the backups, only limited reliance can be placed on the back up procedures in place. In case of major incident, IT resources may not be available, in line with the business requirements and priorities.	A backup policy should be defined and implemented across all systems. LBHF should receive formal assurance that the backups are regularly tested (at least annually) through formal restoration tests and the results are followed-up. The Service Continuity Plan should be tested at least annually or after each major infrastructure change. The results of the test should be documented, and any lessons learned should be captured for updates to the plan, thus introducing a mechanism of improvement of the process.

Management Response	
1) **Backup policy** – Agree this is needed. Some back up notifications are in place but we will carry out a full review and document by end of December. 2) **Service Continuity Plan** - this document details how H&F Digital Services continues to provide a service to H&F. It is not a technical document that would be expected to hold details of backups. Although the point noted about the formal test of the Service Continuity Plan is correct, it is updated on a regular basis to reflect changes to the service – most recently is dated 9th April 2020 to include ongoing lessons learned through the Covid-19 pandemic. Evidence attached.	
Responsible Officer	**Deadline**
Quentin Brooks	31st December 2020

8. Removable Media

Priority	Issue	Risk	Recommendation
Low	LBHF does not have a formalised policy on removable media. Although the default configuration of end user computers blocks removable media, exceptions exist and we could not find reliable information on whether they are recorded and managed.	Without policies the IT control framework may be weak, inconsistent or inefficient, especially on sensitive areas such as malware protection.	Management should consider defining a removable media policy, especially to define the process to handle and track exceptions. If such devices are required, enterprise software should be used that can either configure systems to only allow access to specific USB or that will automatically encrypt all data placed on such devices.
Management Response			
H&F has documented its removable media policy. The policy is owned by the Technical Design Authority and is currently awaiting their review. The policy stipulates the required removable media controls for all devices that can connect directly to the H&F corporate network. The policy describes how end users can apply for exceptions, and how this will be recorded by the Service Desk.			
Responsible Officer			**Deadline**
Ed Crow (representing TDA)			30th June 2020

Appendix 2: Definition of Assurance Opinions and Recommendation Priorities

In order to help put the audit opinion and recommendation priority ratings in context the following tables detail the current ratings used by Internal Audit.

Rating	Description
Su	There is a sound system of control designed to achieve the objectives. Compliance with the control process is considered to be substantial and no material errors or weaknesses were found.
Sa	While there is a basically sound system, there are weaknesses and/or omissions which put some of the system objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
L	Weaknesses and / or omissions in the system of controls are such as to put the system objectives at risk, and/or the level of non-compliance puts the system objectives at risk.
N	Control is generally weak, leaving the system open to significant error or abuse, and/or significant non-compliance with basic controls leaves the system open to error or abuse.

Priority	Description
High	Recommendation addresses fundamental weaknesses, which seriously compromise the effective accomplishment of the system's objectives. Risks presented by the control weaknesses could be damaging in the short term. The management action required should be implemented as soon as possible, certainly within 0-3 months.
Medium	Recommendation addresses serious weakness, which affect the reliance to be placed on the system. Risks presented by control weaknesses could be damaging in the medium term. Management action is required within 0-6 months.
Low	Recommendation addresses minor weaknesses, or suggests a desirable improvement. Risks presented by control weaknesses are unlikely and inconsequential. Management action is recommended to address concerns within 0-9 months.

Appendix 3: Audit Scope & Limitations

This audit was a full risk-based review of the arrangements for Cyber Security arrangements and included the following areas:

Ref	Audit Area - Description	Comments on Coverage / Area Objectives
01	Governance	Sufficient awareness by decision makers of the risks and the determination of an appropriate risk appetite. Definition of the roles and responsibilities of the individuals and organisation responsible for cyber security. Determination of the capabilities and acquisition of the capacity needed to deliver on those responsibilities. Development, implementation and maintenance of the strategy/ policies needed. Operation of a system of checks to ensure ongoing compliance.
02	Culture, Awareness and User Education	Management support and endorsement of cyber secure culture. The effectiveness of user awareness and education programmes.
03	Secure Configuration	Recording of baseline and current configuration. Control of changes to configuration to ensure security. Software patching regimes.
04	Network Security	Intrusion detection systems, monitoring and response.
05	Identity and Access Management	Processes for adding, changing or removal of access. Management of privilege access of systems or individuals. Monitoring of user access logs.
06	Malware prevention	Updating of malware prevention software
07	Incident Management	Identification of security threats and vulnerability assessment. Monitoring and reporting of security incidents.
08	Removable Media	Review of policies on use of removable media and enforcement of those policies.

Limitations to the Scope of the Audit

The following limitations to the scope of the audit were agreed when planning the audit:

- The work will be undertaken using a risk-based approach and testing will be on a sample basis to verify compliance; and
- The audit review does not provide absolute assurance that material error, loss or fraud does not exist.

The internal audit approach was developed through an assessment of risks and management controls operating within the agreed scope. The following procedures were adopted:

- Identification of the role and objectives of each area;
- Identification of risks within each area which threaten the achievement of objectives;
- Identification of controls in existence within each area to manage the risks identified;
- Assessment of the adequacy of controls in existence to manage the risks and identification of additional proposed controls where appropriate; and
- Testing of the effectiveness of key controls in existence within each area.

Inherent Risks

The risks listed below are potential inherent risks which are common for any system/organisation of this type:

- Lack of awareness of cyber security risks and what good cyber security management practices should be followed allows the security of data, IT systems or individuals to be compromised.
- Business decisions are taken without a clear understanding of information assets, assessment of the risks and threats to those assets and a quantification of the risk appetite the organisation can accept.
- Insufficient organisational capability and capacity to deliver cyber security leads to risks not being mitigated to a tolerable level.
- IT systems are developed, or configuration changes made, that expose the organisation to cyber threats and vulnerabilities.
- Ineffective maintenance and vulnerability management exposes IT systems to external malicious activity.
- Poor control over user and privileged access leads to unauthorised access to data or IT systems for malicious purposes.

Appendix 4: Timetable and Distribution List

Stage	Date
End of Fieldwork	08/11/2019
Draft Report Issued	18/02/2020
Responses Received	10/07/2020
Final Report Issued	17/07/2020

Audit Team
Client Engagement Manager – Nicolas Guerin
Auditor – Damien Hoti

Auditee
IT Security Manager – Adrian Dewey
Service Director – Quentin Brooks Operations Manager - Katrine Nowicki Anthony King – Technical Architect Ed Crow - Head of information and data protection officer

Client Sponsor
Chief Information Officer – Veronica Barella

Report Distribution List
Chief Information Officer – Veronica Barella
Head of Information and Data Protection Officer – Edward Crow
Information Manager (interim) – Anthea Ferguson
IT Security Manager – Adrian Dewey
Operations Manager – Katrine Nowicki
Service Director – Quentin Brooks

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Recommendations for improvements should be assessed by management for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

This report is prepared solely for the use of Audit Committee and senior management of the London Borough of Hammersmith and Fulham. Details may be made available to specified external agencies, including external auditors, but otherwise the report should not be quoted or referred to in whole or in part without prior consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose.