INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Infrastructure Security
TO:	Deputy Chief Executive (AJ)	**DATE:**	29 October 2019
C.C.	Chief Executive Head of Finance ICT Services Manager Portfolio Holder – Cllr. Day		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2019/20 an audit review of the Council's Infrastructure Security was completed in September 2019. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 The ICT Services team has proactively undertaken a number of measures to protect the security and resilience of the Council's network infrastructure. The network domain is protected by a suite of vendor supported Cisco firewall appliances. Firewall security is supplemented by the deployment of an Intrusion Prevention system. Network security measures are subject to independent review through a programme of annual external penetration testing.

2.2 This audit was undertaken to ensure the security, integrity and availability of the Council's network infrastructure.

3 Scope and Objectives of the Audit

3.1 The objective of the report was to ensure the integrity and availability of the Council's network infrastructure

3.2 Testing was performed to confirm that controls identified operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on discussions with relevant staff.

3.3 The audit was designed to assess and provide assurance on the risks pertaining to the following key areas:

- Programme of external penetration testing;
- Public Services Network (PSN) Code of Connection;
- Firewall Security including review of firewall rules;
- Patching of Firewall appliances;
- Review of firewall logical security settings and restriction on superuser rights;
- Failover protection; and
- Intrusion Prevention System (IPS) protection.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as this is the first audit of this area.

4.2 External Penetration Testing

4.2.1 The Cyber Essentials Scheme guidelines on Secure Configuration recommend:

'Ensure that computers and network devices are properly configured to

- *reduce the level of inherent vulnerabilities*
- *provide only the services required to fulfil their role'*

4.2.2 Penetration testing, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. It can be automated with software applications or performed manually. The process involves gathering information about the target before the test, identifying possible entry points, attempting to break in and reporting back the findings. The main objective of penetration testing is to identify and resolve any security weaknesses.

4.2.3 Audit testing confirmed that NTA Monitor had been commissioned to undertake both internal and external security testing on the Council's network domain. All reported vulnerabilities were captured in an ICT Action Plan and tracked through to resolution.

4.3 PSN Code of Connection

4.3.1 The Public Services Network (PSN) is the UK government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. To obtain PSN accreditation, all Councils must complete and submit a Code of Connection to the Cabinet Office together with supporting information including a Network Diagram and IT Health Check (ITHC) report. The ITHC report summarises all corrective action undertaken following the annual external penetration test.

4.3.2 Audit testing confirmed that the ICT Services team successfully renewed their PSN Code of Connection on 16 January 2019.

4.4 **Review of Firewall Rules**

4.4.1 The Cyber Essentials Scheme guidelines on Firewalls recommend:

- *ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation; and*
- *remove or disable permissive firewall rules quickly, when they are no longer needed.*

4.4.2 Firewall appliances restrict incoming and outgoing network traffic and determine whether to block or allow traffic against a predefined set of firewall rules.

4.4.3 We were able to confirm that firewall rules were subject to regular review. Examination of firewall rules forms part of the annual PSN security testing. And audit testing on the Cisco platform verified that all insecure or unencrypted network services had been disabled.

4.5 **Patching of Firewall Appliances**

4.5.1 The Cyber Essentials Scheme guidelines on Patch Management recommend:

'Ensure that devices and software are not vulnerable to known security issues for which fixes are available.'

4.5.2 A review of patch management across the firewall server estate identified firewall appliances that had not been patched for significant period of time. For example:

Device Type	**Server**	**Date Last Patched**
Cisco - ASA5525-X	WDC-RH-5525-FW-01	07-Dec-18
Cisco - ASA5545-X	WDC-RH-5545-FW01	30-Mar-17
Cisco - ASA5516-X	Warwick-VPN-ASA	13-Feb-18

4.5.3 To address this issue, ICT Services have sought technical sought from both the firewall vendor (Cisco) and BT. Work is in progress to ensure that all Council firewalls are upgraded to the latest and most stable software release.

Risk

The failure to promptly apply all new security patches contravenes CES security guidelines and may allow unauthorised access to the live network domain.

Recommendation

Firewall appliances should be upgraded to CISCO's recommended Code version.

4.6 **Review of Firewall Logical Security Settings**

4.6.1 The Cyber Essentials Scheme guidelines on Firewalls recommend:

'prevent access to the administrative interface (used to manage firewall configuration) from the Internet, unless there is a clear and documented business need'

4.6.2 Audit testing confirmed that administration access rights on the Council's Cisco firewall estate were restricted to valid, authorised and uniquely identifiable members of the ICT Services technical support team. In addition, firewalls are only accessible via designated workstations in ICT Services.

4.6.3 Examination of the Cisco 'Password Policy' confirmed that password complexity was enabled and a restriction on account lockout set at 3 failed login attempts.

4.6.4 However, audit testing disclosed that the Minimum Password Length was set at only 6 characters. In addition, password history settings had not been enabled to prevent reuse.

Risk

There could be unauthorised access through the use of weak or easily guessable passwords.

Recommendation

The Cisco 'Password Policy' security settings should be reviewed to enforce password history (12) and password minimum length (8).

4.7 Failover Protection for Firewall Appliances

4.7.1 Firewall appliances are security devices that restrict incoming and outgoing network traffic and determine whether to block or allow traffic against a predefined set of firewall rules. It is good practice to deploy firewall appliances in pairs so that they can provided failover in the event of the loss of a single appliance.

4.7.2 Examination of the Council's network topology confirmed that a pair of Cisco firewall appliances had been deployed to protect the Council network domain. As an additional safeguard, a copy of all firewall rules was backed up weekly to the Council's Storage Area Network (SAN).

4.8 Intrusion Prevention Protection

4.8.1 An Intrusion Prevention System (IPS) monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log information and block malicious activity at source.

4.8.2 Audit testing confirmed that ICT Services had acquired a Cisco IPS system to supplement existing firewall protection. However, at the time of our review

the IPS application was only configured to log rather than block malicious network traffic.

4.8.3 Discussions with ICT Services established that they were actively arranging additional technical support to fully configure and enable the IPS system.

4.8.4 In the interim, ICT Services have documented and tested Business Continuity arrangements in place. In the event of a Denial-of-Service attack, Virgin Media, the Council's Internet Service Provider (ISP), would be contacted to block all malicious traffic directed towards the Council's network.

Risk

There could be reputational damage and system downtime from a denial-of-service attack.

Recommendation

The Cisco IPS system should be actively configured to block all malicious network traffic.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did identify two Medium rated issues and one Low rated issue which, if addressed, would improve the overall control environment. As a result, the findings are considered to give SUBSTANTIAL assurance around the management of database security risks.

5.1 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Infrastructure Security – October 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.3	Firewall appliances should be upgraded to CISCO's recommended Code version.	The failure to promptly apply all new security patches contravenes CES security guidelines and may allow unauthorised access to the live network domain.	Medium	ICT Services Manager	Agreed. Some of the Council's firewalls are currently being replaced. Once this is complete, all remaining Firewalls will be updated and maintained to Cisco's latest recommended code version.	Apr 2020

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.6.4	The Cisco 'Password Policy' security settings should be reviewed to enforce password history (12) and password minimum length (8).	There could be unauthorised access through the use of weak or easily guessable passwords.	Low	ICT Services Manager	Agreed. The Council operates several Firewalls and the changes need to be implemented cautiously to avoid lockouts.	Jan 2020
4.8.4	The Cisco IPS system should be actively configured to block all malicious network traffic.	There could be reputational damage and system downtime from a denial-of-service attack.	Medium	ICT Services Manager	Agreed. IPS was originally configured to run in monitoring mode to obtain sufficient data to identify network false positives. Discussions were already being undertaken at the time of the audit to schedule an appropriate time for IPS to become active.	Feb 2020

* Risk Ratings are defined as follows:

High Risk:	Issue of significant importance requiring urgent attention.
Medium Risk:	Issue of moderate importance requiring prompt attention.
Low Risk:	Issue of minor importance requiring attention.