Audit committee 5 December 2007

Internal audit report – Laptop controls review

Executive summary and recommendations

Introduction

As part of the internal audit programme for 2007/8 PKF undertook a review of the IT departments Laptop controls. This included encryption; evaluating password control / security; software licensing; back up and disaster recovery. The report offers the assurance level: Sound.

Decision

The Committee is asked to discuss the report.

Background information

At its meeting in March 2007, the Committee approved the Internal Audit Needs Assessment and Internal Audit Plan for 2007-8. (See paper AUD 22/07).

Resource implications

None

Financial implications

None

Appendices

Date of paper

15 November 2007

Laptop Controls Review

October 2007

Confidential

Assurance Level: Sound

Staff Interviewed: Director of Information Technology, Roy Dunn, Back Office Systems Administrator & Developer, Rick Welsby

Audit Team: Director, Jon Dee

Accountants &
business advisers

Contents

Project timescales

Date project commenced	22/10/07
Date field work completed	25/10/07
Date draft report issued	08/11/07
Date management comments received	13/11/07
Date final report issued	16/11/07

1 Introduction

1.1 In accordance with the 2007/2008 internal programme for the Health Professions Council ("HPC") that was agreed with the Audit Committee in March 2007, we have undertaken a review of the controls in operation over the organisation's laptops.

Scope of our work

1.2 As specified in our audit programme the aim of this project was to provide assurance to the HPC regarding its arrangements for laptop encryption, software licensing, anti-virus and anti-theft controls.

1.3 Specifically we reviewed:

- Passwords and general security controls, including asset tagging, anti virus software and software license monitoring;
- Insurances against hacking such as firewalls, and the results of any external security checks/ penetration testing; and
- Back up logs and disaster recovery

1.4 The work was carried out primarily by holding discussions with relevant staff and management, reviewing any available documentation and undertaking detailed testing on a sample basis, where required. The audit fieldwork was completed in October 2007.

1.5 This report has been prepared as part of the internal audit of the Health Professions Council under the terms of the contract for internal audit services. It has been prepared for the Health Professions Council and we neither accept nor assume any responsibility or duty of care to any third party in relation to it.

1.6 The conclusions and recommendations are based on the results of audit work carried out and are reported in good faith. However, our methodology is dependent upon explanations by managers and sample testing and management should satisfy itself of the validity of any recommendations before acting upon them.

2 Executive Summary

2.1 This report summarises the work undertaken by PKF within the agreed scope of our review of the controls in operation over the HPC's laptops. The work was performed as part of our agreed internal audit plan for 2007/08.

Background

2.2 The HPC employs around 100 staff. We understand that 45 of these have been issued with laptops. Laptops can be used as a standalone PC or to access the HPC network in the office or remotely using the HPC's Virtual Private Network ("VPN").

Risks

2.3 The principal risks associated with laptops have already been identified and are included in the HPC's strategic risk register, which has been reviewed and approved by Council. These are as follows:

- Software virus damage; and
- IT fraud/ theft.

Our assessment

2.4 Based on the audit work carried out we concluded that the HPC's controls over its issued laptops were **sound,** although these arrangements need to be kept under review to ensure that they keep pace with the evolution of viruses and other technological developments that may threaten the security of the organisation's data in the future.

2.5 Whatever protection an organisation puts into place, there will always remain a danger that an expert and determined hacker could access its data. However, in our view the HPC's arrangements are what we would expect for an organisation with the risk profile of the HPC and to heighten security still further would be likely to be a very expensive option.

Principal findings

2.6 All the HPC's laptops require a user name and password before they can be accessed. We understand that Safeguard Easy (a well known hard disk encryption tool) is installed on every laptop before they are issued to employees by the IT Department.

2.7 If confidential data is taken off site, this should only be undertaken using an encrypted disk. This means that even if a laptop or disk were to be lost or stolen, unauthorised users cannot access the device and read data or use the laptop to access the HPC network.

2.8 We note that the HPC has had 2 laptops stolen in the last 3 years- both were encrypted. We understand that this successfully provided the organisation with effective protection against data theft.

2.9 If these controls were successfully by-passed, additional password controls further restrict access to the HPC's network either in the office or through the HPC's VPN.

2.10 A software audit is undertaken periodically by Planet SAM Limited. This enables the HPC to identify any unlicensed software and any licences that are due to expire.

2.11 Management provided us with an audit report covering the period from October 2006 to October 2007 as part of this review. We noted that the report stated that the HPC was 100% compliant with its license commitments.

2.12 Star Technology Services Limited are the HPC's Internet Service Provider and provide the HPC with managed Juniper Netscreen firewall protection, a web content filtering service, the anti-virus service for inbound and outbound e-mail, and integrated VPN security for employees working offsite using laptops. Access to the HPC's network and on-line register is protected by these controls.

2.13 To ensure that the controls are working as expected, penetration testing is undertaken at least annually by external specialists. Our testing indicated that this check was operating effectively.

2.14 Finally, to ensure that the HPC can restore data in the event of damage to its network as a result of a disaster such as a virus attack, back up routines are undertaken on a regular basis. The HPC also has an established and clearly documented Disaster Recovery Plan which sets out those actions to be taken to restore the HPC's data and systems after any disaster.

2.15 We did not therefore raise any recommendations in relation to this area.

2.16 Finally, we wish to thank all members of staff for their availability, co-operation and assistance during the course of our review.

PKF (UK) LLP
October 2007

3 Detailed Findings

Background

3.1 The HPC currently employs around 100 staff. We understand that some 45 of these have been issued with laptops. The IT Department is responsible for ensuring that appropriate policies, procedures and controls are in operation to protect the data stored on the laptops and to prevent damage to the HPC network through their unauthorised use or contamination by a virus. Laptops can be used as a standalone PC or to access the HPC network in the office or remotely using the HPC's VPN.

Risks

3.2 The principal risks associated with laptops have already been identified and are included in the HPC's strategic risk register, which has been reviewed and approved by Council. These are as follows:

- IT fraud/ theft; and
- Software virus damage.

3.3 The principal management controls that are in place to mitigate these risks are as follows:

- Passwords and general security controls, including asset tagging, anti virus software and software license monitoring;
- Insurances against hacking such as firewalls, and the results of any external security checks/ penetration testing; and
- Back up logs and disaster recovery.

3.4 The findings of our review of these controls are set out below.

Findings

Passwords and general security controls

3.5 Following a year's trial of "etching" the organisation's details onto its assets the HPC concluded that this did not provide a permanent solution, since the details tended to erode over time. Management therefore decided to use bar coded self adhesive labels to tag the organisation's IT equipment, including laptops.

3.6 Our review indicated that the HPC has a laptop policy that sets out the responsibilities of staff that have been issued with laptops, HPC computers are not to be used by persons other than the designated employee due to the confidential nature of many of the HPC's activities.

3.7 Laptops are not permitted to be taken out of the HPC's offices without prior approval and employees are expected to make reasonable efforts to keep their computers safe from theft, without placing themselves in danger.

3.8 All the HPC's laptops require a user name and password before they can be accessed. We understand that Safeguard Easy (a well known hard disk encryption tool) is installed on every laptop before they are issued to employees by the IT Department. If confidential data is taken off site, this should only be undertaken using an encrypted disk. This means that even if a laptop or disk were to be lost or stolen, unauthorised users cannot access the device and read data or use the laptop to access the HPC network.

3.9 If a laptop were to fall into the wrong hands the data would remain securely protected even if the hard disk was removed. The hard disk is completely encrypted and access to the data can only be obtained of the user authentication procedure that runs before the system boots, is completed correctly.

3.10 As part of our review we witnessed the controls in action on a sample laptop. Our review work indicated that encryption and password controls over access to laptops were operating effectively. We also note that the HPC has had 2 laptops stolen in the last 3 years- both were encrypted. We understand that this successfully provided the organisation with effective protection against data theft.

3.11 If these controls were successfully by-passed, additional password controls further restrict access to the HPC's network either in the office or through the VPN. Network password controls are based upon Microsoft Strong passwords. These passwords are time stamped to force a change every 31days. A record of the last 5 passwords is maintained, which cannot be reused. Passwords are required to be alpha numeric with upper and lower case characters and are different from the passwords required to access the laptop.

3.12 The HPC's laptops are not provided with the necessary functionality to access the Internet remotely (i.e. it can only be accessed through the network) and employees are not permitted to install or download executable data from the Internet and may only access the Internet using HPC's software and firewall. Employees are not permitted to delete or modify existing systems, programmes, information or data installed on the HPC's systems.

3.13 A software audit is undertaken periodically by Planet SAM Limited. This enables the HPC to identify any unlicensed software and any licences that are due to expire.

3.14 Management provided us with an audit report covering the period from October 2006 to October 2007 as part of this review. We noted that the report stated that the HPC was 100% compliant with its license commitments.

3.15 The HPC's email policy alerts employees to the risk of virus damage to their own files, the service or organisational data and the dangers of opening attachments from unusual sources.

3.16 When employees access the network, Symantec anti-virus checking software is run automatically as part of the start up routines for entering the network.

3.17 Anti-spam software is also in place to check incoming email. This enables any viruses that may have been inadvertently introduced to the network or have been received by email attachment to be identified and acted upon. Our testing indicated that these controls were also operating effectively.

Insurances against hacking

3.18 Star Technology Services Limited are the HPC's Internet Service Provider and provide the HPC with managed Juniper Netscreen firewall protection, a web content filtering service, the anti-virus service for inbound and outbound e-mail, and integrated VPN security for employees working offsite using laptops. Access to the HPC's network and on-line register is protected by these controls.

3.19 To ensure that the controls are working as expected, penetration testing is undertaken at least annually by external specialists - NCC Services Limited. The testing includes:

- External vulnerability testing of the externally facing network infrastructure;
- Application security testing of external public web application; and
- Security testing of the VPN technology in use.

3.20 Our testing indicated that penetration testing was undertaken during March 2007 and that this check was operating effectively. The conclusions of the testing were that the HPC server network was generally considered to be in line with good security practice, although some weaknesses were noted. The findings of this exercise were then followed up in May/June. We are advised by the Director of Information Technology that that the principal matters raised by the March 2007 testing have now been resolved.

Back up logs and disaster recovery

3.21 Finally, to ensure that the HPC can restore data in the event of damage to its network as a result of a disaster such as a virus attack, back up routines are undertaken on a regular basis.

3.22 The IT Department backs up all key data overnight to server directories that are then backed up to corporate scale tape solutions. Month end tapes are stored off site in an underground bunker. Daily tapes sets are taken off site by IT Department staff.

3.23 Data from the LISA registrations system is specifically replicated overnight to servers off site in a secured server farm maintained by Star Technology Services Limited. Lotus Notes data, and therefore the systems therein are replicated every 15 minutes to the same server estate. Our review of the back up logs maintained by the IT Department indicated that back ups were being undertaken in accordance with the required routines.

3.24 The HPC also has an established and clearly documented Disaster Recovery Plan which sets out those actions to be taken to restore the HPC's data and systems after any disaster. Our review work in the past has indicated that the plan is regularly tested. For example, in our previous report in relation to this area (June 2007) we noted that testing was undertaken by the HPC in February 2007 to restore streamed LISA backup data to the organisation's Internet service provider.

4 Assurance Definitions

Assurance Level	Definition
Sound	Satisfactory design of internal control that addresses risk and meets best practice and is operating as intended.
Satisfactory	Satisfactory design of internal control that addresses the main risks but falls short of best practice and is operating as intended.
Satisfactory in Most Respects	Generally satisfactory design of internal control that addresses the main risks and is operating as intended but either has control weaknesses or is not operating fully in some significant respect.
Satisfactory Except For…..	Satisfactory design of internal control that addresses the main risks and is operating as intended in most respects but with a major failure in design or operation in the specified area.
Inadequate	Major flaws in design of internal control or significant non operation of controls that leaves significant exposure to risk.