CROYDON

Final Internal Audit Report

Firewall Management

October 2024

Distribution: Interim Assistant Chief Executive
Interim Chief Digital Officer & Director of Resident Access
Business Operations Manager
Technology and Architecture Manager
Information Security Manager
Senior Project Manager
Corporate Director Resources and S151 Officer
Finance Director and Deputy S151 Officer

Assurance Level	Issues Identified	
No Assurance	Priority 1	3
	Priority 2	3
	Priority 3	1

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Forvis Mazars LLP at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations and confidentiality.

forvis mazars

Contents

Page

Executive Summary

Detailed Report

Appendices

1. Introduction

1.1. In May 2023 the Croydon Digital Service (CDS) ended its managed service agreement with Capita, who amongst other services provided and supported the network, linking Council offices to IT services provided by Croydon Council (the Council) and its third-party suppliers and partners.

1.2. As Capita owned the network devices and MPLS network connections, which were subcontracted from communications partners, the transition of the managed network to the new network supplier (Adept) involved several activities with some extending beyond the termination of the general Capita managed service contract requiring contract extensions for individual network services.

1.3. While this change of network supplier has introduced processes that have not been assured by prior internal audits, the previous internal audit of cyber security was unable to gain assurance of the firewall management controls provided by Capita due to their reluctance to share information that they deemed sensitive.

1.4. Along with the onsite data centre at Bernard Wetherill House (BWH), the Council also has a growing suite of network services operating in Azure. While some internal firewalls are expected to protect network traffic between the Councils' offices and Azure, the most significant risks to manage are at the network perimeter and therefore this audit focussed on the management of perimeter firewalls.

1.5. The Council has 30 sites on its network, each with its own perimeter firewalls. Most of the services are in Microsoft Azure network, which is protected by a Palo Alto virtual firewall, whilst other sites use Cisco and FortiGate firewalls.

1.6. The responsibilities of managing these sites, including their firewalls is split between the Council and third-party service providers. The Palo Alto firewall is managed by Version One (third party). Cisco firewalls are managed internally by the Council and FortiGate firewalls are managed by Wavenet (third party).

1.7. This audit has been undertaken as part of the agreed Internal Audit Plan for 2023/24 and has assessed the adequacy of the perimeter firewall management controls.

2. Key Issues

Priority 1 Issues
The Council had inadequate coverage of penetration tests over all firewalls as the scope of quarterly penetration tests was only limited to Palo Alto firewalls and did not include Cisco or FortiGate firewalls. Furthermore, the vulnerabilities identified from these penetration tests lacked ongoing monitoring and remediation. **(Issue 1)**
The Council had not regularly updated and patched the firewall firmware. On conducting a sample-based testing for four firewalls, Internal Audit observed that one firewall (BWH Cisco) was running on an outdated firmware, and the other three firewalls were not updated and patched to the latest releases. **(Issue 4)**
Intrusion detection and prevention was not enabled on the firewalls by the Council, and there was a lack of deep-level packet inspection and malware protection. **(Issue 5)**

Priority 2 Issues
There was inadequate logging and monitoring of firewall logs due to the lack of an implemented 'Managed Threat and Response' service. Inconsistencies were observed in the sample-based testing of firewalls with respect to insufficient coverage of logs, absence of monitoring and inconsistent log retention. **(Issue 2)**
Inadequate password policy was observed on all the four firewalls during a sample based testing and administrative console credentials were not changed since the exit of Capita services and internal personnel change. **(Issue 3)**
Absence of a periodic rule review process for all the firewalls was noted, and redundant and inactive outbound rules were observed on three out of four firewalls in a sample-based testing. **(Issue 6)**

The one 'Priority 3' issue is included under Section 4 below.

3. Actions and Key Findings/Rationale

Audit Area: Firewall Management and Governance

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 1
1	a) The scope of the PEN testing has been expanded to include all firewalls and a proposal to perform bi-annual penetration testing is ready– the implementation of this proposal is subject to a business case currently going through the approval process. b) There is an organisational restructure awaiting approval which will look to ensure that there is a permanent Security Manager in place and that they also have sufficient staff in their team to support the monitoring and management of security vulnerabilities.	**Expected Control** The Council should conduct regular penetration testing of all firewalls to simulate real world attack scenarios to identify weaknesses in the network security infrastructure. Additionally, vulnerability identified by the penetration test should be promptly addressed to maintain the effectiveness of the firewall in safeguarding sensitive data and preventing unauthorised access to the network. **Finding/Issue** The Council conducts quarterly penetration tests for its network. However, from Internal Audit inspection of the penetration test reports, it was observed that the scope of these penetration tests was only limited to Palo Alto firewalls which covered the Azure network and did not include Cisco or FortiGate firewalls protecting the remaining twenty-nine sites of the Council. Furthermore, the vulnerabilities identified from these penetration tests lacked ongoing monitoring and remediation. We were informed by the Technology and Architecture Lead that a centrally managed spreadsheet, traditionally used for tracking vulnerability closures, was currently unavailable due to the departure of the contractor who played the role of Cyber Security Manager (which changed twice in the last 12 months). Consequently, the Councils reliance on contractors to fulfil roles that operate key controls does present a risk due to their capacity to move to other organisations at short notice. **Risk** Without regular penetration testing of all perimeter firewalls, potential weaknesses in firewall defences may go undetected, exposing the Council to the risk of unauthorised access and data breaches. Furthermore, absence of tracking and resolving vulnerabilities can leave firewalls susceptible to exploitation, as security gaps remain unaddressed.

Responsible Officer	Deadline
Information Security Manager	December 2024

Audit Area: Security Monitoring

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 2
2	A review of all firewalls has been completed and the following actions are in Progress. a) 13 EOL firewalls are being replaced with CISCO Meraki, the logs will be configured to align with Firewall Management Policy. b) Extra disk space will be added to the Firewalls in Azure to capture the logs in alignment with Firewall Management Policy. – Issue resolved c) The suppliers managing the in support on-prem firewalls have been asked to setup the logging in alignment with the council's firewall management policy. d) A business case has been submitted to request funding for a log monitoring service.	**Expected Control** Firewall logs should be captured and monitored to maintain a detailed record of network traffic, including attempted breaches and suspicious activities, which are crucial for incident response and forensic analysis. The Council's Firewall Management Policy also states the logs should be retained for a minimum of one year and alerting should be enabled on all firewalls. **Finding/Issue** On conducting sample-based testing for four firewalls, inconsistencies in logging and monitoring were observed and gaps noted as follows: • Davis House (FortiGate): This firewall is managed by a third party, Wavenet; and log retention for the firewall logs was noted to be seven days as the Council did not have any subscription. Thus, the logs were not retained in line with the Council's policy. • BWH and Town Hall (Cisco): The firewalls are managed internally by the Council, and logs need to be manually monitored as there is no Security Information and Event Management (SIEM) solution deployed for centrally managing all logs. However, we were informed that there is currently no monitoring conducted. Only access logs were captured for the firewall and there was no alerting mechanism set up. • Azure (Palo Alto): This firewall is managed by a third party, Version One; and the firewall logs were captured on the device with 15 GB default space. However, no evidence was provided to verify the types of logs captured and their retention period and thus, no assurance could be provided on effectiveness of the controls by Version One.

		Risk
Responsible Officer	Deadline	The risk of unresolved or undetected vulnerabilities increases if actions to resolve or risk accept vulnerabilities are not tracked, detected and responded to promptly. Without rigorous monitoring of vulnerabilities, the Council may not have a clear understanding of its security risks and upon the completeness of security updates applied by its IT service providers.
Service Delivery Manager (a)	Firewalls will be replaced between August & December 2024	
Service Delivery Manager (b)	Completed	
Business Operations Manager (c)	December 2024	
Interim Chief Digital Officer (d)	December 2024	

Audit Area: Administrative Console

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 3
2	a) Azure Firewalls – Complex Passwords have been implemented and confirmation that the firewalls can only be accessed via an internal jump box resolves the issue of whitelisting. – Issue resolved b) On-Prem Firewalls (CISCO & FortiGate) – The supplier managing these firewalls has been asked to rectify these issues ASAP, we are still awaiting a plan from the suppliers regarding this work. This is being escalated with the suppliers' directors.	**Expected Control** The firewall console, used by the administrators for managing and configuring the firewalls, should be protected by strong passwords along with changing the default passwords provided by the suppliers. Controls to restrict access to the firewall console such as IP whitelisting should also be configured. **Finding/Issue** It was observed that the firewall administrator console credentials for a sample of four firewalls selected had not been changed since the exit of Capita services and internal personnel change. On conducting a sample-based testing of four perimeter firewalls, the following weaknesses were observed. 1. BWH (Cisco) - There was no complex password policy defined for access to the administrative console of the firewall. 2. Azure (Palo Alto) - Inadequate password policy was configured as the only complexity defined in the policy was 'minimum length should be 8 characters'. 3. Town Hall (Cisco) - There was no complex password policy defined for access to the administrative console of the firewall. 4. Davis House (FortiGate) - No password policy was provided for inspection. IP whitelisting was not enabled, but we were informed that once Wavenet gains confidence that the firewall is operating as expected due to its recent implementation, this will be applied. Also, there was no MFA enabled on the firewall.
Responsible Officer	**Deadline**	

Service Delivery Manager (a) Business Operations Manager (b)	Completed December 2024	We were also informed that the default passwords had been changed for all the firewalls and also noted controls in place to restrict access to the firewall console from the internet through IP whitelisting. **Risk** Weak, non-complex, or unchanged passwords increases the risk of unauthorised access and leaving the firewall vulnerable to exploitation by malicious actors, potentially compromising network security.

Audit Area: Firewall Configuration

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 4
1	A full review of all the council's firewalls has been completed and the following actions have been taken. a) Azure Firewalls – Firmware has been upgraded - Issue resolved. b) 13 EOL on-prem CISCO firewalls on-prem Firewall can't be updated, these firewalls are being replaced. c) On-Prem Firewalls (CISCO & FortiGate) – All CISCO	**Expected Control** As an accepted security practice and in alignment with the Council's 'Firewall Management Policy', all firewalls must run on the current and supported version of the supplier's operating software, and not run on outdated firmware. Firmware is a software that is embedded into the firewalls to control its operations. **Finding/Issue** On conducting sample-based testing for four firewalls, it was observed that one firewall (BWH (Cisco)) was running on an outdated firmware, and the other three firewalls were not operating with the latest firmware release as follows:

firewalls have been upgraded to the latest software excluding the EOL devices which are being replaced as we can no longer get support on them. The majority of the Fortinet Firewalls have been patched to a newer firmware, a handful failed and are being looked at.

Responsible Officer	Deadline
Service Delivery Manager (a)	Completed
Service Delivery Manager (b)	Firewalls will be replaced between August & December 2024
Business Operations Manager (c)	06/09/2024

- BWH (Cisco) - This firewall was running on outdated firmware, version Cisco ASA 9.9(2) 61, which had reached its end of life and support on May 31, 2023. The latest version for Cisco ASA is 9.20(x).
- Azure (Palo Alto) - This firewall was running on a legacy PAN-OS version for PA VM-300 version 10.1.10, however, the latest release is version 11.1. The current version is 10.1.10 that is in support until December 2024.
- Town Hall (Cisco) - This firewall was running on firmware Cisco ASA 9.12(4) which is supported until February 28, 2026. However, the latest series for Cisco ASA is 9.20(x).
- Davis House (FortiGate) - The firewall was running on FortiOS v7.0.14, however, the latest version for FortiOS is v7.4.3. The current version 7.0.14 has its end of engineering support in March 2024 and end of support in September 2025.

Risk

Outdated firmware may contain known vulnerabilities that could be exploited by attackers to gain unauthorised access to the network, compromise sensitive data, or disrupt operations. Without the latest firmware updates, the Council is leaving their systems susceptible to exploitation by cyber threats, as outdated firmware may lack security features, performance enhancements, and compatibility fixes present in newer versions.

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 5
1	Currently there are no monitoring services available or resources to manage this service. A business case has been submitted to request funding for an IDS/IPS monitoring service. If funding is approved this service will be turned on.	**Expected Control** Intrusion detection and prevention should be enabled on all firewalls to analyse network traffic in real time to detect and prevent suspicious or malicious activities. **Finding/Issue** Intrusion detection and prevention system was not enabled on any of the firewalls, and there was a lack of deep-level packet inspection and malware protection to block malicious traffic at the network level and safeguard against advance threats and cyber-attacks. We were informed by the Technology and Architecture Lead that firewall management had not received sufficient attention thus far, leading to such shortcomings. While the Council is aware of this deficiency, they plan to address this soon. **Risk** The network is more susceptible to unauthorised access attempts, malicious activities, and potentially undetected security breaches. IDS/IPS play a crucial role in monitoring and analysing network traffic, detecting suspicious or anomalous behaviours, and actively preventing intrusions in real-time.

Responsible Officer	Deadline
Interim Chief Digital Officer	December 2024

<table>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 6</th></tr>
<tr><td><b>2</b></td><td colspan="2">All firewall rules have been reviewed and a date has been put in the diary to review them again in 12 months’ time – Issue resolved.</td><td rowspan="3"><b>Expected Control</b>
Firewall rule reviews should be regularly conducted to identify outdated and unnecessary rules, and to enhance the overall effectiveness of the firewall in protecting the network infrastructure.
<b>Finding/Issue</b>
We were informed by the Technology and Architecture Lead that no firewall rule reviews were conducted for any of the firewalls. From sample-based testing for four firewalls, it was observed that three firewalls, i.e., BWH Cisco, Azure Palo Alto and Town Hall Cisco, had redundant outbound rules as there was no rule review process in place. Analysis also indicated that several firewall rules were inactive, as evidenced by the absence of traffic flow and there was no justification available for their existence.
<b>Risk</b>
Unnecessary outbound connections can pose a risk of providing avenues for data theft or communication with malicious entities. Absence of a firewall rule review, would further increase the risk of failing to identify such unnecessary rules and potentially allowing unauthorised access.</td></tr>
<tr><th colspan="2">Responsible Officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Service Delivery Manager</td><td>Completed</td></tr>
</table>

4. Priority 3 Finding

Agreed action	Findings
Control Area: Firewall Management and Governance **Action proposed by management:** The Policy was reviewed and approved in July 2024 the monitoring system has been setup to alert the Council's security manager next year when it is due for review again. **Responsible Officer:** Information Security Manager **Deadline:** Completed	**Expected Control** As an industry best practice, it is recommended that all policies should undergo an annual review and be approved by the management. **Issue/Findings** The Council had defined a 'Firewall Management Policy', which provided detailed guidance on the security and management of firewalls. However, we observed that the Firewall Management Policy, did not undergo annual review and was last reviewed in November 2020. **Risk** With the dynamic nature of cyber threats, an outdated policy may leave vulnerabilities unaddressed, increasing the likelihood of unauthorised access or data breaches. It may also result in potential compliance violations, and an overall diminished ability to safeguard sensitive information and crucial systems.

Appendix 1

AUDIT TERMS OF REFERENCE

Firewall Management

1. INTRODUCTION

1.1 In May 2023 the Croydon Digital Service (CDS) ended its managed service agreement with Capita, who amongst other services provided and supported the network, linking Council offices to IT services provided by Croydon Council (the Council) and its third-party suppliers and partners.

1.2 As Capita owned network devices and subcontracted the MPLS network connections from communications partners, the transition of the managed network to the new network supplier (Adept) involved several activities with some extending beyond the termination of the general Capita managed service contract requiring contract extensions for individual network services.

1.3 While this change of supplier has introduced processes that have not been assured by prior internal audits, the previous internal audit of cyber security was unable to gain assurance of the firewall management controls provided by Capita due to their reluctance to share information that they deemed sensitive.

1.4 As well as the onsite data centre at Bernard Wetherill House, it also has a growing suite of network services operating in Azure. While some internal firewalls are expected to protect network traffic between the Councils’ offices and Azure, the most significant risks to manage are at the network perimeter and therefore this audit will focus on the management of perimeter firewalls.

1.5 This audit has been undertaken as part of the agreed Internal Audit Plan for 2023/24 and has assessed the adequacy of the firewall management controls.

2. OBJECTIVES AND METHOD

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.

2.2 The audit will for each controls / process being considered:

- Walkthrough the processes to consider the key controls
- Conduct sample testing of the identified key controls, and
- Report on these accordingly.

3. SCOPE

3.1 This audit, focused on firewall management, was undertaken as part of the 2023/24 Internal Audit Plan. The specific scope included the following areas and identified issues:

Audit Area	Identified Issues		
	Priority 1 (High)	**Priority 2 (Medium)**	**Priority 3 (Low)**
Firewall Management and Governance	1	0	1
Security Monitoring	0	1	0
Access to the Administrative Console	0	1	0
Firewall Configuration	2	1	0
Change Management	0	0	0
Totals	**3**	**3**	**1**

Appendix 2

Definitions for Audit Opinions and Identified Issues

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

🟢	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are constantly applied.
🟡	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance of the controls which may put this achievement at risk.
🟠	Limited Assurance	There are significant weaknesses in key areas of system controls and non-compliance that puts achieving the system objectives at risk.
🔴	No Assurance	Controls are non-existent or extremely weak, leaving the system open to the high risk of error, abuse, and reputational damage.

Priorities assigned to identified issues are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, still provides an opportunity for improvement. May also apply to areas considered to be of best practice that can improve for example the value for money of the review area.

Appendix 3

Statement of Responsibility

We take responsibility to London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.