Audit Committee 28 November 2012

Internal audit report – ICT Security

Executive summary and recommendations

Introduction

Mazars has undertaken a review of ICT Security controls, in accordance with the internal audit plan agreed by the Committee in March 2012. The report is attached as an appendix to this paper.

Decision

The Committee is asked to discuss the report.

Background information

At its meeting in March 2012, the Committee approved the Internal Audit Plan for 2012-13.

Resource implications

None.

Financial implications

£11,000 estimated costs for the completion of the three housekeeping recommendations.

Appendices

Internal audit report – ICT Security

Date of paper

08 November 2012

Internal Audit Report

ICT Security (03.12/13)

November 2012

FINAL REPORT

MAZARS

CONTENTS

AUDIT CONTROL SCHEDULE:

Client contacts:	Guy Gaskins: Director of IT Jason Roth: IT Infrastructure Manager	**Internal Audit Team:**	Peter Cudlip: Partner Graeme Clarke: Director James Sherrett: Manager Neil Belton: IT Audit Manager
Finish on Site \ Exit Meeting:	20 September 2012	**Management responses received:**	12 November 2012
Draft report issued:	5 October 2012	**Final report issued:**	12 November 2012

If you should wish to discuss any aspect of this report, please contact, Graeme Clarke, Director, graeme.clarke@mazars.co.uk or Peter Cudlip, Partner, peter.cudlip@mazars.co.uk.

1. INTRODUCTION

1.1 As part of the Internal Audit Plan for 2012/13, we have undertaken a review of the Health and Care Professions Council's (HCPC) ICT Security arrangements to prevent unauthorised and inappropriate use of IT. This area was included in the Plan due to the significance of risks associated with this area in HCPC's Risk Register.

1.2 We are grateful to the Director of IT and his team for their assistance during the course of the audit.

1.3 This report is for the use of the Audit Committee and senior management of HCPC. The report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Such matters have been discussed with the relevant staff.

2. BACKGROUND

2.1 HCPC's IT infrastructure is a Windows based network operating Active Directory under Windows Server 2008. Whilst operating under one domain the network is split into various Segments and Vlans to which the users will have access dependent on their role and access requirements. The environment has been substantially virtualised, through VMWARE, reducing its space footprint and designed with security as a high priority.

2.2 The main server room is based at Park House in a secure area of the main building with a managed backup to 'Rackspace' a hosted location outside of London which also provides a disaster recovery facility should it be required.

2.3 The Cisco ASA firewall configuration, alongside other tools in use, offers multiple layers of protection from external attack with active tools in place for port configuration, monitoring and reporting.

3. SCOPE AND OBJECTIVES OF THE AUDIT

3.1 Our audit considered the following risks relating to the area under review:

- Software Virus damage (*Risk 5.1, HCPC Risk Register, March 2012*);
- IT fraud or error (*Risk 5.3, HCPC Risk Register, March 2012*);
- Malicious damage from unauthorised access (*Risk 5.5, HCPC Risk Register, March 2012*);
- Electronic data is removed inappropriately by an employee (*Risk 17.1, HCPC Risk Register, March 2012*); and
- Loss of Registrant personal data by the registration system ('NetRegulate') application support provider in the performance of their support services (*Risk 17.6, HCPC Risk Register, March 2012*).

3.2 In reviewing the above risks, our audit considered the following areas:

- IT policies and procedures relevant to IT security;
- IT asset register;

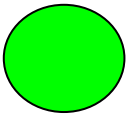
- User accounts, access rights, controls and account management;
- Security testing, surveillance and monitoring;
- Malicious software prevention, detection and correction;
- Network security;
- Exchange of sensitive data;
- Portable devices controls, i.e. USB drives;
- Data Management; and
- Disposal of data and IT equipment including certificates of destruction.

3.3 The objectives of our audit were to evaluate the adequacy and effectiveness of controls and processes for ICT security, and the extent to which controls have been applied, with a view to providing an opinion on the extent to which risks in these areas are managed. In giving this assessment, it should be noted that assurance cannot be absolute. The most an Internal Audit service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control.

3.4 An internal audit of Information Security and Data Protection was carried out in 2011/12 (report 01.11/12 refers). Consequently we have not duplicated that review and so the focus of this review was on risks related to IT infrastructure and IT security controls.

3.5 We are only able to provide an overall assessment on those aspects of the controls and processes for ICT Security that we have tested or reviewed. The responsibility for maintaining internal control rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy of the internal control arrangements implemented by management and perform testing on those controls to ensure that they are operating for the period under review. We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone are not a guarantee that fraud, where existing, will be discovered.

4. AUDIT FINDINGS: ONE PAGE SUMMARY

Assurance on effectiveness of internal controls	
	**Substantial Assurance**

Recommendations summary	
Priority	**No. of recommendations**
1 (Fundamental)	None
2 (Significant)	None
3 (Housekeeping)	3
Total	**3**

Risk management
HCPC has dedicated sections within its Risk Register for both Information and Data Security. Within this review we considered five of the risks identified in the Register and which are detailed in 3.1 above. Each risk has a number of mitigation actions, a number of which were tested as part of this review and considered to be operating effectively. HCPC has also taken a number of steps to enhance the effectiveness of its data security such as working towards ISO 27001, which focuses on information security, regular infrastructure penetration testing and undertaking a number of measures identified through the Poynter Review, which was commissioned after the HM Revenue & Customs data loss in 2007. HCPC has also invested heavily in IT infrastructure design, monitoring and reporting tools in order to address ICT Security risks.

Value for money
Value for money (VfM)considerations can arise in this area through the costs involved in designing, implementing and maintaining an secure ICT environment; however the reputational risks which could arise in the event of an incident occurring can be considerable. During our review, we did not identify any specific VfM issues that we need to bring to the attention of HCPC.

5. SUMMARY OF FINDINGS

Overall conclusion on effectiveness and application of internal controls

5.1 Taking account of the issues identified in paragraphs 5.2 to 5.4 below, in our opinion the control framework for ICT Security, as currently laid down and operated at the time of our review, provides **substantial** assurance that risks material to the achievement of HCPC's objectives in respect of this area are adequately managed and controlled.

Areas where controls are operating effectively

5.2 The following are examples of controls which we have considered are operating effectively at the time of our review:

- An Information Technology Policy is documented as part of the staff handbook. The policy covers a number of standard areas including acceptable use, the ownership of systems, security over passwords and the monitoring mechanisms in place. Users are required to sign-up to this policy on joining HCPC as part of the awareness of the wider handbook. However, there is a need to review and update the policy to reflect all current practices and technologies in use;
- All users of the IT systems are authorised prior to access being granted, and are identifiable and unique. A starters and leavers process is documented and is operated and recorded through the Lotus Notes system;
- At the network level, passwords are subject to change every 31 days as part of the default security policy. Password minimum length is 6 characters, and additional measures include password complexity rules, lockout after 5 login attempts and a short forced log out after a period of inactivity. These controls are comparative to best practice;
- Leavers are set to be disabled at the network level on the day of leaving. Further actions are taken over the course of the following week and month to tidy up access rights, such as to applications and email;
- HCPC makes use of the Symantec range of anti-spam and anti-virus software. It is installed on all supported servers, desktops and laptops with updates rolled out from central server managed by the infrastructure team. Symantec are recognised as one of the leading market players in this area;
- The number of remote users is limited but controlled through the use of two factor authentication. The user must exist on the active directory and must make use of a 'token' with a unique code issued through a Radius server either via a specific device or phone. These systems are recognised as industry standard two form factor authentication methods and considered secure; and
- HCPC is currently rolling out Endpoint security software from Sophos to all its machines after a completed pilot. At present approximately 65 out of 170 users have this applied which prevents the use of CD or USB devices unless expressly 'whitelisted' and known internally and are subject to encryption. Users receiving a 'whitelisted' device must also sign an agreement to the usage conditions and return the device when no longer required. All loses must be reported to the IT team immediately;
- All laptops are issued encrypted at a 'pre' BIOS level requiring separate authentication of the laptop, at the point of it being switched on, which can only

be circumnavigated using a complex 24 character passcode obtained through the IT Department; and

- The backups utilise the 'Net backup' encryption routines that encrypt the tapes. Tapes are only removed off-site monthly as data is mirrored off-site via a direct connection to 'Rackspace'.

Areas of good practice

5.3 Our testing highlighted the following particular areas of good practice:

√ Penetration testing which covers both infrastructure and application level testing is undertaken on a quarterly basis. Reports show that overall good security practices are implemented across the majority of the external network infrastructure;

√ The latest penetration testing report dated July 2012 highlights no high or medium level vulnerabilities in either the application or supporting infrastructure. Some low levels issues relating to application cookie configuration, web server configuration and the presence of metadata on the publically published documents were identified and these are being assessed and addressed internally;

√ HCPC are continuing to work towards ISO27001 information security certification, which will provide an overall management and control framework for managing HCPC's information security risks;

√ The level and depth of the monitoring tools, including Tripwire, the ASA Firewall and Web Applications Firewall (WAF), at the perimeter of the network is comprehensive providing a full range of reporting and monitoring of potential threats to the infrastructure; and

√ The IT infrastructure design was defined using specialist security consultants in order to minimise risk.

Areas for further improvement

5.4 We identified certain areas where there is scope for further improvement in the control environment. The matters arising have been discussed with management, to whom we have made a number of recommendations. The recommendations have been, or are being, addressed as detailed in the management action plan (Section 6 below).

6. ACTION PLAN

***Risk 2**:* IT fraud or error (*Risk 5.3, HCPC Risk Register, March 2012*)					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.1	*Observation:* An Information Technology Policy is documented as part of the staff handbook. The policy covers a number of standard including acceptable use, the ownership of systems, security over passwords and the monitoring mechanisms in place. Users are required to sign-up to this policy on joining the organisation as part of the awareness of the wider handbook. However there are some matters which require review and the policy is currently in the process of being updated. The Director of ICT has liaised with a number of similar organisations in the sector to obtain their IT Security policies to benchmark against. *Risk:* Policy in place does not reflect current practice, intention or controls.	As planned, HCPC should review and update the Information Technology Policy held within the Employee Handbook to ensure it provides more detail on the use of USB data drives and reflects current technologies and policy on the use of IT.	3	The IT policy is being reviewed as part of the 2012-13 IT Work Plan.	Director of IT

Risk 3: Malicious Damage from unauthorised access (*Risk 5.5, HCPC Risk Register, March 2012*)					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.2	*Observation:* Penetration testing of both Infrastructure and Applications is carried out by a third party contractor, NCC Group, on a quarterly basis but from an external only perspective. The recent reports indicate overall good security practices are implemented across the majority of the external network infrastructure and the latest report dated July 2012 highlights no high or medium level vulnerabilities in either the application or supporting infrastructure. However, as yet no penetration testing has been conducted from an internal perspective inside the business. Given the broadly clean bill of health from the externally facing infrastructure, testing of the internal infrastructure and risks internally would be the next logical step in ensuring the security of the network. *Risk:* Internal penetration risks exist which put the control environment at risk.	HCPC should consider undertaking penetration testing from an internal perspective to provide a full assessment of the environment and confirm all internal controls are operating as expected.	3	Penetration testing from an internal perspective will be considered as part of the 2013-14 IT Work Plan.	Director of IT

Risk 5: Loss of registrant personal data by the registration system ('NetRegulate') application provider in the performance of their support services (*Risk 17.6, HCPC Risk Register, March 2012*)					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.3	*Observation:* There has been no exchange of data between HCPC and the system supplier for 'NetRegulate', Digital Steps Limited (DSL) that can be remembered by IT Staff. Controls and expectations are outlined in the contracted arrangements between the two parties and these were re-enforced by letter in 2010. A secure facility, known as 'Jump and Dump' has also been established to provide secure access for the suppler and to prevent the supplier removing data without the express permission of HCPC. However, despite both of these controls there is no formal mechanism to confirm destruction of data should it be required. *Risk:* Confidential data exists outside the control of HCPC and at risk of unauthorised usage or access.	In the event that live data is exchanged in the future then HCPC should request written confirmation from DSL that the data has been destroyed once no longer required.	3	DSL currently only hold HCPC data that has been anonymised. In future where projects require data in its original form, i.e. not anonymised, then we will request written confirmation that data has been deleted following the closure of the project it was intended for.	Director of IT

Appendix 1 – Definitions of Assurance Levels and Recommendations

We use the following levels of assurance and recommendations in our audit reports:

Assurance Level	Adequacy of system design	Effectiveness of operating controls
Substantial Assurance:	While a basically sound system of control exists, there is some scope for improvement.	While controls are generally operating effectively, there is some scope for improvement.
Adequate Assurance:	While a generally sound system of control exists, there are weaknesses which put some of the system objectives at risk.	While controls are generally operating effectively, there are weaknesses which put some of the system objectives at risk.
Limited Assurance:	Control is generally weak leaving the system open to significant error or abuse.	Control is generally weak leaving the system open to significant error or abuse.

Recommendation Grading	Definition
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose HCPC to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose HCPC to a moderate degree of unnecessary risk.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.