INTERNAL AUDIT REPORT

FROM: Audit and Risk Manager

TO: ICT Services Manager

C.C. Chief Executive
Deputy Chief Executive (AJ)
Head of Finance

SUBJECT: ICT Infrastructure and Resilience Framework

DATE: 5 March 2015

1 INTRODUCTION

1.1. In accordance with the Audit Plan for 2014/15, an examination of the Council's ICT Infrastructure and Resilience Framework was completed in February 2015. This report is intended to present the findings and conclusions for information and action where appropriate.

1.2. Wherever possible, results obtained have been discussed with the staff involved in the various procedures examined and their views are incorporated as appropriate in any recommendations made. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 SCOPE AND OBJECTIVES OF AUDIT

2.1 The audit was undertaken in order to report a level of assurance on the controls in place to ensure the security and resilience of the Council's ICT infrastructure.

2.2 The audit comprised an evidential risk-based review and appraisal of the following key aspects of the infrastructure:

Network structure and design;
Firewall security;
Anti-virus and malware applications;
Active Directory/ Desktop management;
Backup and Disaster Recovery (DR) arrangements.

2.3 The audit was conducted through discussion with ICT management, the infrastructure team and other relevant staff with reference to documents and system records and/or evidence as appropriate. The principal contacts were Ty Walter (ICT Services Manager), Richard Bates (ICT Infrastructure Manager) and Lee Millest (Desktop Services Manager).

3 FINDINGS

3.1 Network Structure and Design

3.1.1 The Council's network is documented and described in a series of network and topology diagrams. These include 'Warwick DC Network Diagram', 'Riverside House LAN Fibre Topology' and 'Cisco PIX Diagram'.

3.1.2 The Warwick District Council (WDC) network environment is protected by a suite of Cisco firewall appliances and subject to both internal and external penetration testing. Sophos anti-virus software is deployed at the network and desktop level, incorporating on-access scanning plus scanning of email and internet access. Firewall and Anti-virus / malware controls are discussed further in 3.2 and 3.3 below.

3.1.3 It was noted that there is an absence of any intrusion prevention system (IPS) installed at the network perimeter which would identify, log, block and report any malicious network activity. This had also recently been raised in the audit of ICT Risks. Management advised us that the Council had decided against the implementation of an IPS as "*The resource requirements to implement intrusion prevention technology exceeds those available to the Council. Implementation without the necessary resource will result in excessively tolerant settings to prevent false positives and will result in poor value for money and will not improve the Council's security posture*."

3.1.4 As this issue has been raised by Internal Audit and considered by management previously no recommendation is forthcoming on this occasion.

3.1.5 Staff access to the internet via the network is restricted via the use of firewall and proxy servers. In order to minimise risks around staff access to high risk internet sites and malicious software being introduced into the network through web site access, all internet access is filtered and access to unsuitable sites blocked accordingly.

3.1.6 All Council laptop and tablet computers have disk encryption implemented using Microsoft 'Bitlocker' encryption. This ensures that data cannot be accessed on mobile computers without appropriate credentials, restricting access to data on the machine and minimising the risk of unauthorised access to the network in the event of the loss or theft of the machine.

3.1.7 Use of unauthorised USB devices is restricted on the network using the Sophos 'Endpoint' system. In order to address the risk of theft of corporate data USB access is restricted by default and limited to a small number of IT staff who require access as part of their day-to-day duties.

3.2 Firewall Security

3.2.1 Audit review of network infrastructure confirmed the WDC network environment is protected by a suite of internal and external Cisco firewall appliances.

3.2.2 Review of logging settings on the internal firewall confirmed they are configured to capture and record activities including; log-in attempt success and failure, administrator activities performed and changes to firewall configuration. It was found through review of firewall configuration settings and discussion with infrastructure team staff that this logging is not in place for the external firewall devices.

Risk
The absence of sufficient firewall logging may impair the identification and/or analysis of network activity in the event of a security breach.

Recommendation
The infrastructure team should review options around enabling firewall logging on the external firewalls.

3.2.3 A review of user access rights on the WDC firewalls revealed the following generic accounts:

Firewall	**Account Name**
WDC-RH-5525-FW-01	warwick-support
Warwick-FW-warickdc.gov.uk	warwick-support

Management advised us that the ‘warwick-support’ account is a shared administrator account used by the infrastructure team to make changes to firewall configuration settings and rulesets.

Risk
The use of shared or generic accounts removes accountability for activities performed and increases the risk of unauthorised access to the firewalls.

Recommendation
The ‘warwick-support’ account should be disabled on each of the firewalls and replaced with named individual administrator accounts for those requiring access.

3.3 Anti-virus and Malware

3.3.1 The Council has adopted a multi-layered approach to anti-virus and malware prevention and detection, with virus protection controls being deployed at the internet / network gateway level, at the network / server level and on individual laptop and desktop machines.

3.3.2 Internet gateway controls include:

perimeter located SPAM detection is used to reduce the risk of virus infected e-mails reaching the Council’s e-mail server;

anti-virus solutions from two separate vendors (Kaspersky & Sophos) are used to scan inbound e-mail traffic;

an annual penetration test is undertaken by third party ‘Arisiti’ in order to identify weaknesses in the security of the network perimeter;

use of an internet proxy to restrict staff access to unwanted or unauthorised high risk sites.

3.3.3 At the server level anti-virus software is installed on the Council's servers where approval has been obtained from the application vendor and it has been determined that server performance is not compromised. All servers are backed up by the infrastructure team to mitigate the risk of a virus infection.

3.3.4 Desktop and laptops are protected against malware via the use of Sophos. Automatic updating of virus definitions and updates is enabled to ensure machines are protected from the latest threats. Sophos is also used to restrict access to read/write from USB keys and external hard drives, to minimise the risk of viruses being introduced via that channel.

3.4 Active Directory/ Desktop Management

3.4.1 Access to the WDC network is provided to users through the creation of an Active Directory account. By default users are assigned the minimum levels of access required to perform their role. This includes the provision of domain membership, application of standard desktop configuration policies and access to the internet through the proxy (referred to in 3.3.2). This minimum level of access can be upgraded at the discretion of the user's line manager, who is able to request that the user's access be matched to an existing users permission levels.

3.4.2 User access requests are sent to the service desk in the form of an email from a senior, approved member of staff. This email incudes detail on the access levels that the user requires and acts as the authorisation needed to create or change users' access permissions. The information provided in the email is then used to raise a Supportworks case. There is, however, no user access request / change form in use to capture and record all user access changes, approvals and removals. During the audit we discussed the suitability of introducing such a form in order to standardise the processes around information provision for user access requests and provide an improved audit trail. ICT management advised that this might be considered in future. We consider this as a housekeeping point rather than a control weakness; as such, a formal recommendation has not been made and we have left ICT management to reflect on the benefits of introducing such a procedure.

3.4.3 Review of WDC Active Directory accounts identified the following accounts:

Account Name	**Enabled**
Admin	True
Administrator	True
Guest	False

The Admin and Administrator accounts are default members of the Domain Admins group in Active Directory. These accounts are the most powerful in the domain, granting the user the highest level of access privileges. The Administrator account cannot easily be removed or deleted, but can be renamed. As this account type is known to exist by default it is good practice that it is renamed in order to make malicious access attempts more difficult.

Similarly, the Guest account is a default AD account that is designed to enable users without an account to log on the domain as a guest. This has been disabled on the WDC AD domain as per good practice, but renaming the account would provide an additional level of protection against unauthorised access.

Risk

Slight increased risk of unauthorised access to WDC network and systems should the domain be enabled.

Recommendation

The Admin, Administrator and Guest accounts should all be renamed as a matter of good practice.

3.4.4 Review of Active Directory password parameters and logging settings also highlighted the following:

No audit policies were enabled. This may expose the Council to risk in the event of malicious user activity/ system misuse going undetected due to lack of an audit trail.

Minimum Password Age was set to 0, and Password History to 4 meaning a user could cycle through passwords repeatedly until they get to an old favourite, and therefore less secure, password.

These issues were reported in the recent ICT Risks audit and it is understood from discussion with management that both issues are in the process of being addressed and that changes to the settings should be implemented during the first quarter of 2015/16.

3.5 Backup and Disaster Recovery

3.5.1 HP Data Protector is used to create backups of all Council servers and data. Testing confirmed that daily backups are made each weekday and kept in the onsite tape library for two weeks. These backups are a combination of incremental and full backups depending on the server and/or the data.

3.5.2 Weekly backups are performed over the weekend and include all systems. The weekly tapes are taken by a member of the infrastructure team to be stored off-site at the Town Hall where they are kept for a four week period. Monthly full backups are also made and taken off-site on a monthly basis. These are retained for six months. A sample of daily, weekly and monthly backups was selected and reviewed to confirm that backups were up to date and had been completed successfully.

3.5.3 To minimise the impact of accidental data loss, storage of data on Council desktops is restricted by Group Policy. Staff are required to save all documents to their network drive, the local H-drive. These directories are included in the daily backup routine.

3.5.4 The infrastructure team completes a daily backup log in order to keep a record of backups, their status, which tapes are used and to maintain records relating to the housekeeping of the backup system. Review of a sample of logs from the past year confirmed these were being completed according to the process and that testing of backups was being performed. In the event of an unsuccessful backup, the infrastructure staff responsible take steps to record, investigate and resolve the failure, making manual backups of the data where required.

3.5.5 The third party 'Phoenix IT Continuity and Resilience Services Ltd' has been contracted to provide a fallback data centre to be utilised in the event of a DR situation. An annual business continuity test of this facility is undertaken in order to provide assurance on the ability to recover the Council's data and systems and ensure the data recovery procedures are aligned to recovery objectives.

3.5.6 The last test was performed in June 2014. Although this test was completed successfully, we were not able to obtain reports detailing and summarising the test results. It is good practice that an output from each test is documented and reported in a test report. This report should include detail on the testing performed, the time taken to recover systems and services, whether recovery objectives have been met and include detail on any issues and/or actions arising from the testing.

Risk

Lack of visibility of recovery timescales and assurance that potential issues are being identified and addressed.

Recommendation

Management should create a Disaster Recovery report template to be used during the next annual test. This should include the time taken to recover systems and services, whether recovery objectives have been met and include detail on any issues and/or actions arising from the testing.

4 CONCLUSIONS

4.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did identify some Low and Medium rated issues which, if addressed, would improve the overall control environment. As a result the findings are considered to give SUBSTANTIAL assurance that appropriate controls are in place around the management and operation of the ICT Infrastructure.

5 MANAGEMENT ACTION

5.1 Recommendations to address the issues raised are reproduced in the Action Plan together with the management response.

Richard Barr
Audit and Risk Manager