Aberdeen City Council

IT Security (Network and perimeter)

Internal Audit Report 2014/2015 for Aberdeen City Council

August 2014

Internal Audit KPIs	Target Dates	Actual Dates	Red/Amber/Green	Commentary where applicable
Terms or reference agreed 4 weeks prior to fieldwork	16.06.2014	27.05.2014	**Green**	
Planned fieldwork start date	14.07.2014	14.07.2014	**Green**	
Fieldwork completion date	25.07.2014	05.08.2014	**Amber**	Fieldwork completion was delayed due to ACC staff holidays.
Draft report issued for Management comment	19.08.2014	18.08.2014	**Green**	
Management Comments received	02.09.2014	27.08.2014	**Green**	
Report finalised	09.09.2014	09.09.2014	**Green**	
Submitted to Audit and Risk Committee	24.09.2014	24.09.2014	**Green**	

Contents

Section	Page
1. Executive Summary	3
2. Background and scope	5
3. Detailed findings and recommendations	7
Appendix 1 – Agreed Terms of reference	11
Appendix 2 - Limitations and responsibilities	13

1. Executive Summary

Report classification	Total number of findings ← Section 3 →				
		Critical	**High**	**Medium**	**Low**	**Advisory**
Medium Risk	Control design	-	-	2	1	-
	Operating effectiveness	-	-	-	-	-
	Total	-	-	**2**	**1**	-
	Responsible Director: Director of Corporate Governance Project Sponsor: Head of Customer Service and Performance					

Summary of findings

1.01 ICT is responsible for the management of security for the Council's IT networks. The scope of our review was to assess the security and vulnerability management processes, and security management controls, in place over the network perimeter. In the course of our review we have identified areas of good practice as outlined in paragraph 1.02 below; however we have also highlighted two medium risk findings and one low risk finding concerning areas of weakness in the current processes and controls.

1.02 We have identified areas of good practice in ICT's management of network security. There is a dedicated team of security and technology analysts within ICT whose job descriptions detail their specific roles and responsibilities in respect of network security. A new Security Architect position has also been created and a person will be in post for the end of September 2014. This clearly indicates that ICT is conscious of its role in managing network security and has assigned resources to the task. In addition we also noted that the patching process is robust, with weekly patch updates for systems to ensure that the latest security fixes have been applied. There was also evidence of penetration testing and vulnerability scanning being performed (see paragraph 1.05 below), which enables ICT to identify areas of weakness in network security.

1.03 The current administration and monitoring process for the firewall is not aligned with good practice. We were made aware by management that the firewall can be accessed through a generic administrator account for which the password is known to several members of the ICT team. There are also no controls for monitoring the firewall for unauthorised changes to firewall rules. Although management has a process for review and approval of firewall changes, the combined

impact of these two findings undermine the effectiveness of that process, as they allow for administrator users to bypass the manual change controls. We also identified, in our sample testing of firewall rules, that the review and approval by management could not be evidenced. While we did not identify any concerns with the specific firewall rules tested, the lack of documented evidence of review raises the risk that there are firewall rules in place that may not be appropriate.

1.04 Our recommendation is that ICT management review the processes for firewall administration and change management. Access to the generic administrator account should be restricted to limit access to certain key ICT personnel in the event of an emergency. The firewall software should be configured to notify ICT management of changes to firewall rules to allow management to verify the authenticity of those changes against approved change requests. Finally ICT management should consider performing a review of all firewall rules to certify their appropriateness. Implementing these recommendations will help the Council minimise the risk of unauthorised changes being made to the firewall that expose the organisation to unauthorised access to its network and data.

1.05 ICT currently engage with a third party service provider to provide vulnerability scanning of key systems for the purposes of complying with Payment Card Industry Data Security Standards (PCI-DSS). These scans are performed on a quarterly basis and there is a robust process for responding to any findings from the reports issued and addressing vulnerabilities. However, for other Council systems, vulnerability scans are performed on an ad-hoc basis rather than on a regular schedule. It is recommended that ICT management extend the scope of the quarterly vulnerability scans to include other critical Council IT systems. Regular scanning of the Council's networks will help provide comfort against the risk of intruders exploiting unknown vulnerabilities.

1.06 There is currently limited management information collated by ICT management on the nature and extent of security incidents on the Council's network. Data from security incidents is available from several sources, for example users registering calls on the help desk, virus alerts from anti-virus software, or from vulnerability scanning. However, this data is not being collated and analysed to enable ICT management to identify specific areas of risk. ICT management plan to develop and use effective management information for security incidents when the new role of Security Architect commences.

Management comments

The audit review reflects areas of good practice which have been implemented to manage the Council's network perimeter. We agree with the findings and will continue to maintain and improve our management in this area to minimise electronic threats and disruption to Council Services.

2. Background and scope

Background

2.01 The overall scope of our review was to review the threat and vulnerability management processes, and security management controls, in place over the Council's network perimeter. Our specific focus was on the following sub-processes; policy and procedures, firewall rules, and resolution of penetration testing findings.

Policy and procedures

2.02 ICT has a team of three Security Analysts and nine Technology Analysts reporting to a senior analyst. Each has a job description with roles and responsibilities for managing security on the Council's networks. In addition a Security Architect has been appointed with responsibility for designing and developing technical security measures for ICT.

2.03 Security incidents are identified through several systems. Predominantly incidents are identified through users reporting issues to the help desk. These help desk calls are then analysed and, where they relate to security incidents, are then escalated to the Security or Technology Analysts for resolution. Virus incidents are more often identified through the anti-virus software and responded to by the Security Analysts. Other sources of information concerning security incidents are also obtained through quarterly vulnerability scans of systems relevant for the Payment Card Industry Data Security Standard. At present though there is no process for analysing the data on security incidents for management information purposes (see finding 3.03).

2.04 ICT uses a third party service provider, Sure Cloud, to provide quarterly vulnerability scanning to comply with the Payment Card Industry Data Security Standards). These scans are limited to focus on those systems relevant for PCI-DSS. The remainder of the Council's network is only scanned on an ad-hoc basis when changes have been made, for example a patch upgrade to a server (see finding 3.02).

2.05 Patches for network servers are scheduled on a weekly basis with each server allocated to one of ten patch groups. Each week the relevant patch group is assessed for any required patch upgrades and scheduled for patching as appropriate. ICT has a robust process for approving patch upgrades through the Change Advisory Board (CAB) in conjunction with the third party managed data centre provider, ATOS. Emergency patches, for example in the event of an urgent security fix for a server, are made as required with approval of the CAB.

2.06 The policy within ICT for administrator access to the firewall is that firewall administrators should access the firewall software, Checkpoint, using a named administrator account. However, there is a generic administrator account, for which the password is known among ICT management and firewall administrators, which can be used to access the firewall software (see finding 3.01).

Firewall rules

2.07 There are 247 firewall rules on the Council's network. Of these it was estimated by the firewall administrators that there are 100-150 active rules. Changes to firewall rules require a help desk ticket to be raised and for approval from ICT management before any change can be implemented. However, this approval by ICT management is often done verbally and there is no formal process for documenting this approval (see finding 3.01). There is currently no control for reviewing the firewall rules for appropriateness.

Resolution of penetration testing findings

2.08 Penetration tests are performed whenever ICT implement any significant network changes. The assessment of 'significance' is a qualitative judgement made by ICT. Tests are performed using the tools provided by the third party service provider Sure Cloud. Issues identified in penetration testing are recorded in the help desk and changes are implemented, as required, to address vulnerabilities and security threats identified.

Scope and limitations of scope

2.09 The detailed scope of this review is set out in Appendix 2 in the Terms of Reference. We have undertaken a review of the design and operating effectiveness of the Council's controls for IT Security (network and perimeter) in the areas contained within this Terms of Reference. Our work was undertaken using a sample based approach.

3. Detailed findings and recommendations

3.01 Firewall administration and change management – Control design deficiency

Findings

There is a four person firewall administrator team in ICT with responsibility for managing and monitoring the Council's firewall. Part of their role is to implement changes to firewall rules that have been requested through the help desk and approved by senior ICT management. In our review of the administration and monitoring controls of the firewall we identified the following findings:

- Discussions with ICT management identified that several ICT users have knowledge of the password for accessing a generic administrator account on the firewall. The policy currently is that firewall administrators should log in using their own personalised administrator accounts to ensure traceability of all activity on the firewall. It is good practice to restrict access to generic administrator accounts to ensure that such accounts are only used in emergency situations. This ensures that all administrator activity that occurs on the firewall, for example changes to firewall rules, can be audited and traced to a specific administrator account to ensure accountability. We did however inspect the audit logs from Checkpoint (the firewall software) that were available for the last three months and these logs indicated that the generic administrator account had not been used to access the firewall. This would indicate that, despite the risk, the firewall administrators have been accessing the log, for the last three months at least, using only their own named administrator accounts.
- We selected a sample of 45 firewall rules from a population of 247 and requested documentation to evidence management approval and review of those rules. In every instance there was no documentation to evidence approval for the rules currently in place. On enquiry with ICT management it was explained that there is no formal process for documenting the management review and approval for change. At present approval is often given verbally to the firewall administrator team who then implement the change. We discussed with the firewall administrator team the rationale for the rules we selected for sampling and did not identify any specific concerns with the rules as implemented, however, it is important that management have comfort that the rules are appropriate. Without evidence of management's review it is not possible for us to validate whether those rules are appropriate for the organisation.
- ICT management raised their concern that firewall rules might be changed without having been approved by the management. We found that there were no effective monitoring controls in place to mitigate this risk. Preventing unauthorised changes to IT systems is a risk for nearly all organisations and the most effective control to mitigate this risk is to have proactive auditing of system changes to alert management to unauthorised changes.

Risks		
A lack of control over the administration and monitoring of the firewall creates a risk that inappropriate changes could be made to the firewall that expose the Council to the risk of unauthorised access to Council networks and data.		
Action plan		
Finding rating	**Agreed action**	**Responsible person / title**
Medium	• The password for the generic administrator account will be changed and access to the account will be restricted to senior ICT management. The account will only be used on a 'break-glass' basis and ICT management will monitor the firewall to ensure that use of the generic administrator is restricted to only properly approved emergency situations. • ICT management will undertake a full review of the current firewall rules to ensure that they are all appropriate to the needs of the organisation. Once completed the firewall administrator team will be responsible for performing a quarterly review of the rules to ensure active rules are still required. • ICT management will ensure that formal evidence is retained for all approved changes to the firewall rules. • The Checkpoint firewall software will be configured to send an email alert to ICT management to notify of any changes in firewall rules, who will then verify these changes to ensure they were approved. ICT Management will ensure that changes are not self-approved.	Sandra Massey, ICT Manager **Target date:** 31 December 2014

3.02 Vulnerability scanning of Council systems – Control design deficiency

Finding

ICT use a third party service provider, Sure Cloud, to run quarterly vulnerability scans for compliance with the Payment Card Industry Data Security Standards (PCI DSS). However, these scans are currently only focused on those systems that are relevant for PCI, and do not cover other critical Council IT systems. At present the current policy is to perform ad-hoc scanning of systems only when changes are made, for example following a patch upgrade to the email servers.

Excluding non-PCI systems from regular vulnerability scanning could mean that vulnerabilities exist elsewhere within the Council's networks that are not detected. This could put at risk sensitive Council data, such as housing benefit information, school records or financial data, and expose the organisation to legal and regulatory implications under data protection. Extending the current quarterly scans to include these non-PCI critical systems on a scheduled basis would provide ICT with greater comfort about the security of those systems.

Risks

Vulnerabilities exist in non-PCI Council systems exposing the organisation to the threat of unauthorised access to networks and data.

Action plan

Finding rating	Agreed action	Responsible person / title
Medium	• All critical Council IT systems will be included in vulnerability scans on a quarterly basis. • Critical systems will be identified through a risk assessment that will consider those risks of most significance to the Council, for example legal and regulatory risks and financial risks.	Steve Robertson, Senior Analyst Sandra Massey, ICT Manager
		Target date:
		30 September 2014

3.03 Security incident analysis and effective management information – Control design deficiency

Finding

There are several sources of information through which ICT can identify security incidents; for example issues could be reported through the help desk by users, virus incidents are reported through the anti-virus software and other security issues can be identified through vulnerability scanning and penetration testing. ICT has limited management information from the vulnerability scanning performed by Sure Cloud, with the reports provided giving trend analysis of levels of vulnerabilities. However, in discussion with ICT management we found that there currently is no process for collating the available information to provide an overall picture for management information on security incidents at the Council.

Ensuring effective IT security involves taking a proactive approach to identify potential areas of threat and monitor ongoing security trends at the organisation. This approach requires effective management information for management, and IT security analysts, to make informed decisions about how best to utilise security resources in addressing security risks. It is generally good practice to ensure, as a minimum, that management have trend analysis information on security incidents and that all security incidents are recorded and categorised appropriately.

Risks

Persistent security threats are not identified resulting in the Council's systems being exposed to security breaches.

Action plan

Finding rating	Agreed action	Responsible person / title
Low	ICT management will develop and use management information for security incidents when the new role of Security Architect commences. As a minimum this management information will include a trend analysis of security incidents and categorisation of incident severity.	Sandra Massey, ICT Manager
		Target date:
		31 December 2014

Appendix 1 – Agreed Terms of reference

Background

The current IT network architecture within Aberdeen City Council ("ACC") is complex due to the wide variety of services and users that rely on Council systems. As a result of this, there is a higher level of inherent risk around network security, both in the current environment and in respect of network changes and requirements resulting from ongoing strategic programmes. For ACC, the loss of data may result in adverse media coverage, loss of stakeholder confidence, an impact on financial results and could ultimately impact the essential services provided by the Council.

The key component of data security within ACC is the 'perimeter security' of the network.

Scope

The overall scope of this review will be to review the threat and vulnerability management processes and security management controls in place over the network perimeter. The sub-processes and related control objectives included in this review are:

Sub-process	Objectives
Process and procedures	• Staff with security responsibilities are aware of the required process for proactively managing network security threats and vulnerabilities • Procedures and escalation plans are documented and are made available to key staff • Controls and procedures are sufficient to prevent unauthorised access being gained to systems and data resulting in the loss of data.
Firewall rules	• Firewall rules are documented and are effectively designed to prevent unauthorised traffic entering the internal network.
Resolution of penetration testing findings	• Penetration testing is performed on all changes to network hardware, to ensure perimeter security is maintained • Network security and data loss risks are addressed in a timely and appropriate manner.

Limitations of scope

The section above sets out the scope of the matters covered within this review. Our review will be conducted based on interviews and controls will be tested on a sample basis in line with PwC internal audit methodology.

It is Management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for Management's responsibilities for the design and operation of these systems.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the procedures and key controls in place to manage and monitor threats and vulnerabilities in relation to perimeter security
- Obtain and review the firewall rules that are in place against current recommended practice
- Review a sample of security penetration test reports, and obtain evidence that the threats and vulnerabilities identified have been addressed by management
- Evaluate the design of the controls in place to address the key risks
- Test the operating effectiveness of the key controls on a sample basis.

Key Council Contacts

Name	Title
Paul Fleming	Head of Customer Service and Performance
Sandra Massey	Operations Manager ICT
Steve Robertson	Senior Analyst

Appendix 2 - Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken a review of IT Security (network and perimeter), subject to the limitations outlined below.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls relating to IT Security (network and perimeter) is as at 5 August 2014. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.