Deloitte.

Report 6c

Final Internal Audit Report

Network and Communications

April 2008

Contents

Executive Summary

Introduction

1. This audit forms part of the 2007/2008 Internal Audit Plan, which has been approved by the Mayor and Audit Panel. The plan entails an audit of the control framework established for the management and administration of the Authority's network infrastructure.

Summary

2. The overall control environment has obtained a substantial audit assurance. However, nine internal audit recommendations for further improvement in the environment were identified and agreed with management, which are detailed in the body of the report and highlighted below in the summary evaluation of the areas covered in the audit.

3. Device and firewall security – The firewall rules showed clear evidence of being proactively secured. However, two recommendations were raised over network logging and both domain server and firewall anti virus and patch management settings.

4. Benchmarks and monitoring – The network operating system security settings are periodically evaluated by the Sekchek security evaluation and benchmarking tool which, as appendix 3 shows, are currently in line with the security standards applied elsewhere in the public sector. However one recommendation was raised to make further use of appropriate key performance benchmarking tools and indicators.

5. Network operating system settings, - Three recommendations for further improvement were raised in this area regarding -

   - Account lockout settings;
   - Generic account names; and,
   - Account permissions that have been granted to highly sensitive privileges.

6. Remote access and trusted domains – Two recommendations for further improvement in this area were raised to secure windows remote access services accounts and to confirm the adequacy of security settings in all trusted domains.

Audit Opinion

Substantial Assurance

Evaluation Opinion: While there is a basically sound system there are weaknesses, which may put some of the system objectives at risk.

Testing Opinion: There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Observations and Recommendations

In order to assist management in using our reports:

We categorise our **opinions** according to our assessment of the controls in place and the level of compliance with these controls

Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
Substantial Assurance	While there is a basically sound system, there are areas of weakness 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.
Limited Assurance	Weaknesses 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.
No Assurance	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.

b) We categorise our **recommendations** according to their level of priority.

Priority 1	Major issues for the attention of senior management.
Priority 2	Other recommendations for local management action.
Priority 3	Minor matters.

Device and firewall security

1. Domain Server Security Configuration (Priority 2)

Recommendation	Rationale
The latest Windows Service Pack (Service Pack 2) Anti Virus software and security patches should be installed on the Network Domain Server and monitored to ensure they are maintained as current and up to date.	Applying the recommended Service Pack will help ensure that the integrity of the operating system is maintained and that the latest versions of the Operating System released by the software supplier are applied in a timely manner. Examination of the Network Domain controller identified that • No antivirus software is installed on the domain server; and • The latest Windows Service Pack and security patches are not installed. Failure to ensure that the network servers have the latest anti viris, service packs and security patches applied increases the risk that unauthorised activity may occure and that known Windows security vulnerabilities may be exploited.
Management Response – Head of Technology Group	
Agreed – This is part of our programme of patching and is planned. Implementation Date : July 2008	

2. Firewall Device Settings (Priority 2)

Recommendation	Rationale
Consideration should be given to ensuring that anti virus and security patch update frequency and are maintained as current and up to date and confirmed as such by periodic monitoring review or penetration tests.	Effective and tested Firewalll rules help to minimise the risk of unauthorised access. Review of the Firewall Rules noted that the rule base showed clear evidence of being proactively secured as protocols were disabled unless specifically permitted and the banner title does not assist enumeration probes. However two points of potential concern were identified regarding virus and security patch update frequency. Unless Anti Virus and Secuity Patches are maintained as up to date, and confirmed as such via periodic review or penetration tests there is an increased risk that unauthorised activity may occur.

Management Response – Head of Technology Group
Agreed – The Firewall devices are due to be replaced in this financial year, anti-virus and security patch update frequency are deliverables from this project. Implementation Date: May 2008

Benchmarking

3. Benchmark Monitoring (Priority 2)

Recommendation	Rationale
Consideration should be given to expanding the use of network benchmarking indicators such as • The Microsoft Security Baseline Analyser, to confirm patches are applied as expected, • The use of appropriate Key Performance Indicators (see . http://kpilibrary.com - you just need to complete the free registration to gain access) or • The Exchange best practice evaluation tool also provided by Microsoft.	Effective benchmarking helps ensure that network activities and achivements are appropriately monitored against expected norms. Windows security benchmarking takes place on a regular basis and Appendices 3 and 4 show current settings are inline with the the public sector. However other best practice microsoft benchmarking tools for exchange servers are not currently in use and no performance indicators of the network security patch management activities are currently monitored e.g. by use of the Microsoft Security Baseline Analyiser tool. Until wider use is made of benchmarking tools there is an increased risk that network management and configuration arrangements may slip below expected standards that may be impact on network availability by error or intent.

Management Response – Head of Technology Group
Agreed – As part of the patching programme, benchmarking network indicators will be implemented Implementation Date: July 2008

Network Operating System Settings

4. Account lockout policy settings (Priority 2)

Recommendation	Rationale
Consideration should be given to the use of the following account policy lockout settings: • The time the account is locked out (lockout duration) should be set to 0; • The value for reset lockout counter should be set to 1440 minutes (24 hrs).	Effective account policy lockout settings help to minimise the risk of unauthorised access. Examination of the current system account locout policies found that accounts are locked fot three days if seven failed password attempts are made in a 30 minute period. The current control settings therfore protect accounts that are targeted on an individual basis. Unless the lockout counter reset value is increased from 30 to 1440 minutes (24 hrs) there is a potential risk that access may be compromised by auomated hacking tools that would rotate the period between password guessing access attempts so that no ome that one or two password guessing attempts would be made in any 30 minute period so that the counter is reset to zero before the next password guessing attempt is made.

Management Response – Head of Technology Group
Agreed – Recommendation will be passed to the Security Board to be reviewed and agreed Implementation Date: May 2008

5. Generic and default account names (Priority 2)

Recommendation	Rationale
Consideration should be given to the ongoing use of generic account names, and ensuring that their use is adequately restricted. If a requirement for their use is essential, a process should be introduced where such use is authorised, logged and monitored.	Allocating accounts to specifically named individuals helps ensure accountablity for network activities. Examination of network account names and details identified that – • Default system account names have been disabled or renamed; and, • Potential generic accounts names exist. There is an increased risk of passwords being shared and accountability being compromised, via error or intent, by the continued use of generic accounts.
Management Response – Head of Technology Group	
Agreed – Work is planned to implement procedure and monitoring for all generic accounts Implementation Date: 30th June 2008	

6. Account Permissions (Priority 3)

Recommendation	Rationale
Consideration should be given to confirming that administration accounts are restricted to authorised users and that the following rights are granted to no one unless an essential busoiness requirement exists: • Act as Part of the Operating System; • Adjust Memory Quotas for Process; and • Log on As a Service. Processes should also be developed to facilitate the regular review and updating of these rights and privileges	Restricting powerful system rights helps minimise the impact of system disruptions and to ensure that recommended Windows security practices are appropriately configured and applied. Examination of user permissions identified that rights and privileges which should be granted to no one were assigned as follows: • 33 accounts have Administration privilege of which 20 are named officers within IT; • Act as part of the Operating System has been granted to some users; • Adjust memory quotas for process has been granted to the Administrators group; and • Log on as a service has been granted to administrators. Restricting the use of powerful systems rights reduces the risk of either accidental or deliberate misuse of these permissions.

Management Response – Head of Technology Group
Agreed – A programme of work exists for this Implementation Date: May 2008

Remote Access and Domain Trusts

7. Remote access (Priority 2)

Recommendation	Rationale
Consideration should be given to performing a regular review of the user accounts configured to use the Remote Access service. Those user accounts no longer requiring the service should be removed. Where dial up access controls are used for remote access users, it is further recommend that this access is enhanced with the introduction of additional (secondary) authentication or dial back.	Remote Access Services (RAS) security settings help ensure that remote access is restricted to authorised users. Secure remote access is mainly achieved by the use of neoterris on the intrenet. However, Windows RAS accounts also exist to provide reslilance to the neoterris solution and examination of the Windows RAS accounts identified that: • 56 Accounts have access via RAS; • 16 users are not called back by RAS; • 21 users can set their own RAS number and 5 of these are administrators. RAS increases the risk of unauthorised access as the system is visible to a much larger number of potential intruders via the public telephone network. The risk is even greater where secondary authentication methods such as dial back are not in use.
Management Response – Head of Technology Group	
Agreed – This has been implemented. Implementation Date: Feb 2008	

8. Domain Trusts (Priority 3)

Recommendation	Rationale
Management should ensure that security standards defined on the trusted network domain controller are equal to those applied within the trusting domain. (e.g. by use of the Microsoft Security Baseline Analyser).	A trust provides a means of allowing users from a trusted domain to access services in a trusting domain and the security of the trusting domain is therfore also reliant on the security standards applied by any trusted domain. Analysis of the Network Domain Controller identified trust relationships with two other domains. One is a trusting and a second is a trusted domain. Until the security standards applied in any trusted domain is confirmed as effective there is a potential risk that security may be compromised in the trusting domain by weakness in the trusted domain.

Management Response – Head of Technology Group
Agreed - As part of the shared services programme, baseline security analyser will be implemented and their findings will be reviewed in all trusted domains. Implementation Date: July 2008

Appendix 1 - Audit Framework

Audit Objectives

The audit was designed to evaluate the adequacy of the control environment that has been established and applied to the Network Security settings.

Audit Approach and Methodology

The audit approach was developed by an assessment of risks and management controls operating within each area of the scope.

The following procedures were adopted:

- identification of the role and objectives of each area;
- identification of risks within the systems, and controls in existence to allow the control objectives to be achieved; and
- evaluation and testing of controls within the systems.

From these procedures we have identified weaknesses in the systems of control, produced specific proposals to improve the control environment and have drawn an overall conclusion on the design and operation of the system.

Areas Covered

Audit work was undertaken to cover controls in the following areas:

- Device And Firewall Security
- Benchmarks And Monitoring
- Network Operating System Settings
- Remote Access and Domain Trusts

Appendix 2 - Staff Interviewed

We would like to thank all staff that provided assistance during the course of this audit, and in particular the:

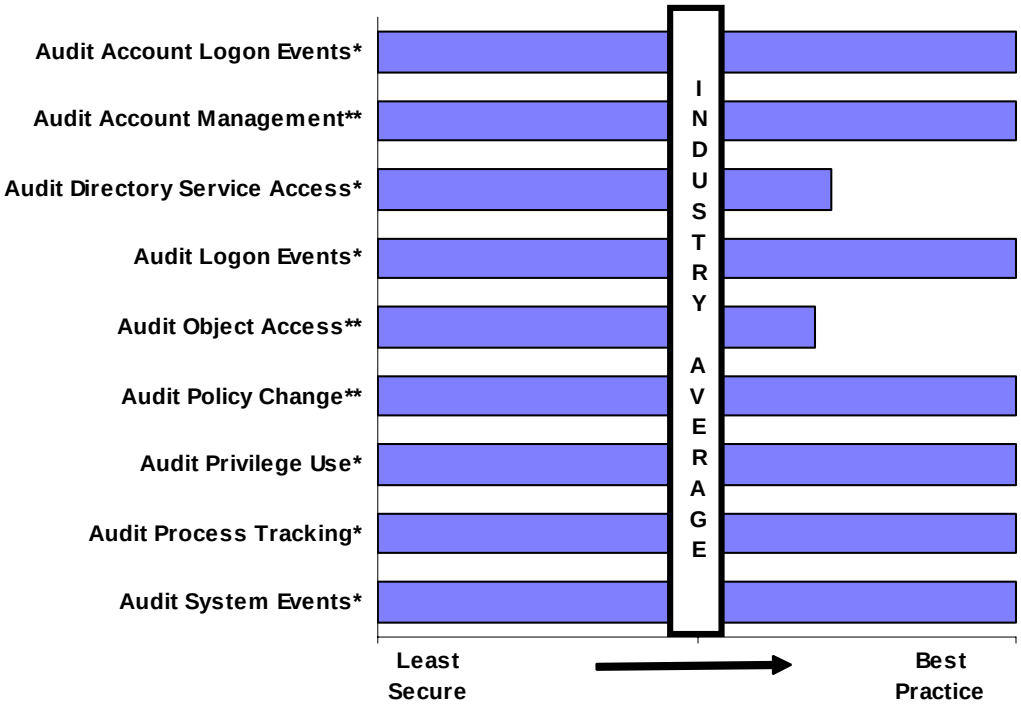
- Technology Group Operations Manager
- Technology Group Firewall Administrator
- Technology Group Windows Network Administrator

Appendix 3 –Benchmark Results

Rating Against Industry Average		
☺	😐	☹
	X	

December 2007 Summary of Domain Accounts Policy Values

Summary of the Domain Controller Audit Policy Settings December 2007



Statement of Responsibility

We take responsibility for this report, which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those, which came to our attention during the course of our internal audit 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 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.

Deloitte & Touche Public Sector Internal Audit Limited

St Albans

April 2008

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte & Touche LLP, which is the United Kingdom member firm of Deloitte Touche Tohmatsu. Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of it member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Deloitte & Touche Public Sector Internal Audit Limited is registered in England and Wales with registered number 4585162. Registered office: Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom.