INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	ICT Remote Access
TO:	Deputy Chief Executive (AJ)	**DATE:**	6 March 2018
C.C.	Chief Executive Head of Finance ICT Services Manager Desktop Services Manager Portfolio Holder (Cllr AM)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2017/18 an audit review of remote access controls was completed in February 2018. 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 This audit was undertaken to gain a level of assurance on data security or management control weaknesses in the introduction, operation and management of devices which work remotely from the Council's network infrastructure.

3 Scope and Objectives of the Audit

3.1 The objective of the report was to review and appraise the adequacy of the systems and controls in place to ensure that remote working arrangements are secure and that devices are appropriately managed.

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

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

- Council policies and procedures relating to remote access
- Access protocols to network infrastructure and data
- Transmission protocols
- Mobile device management
- Mobile device security.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 The current position in respect of the recommendations from the audit reported in February 2013 is as follows:

Recommendation	Management Response	Current Status
1 Potential mechanisms for preventing uncontrolled access to the internet from Council-issued laptops and tablets should be investigated with a view to implementation.	The Council wishes to allow controlled Internet access from non-council locations to support the Agile Working agenda. In response the Council has upgraded its existing Sophos product suite to enable non-council gateway access to the Internet whilst enforcing content filtering policies.	Completed. Web filtering software is used to block access to sites which are classified inappropriate material and sites when connected to the Council network.
2 The potential for monitoring failed log on attempts and locked accounts should be investigated with a view to identifying key security events.	The Council retains log files for the all the remote access methods identified. The logs contain details of key security events, such as failed logons and can be used for investigative purposes. However to correlate the logs in a proactive and meaningful way that would to identify trends would require log management and/or Intrusion Detection Software. The costs and the resources required to undertake further action is not warranted. This approach has been declared to CESG as part of our CoCo assessment and has been accepted.	Completed. Failed logon attempts are logged and available for review in the event they are required as part of an investigation.
3 Periodic monitoring of devices connected via Active Sync for synchronised downloads should be introduced.	A procedure has been put in place to monitor which devices connect to the Council's email system via Active Sync. Any breaches will be reported to an appropriate authority.	Completed. Reporting on connected devices is periodically reviewed for anomalies such as any devices that are not Council owned.

4.2 Policies & Procedures

4.2.1 The ICT policies and procedures relevant to the management of remote access were identified and obtained during the review. These were used in the process of reviewing the suitability of the controls in in operation at the Council.

4.2.2 Policies identified as being of relevance to this review are as follows; Remote Working Policy, Information Security and Conduct Policy, Internet Acceptable Usage and Email Acceptable Usage.

4.2.3 User responsibilities in relation to secure remote working are detailed in the Remote Working Policy, which also provides information on the security procedures to be applied when remotely accessing the Council network and when using mobile devices.

4.2.4 ICT policies are made available to all staff via the Council's intranet. Key messages from the policies are included in the mandatory online training packages that are completed by all staff as part of the Council's induction process.

4.2.5 Policies were found to be subject to regular review and revision and, where required, this was on at least an annual basis. The policies include sections for version control, a revision history and details of the relevant ICT staff who own and are accountable for the policy.

4.3 Authentication & Transmission Protocols

4.3.1 The methods used to manage and enable remote access to the Council network are; secure VPN using the Cisco AnyConnect Secure Mobility Client, some use of the Horizon View VMware tool, and smartphone access to email using Microsoft Active Sync. Each of the methods require authentication via the network / Active Directory plus an additional stage i.e. the use of tokens and / or PIN numbers.

4.3.2 Through review of the version information and recent IT health check reporting it was noted that the version of AnyConnect in use at the Council at the time of review was a version susceptible to a known 'high' rated vulnerability which could potentially allow an attacker with valid user credentials to install and run an executable file with a significant privilege levels. It is understood management are investigating options to mitigate this risk.

Risk

An attacker may be able to exploit a known vulnerability and run scripts compromising the confidentiality, integrity and / or availability of Council systems.

Recommendation

ICT Management should upgrade to Cisco AnyConnect Secure Mobility Client version 4.3.4019.0 or later, which is not affected by the known vulnerability.

4.3.3 Requests to grant home / remote working privileges to users are handled and processed by the ICT helpdesk. These are generally made in the form of an email from the user's Team Leader authorising the user for remote working, which is then logged and processed by ICT.

4.3.4 It was noted that there is no form currently in use to ensure a standardised process has been followed when setting up users for remote access and that a consistent audit trail of authorisation activities is maintained.

Risk

Processes may be followed inconsistently leading to users being granted incorrect or unauthorised access privileges.

Recommendation

ICT should add a standard change process / check sheet to the system to provide an audit trait of remote working authorisations and activities.

4.4 Mobile Device Management

4.4.1 The 'InTune' mobile device management tool is used to manage and control device security, including management of Councillor and WDC issued iPads and WDC Android devices connecting to the Council network. Security settings for these devices were obtained and reviewed as part of the audit and found to be an effective baseline for the security of the devices. Key requirements of this policy are detailed below.

4.4.2 Mobile devices access to Council data is secured via the use of a Virtual Private Network (VPN). The policy requires that users authenticate to the devices using passwords, the device must be locked after 15 minutes of inactivity by the user after which the user is prompted to re-enter the password, and the user is prevented from reusing the previous 24 passwords.

4.4.3 Council issued devices are subject to encryption, with any device detected by the management software as being jailbroken or rooted i.e. devices identified as being modified in such a way as to bypass the devices security controls, being prevented from accessing the Council network.

4.4.4 Councillor owned devices are subject to the following additional controls: the PIN is reset after five incorrect attempts, the user is restricted from saving files to the device itself and from cutting and pasting data from apps.

4.4.5 InTune managed devices can be remotely wiped using the administrative interface. This option is used in the event it is lost or stolen and can either delete all Council application data held on the device or fully wipe and return to factory settings, depending on whether the device is Council or privately owned.

4.5 Mobile Device Security

4.5.1 The Council makes use of the Exchange Active Sync Service (EAS) to secure and provide access to corporate e-mail using WDC owned mobile devices such as smartphones.

4.5.2 The process of transferring and synchronising email to local device storage is managed via EAS. Staff with Council owned smartphone devices are

permitted to access email, with a limited number of members permitted to access email via their own devices.

4.5.3 Policy settings were obtained and reviewed and it was determined that EAS is used to enforce the requirement that WDC phones are protected by a four digit PIN code. Devices that do not have a PIN code set are prevented from accessing and receiving e-mail. The system also blocks access to email after four failed login attempts.

4.5.4 Data stored on Council laptops is further protected from unauthorised access through use of Bitlocker protection which encrypts all data stored locally on all Council owned machines.

5 Conclusions

5.1 The audit identified one medium and one low rated recommendation, giving a SUBSTANTIAL level of assurance around the management of remote access to the Council network.

5.2 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 ICT Remote Access – March 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.2	ICT Management should upgrade to Cisco AnyConnect Secure Mobility Client version 4.3.4019.0 or later, which is not affected by the known vulnerability.	An attacker may be able to exploit a known vulnerability and run scripts compromising the confidentiality, integrity and / or availability of Council systems.	Medium	ICT Infrastructure Manager	Accepted – The upgrade of AnyConnect is scheduled for 6th March 2018.	No further action.
4.3.4	ICT should add a standard change process / check sheet to the system to provide an audit trait of remote working authorisations and activities.	Processes may be followed inconsistently leading to users being granted incorrect or unauthorised access privileges.	Low	Desktop Services Manager	Accepted – A standard change checklist has been produced which is linked to a helpdesk request for remote access.	No further action.

* 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.