hpc health professions council

Audit Committee 29 September 2011

Internal audit report – Information Security / Data Protection review

Executive summary and recommendations

Introduction

Mazars have undertaken a review of Information Security / Data Protection, in accordance with the internal audit plan agreed by the committee in March 2011. The report is attached as an appendix to this paper.

The report rated this area “Substantial Assurance” and made 9 housekeeping recommendations.

The new rating scale is detailed in Appendix 1, on page 14 of the report.

Decision

The Committee is asked to discuss the report.

Background information

At its meeting in March 2011, the Committee discussed the Internal Audit Plan for 2011-12.

Resource implications

None.

Financial implications

None.

Appendices

Internal Audit Report Information Security / Data Protection (01.11/12)
September 2011 Final report.

Date of paper

19 September 2011.

Internal Audit Report

Information Security / Data Protection (01.11/12)

September 2011

FINAL REPORT

CONTENTS

AUDIT CONTROL SCHEDULE:

Client contacts	Greg Ross-Sampson: Director of Operations Roy Dunn: Head of Business Process Improvement Marc Seale: Chief Executive and Registrar	**Internal Audit Team**	Peter Cudlip: Partner Graeme Clarke: Director Peter Williamson: Assistant Manager
Finish on Site \ Exit Meeting:	28 July 2011	**Management responses received:**	15 September 2011
Draft report issued:	22 August 2011/ 9 September 2011	**Final report issued:**	15 September 2011

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.

Status of our reports

This report is confidential and has been prepared for the sole use of the Health Professions Council.

This report must not be disclosed to any third party or reproduced in whole or in part without the prior written consent of Mazars LLP. To the fullest extent permitted by law, no responsibility or liability is accepted by Mazars LLP to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.

1. INTRODUCTION

1.1 As part of the Internal Audit Plan for 2011/12, we have undertaken a review of the Health Professions Council's (HPC) arrangements for ensuring information is securely including compliance with the principles of the Data Protection Act 1998. This area was included in the Plan due to number and significance of risks associated with this area in HPC's Risk Register.

1.2 Whilst this audit considered certain aspects of HPC's IT arrangements, such as backups, penetration testing and encryption of laptops and computers, these arrangements were not looked at in detail as a specific IT Security audit is currently planned for 2012/13.

1.3 We are grateful to the Director of Operations, Director of Fitness to Practice, Director of IT, the Head of Business Process Improvement and other staff across HPC for their assistance provided to us during the course of the audit.

1.4 This report is confidential and for the use of the Audit Committee and senior management of HPC. 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 HPC maintains a significant amount of personal and sensitive information on its registrants. This information is not only held as paper copies in respect of applications and Fitness to Practise cases but is also stored within HPCs NetRegulate system. Information is also regularly transferred to third party assessors and partners for review.

2.2 At the time of the review, HPC were in the early stages of working towards ISO 27001, which is a formal set of specifications against which HPC may seek certification of their Information Security Management System (ISMS). Once this has been achieved this will provide assurance to its management and Council members that its information security controls are robust and these will be subject to regular independent verification.

2.3 HPC is registered with the Information Commissioner, registration number Z6621691. This expires on 2 May 2012.

3. SCOPE AND OBJECTIVES OF THE AUDIT

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

- Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1);
- Paper record Data Security (Data Security – Risk No 17.2);
- Loss of electronic data held by third party suppliers in the delivery of their services (general risk) (Data Security – Risk No 17.3); and
- Loss of physical data despatched to and held by third party for the delivery of their services (Data Security – Risk No 17.4).

- Loss of Registrant personal data by the registration system (Net Regulate) application support provider in the performance of their support services.

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

- Information Security Strategy;
- Risk Register;
- Process Mapping of all information – including controls around security;
- Policies and Procedures – including Data Protection Policy;
- Identification of roles and responsibilities in respect of information management/security/ data protection;
- Data Protection agreements;
- IT systems used for the collection/ storage of data;
- Processes for the safe transition of paper based data to and from archiving and storage facilities;
- Protection of third party information – address/bank/credit card details;
- Security of electronic data - in respect of password protection/ encryption technology/ penetration testing of system;
- Physical and environmental security arrangements;
- Internal/ external assessments carried out on robustness of data security/ data protection arrangements;
- Back up arrangements for all electronic data; and
- Monitoring and reporting of information security issues to Management Team/ SMT / Committee/Council.

3.3 The objectives of our audit were to evaluate the adequacy of controls and processes for information security and data protection, 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 We are only able to provide an overall assessment on those aspects of the controls and processes for information security and data protection 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**
Fundamental	None
Significant	None
Housekeeping	9
Total	**9**

Risk management

HPC have a dedicated section within its Risk Register for Data Security. Within this section there are six risks identified (17.1, 17.2, 17.3, 17.4, 17.5 and 17.6). 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.

HPC has also taken a number of steps to further enhance the effectiveness of their data security such as working towards ISO 27001, which centres on information security, and undertaking a number of measures identified through the Poynter Review, which was commissioned after the HMRC data loss in 2007.

HPC are also looking at improving its controls around its PCI processes, after a number of issues were raised in a recent report. This will include entering into a contractual agreement with Semafone to handle the telephone credit card payments and moving the PDQ machine to a more secure part of the building.

Value for money

Whilst there are effective processes in place in respect of information security, management are aware that currently the paper based application process and the processes adopted with Service Point for the scanning and copying of applications is not the most efficient and economical way of processing; it is also increases the potential risk of data loss.

HPC are currently looking into the introduction of online applications which would serve to improve control over personal data as well as streamlining existing processes.

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 the areas under review, as currently laid down and operated at the time of our review, provides **substantial assurance** that risks material to the achievement of HPC's objectives in respect of Information Security and Data Protection 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:

- HPC has established a Information Security Policy Statement which has been approved by the Executive Team and has been communicated to all staff;
- Employment contracts provide explicit reference to data protection and a confidentiality agreement;
- Responsibilities for the overseeing of information security has been clearly been assigned to the Operations Directorate, with the Head of Business Process Improvement designated the Chief Information Security Officer and the Director of Operations the Chief Risk Officer;
- Training on information security has recently been provided to staff, with ongoing refresher training planned. HPC have also incorporated information security into the induction process;
- There is a set process in place within HPC for dealing with subject access requests, under the Data Protection Act 1998. This is coordinated through the Secretary to the Council;
- Service level agreements are in place with Service Point for the secure transfer of personal data for scanning and archiving and with Deepstore for the longer term storage of data. Departments reviewed had established logging in and out processes for monitoring the transfer of hard copy files;
- There is also a service level agreement with Iron Mountain for the removal and destroying of sensitive documentation waste. Whilst the process appears to be robust we have recommended a slight change to the agreement to more accurately reflect current practice;
- There are a number of physical security arrangements in place including, door access restrictions within each of the departments visited, alarm systems and lockable cabinets; and
- Laptops and desktops are encrypted and there are restrictions in place on the use of USB mass data drives. It was also observed that all passwords were required for initial log on to the server and all applications reviewed required an additional password.

Areas of good practice

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

√ Penetration testing which covers both infrastructure and application level testing is undertaken on a quarterly basis,

- √ HPC are currently working towards ISO27001 information security certification, which will provide an overall management and control framework for managing HPC's information security risks; and

- √ The Fitness to Practise Directorate has a detailed document retention policy in place which clearly sets out the timescales for retaining different documents held within the directorate.

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 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)

	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
6.1	*Observation:* Staff are asked to sign up to the Information Technology Policy under section 5h of the Employee Handbook. This policy details the responsibilities of the staff and the use of devices such as laptops and PDA's and use of email, telephone calls etc. Whilst it mentions that information held on USB drives is the property of HPC, it does not mention HPC's specific policy in respect of these tools. For example, the responsibilities of Staff using USB drives, that only encrypted drives can be used, what USBs should be used for and the security of these. We were informed that the Policy is currently being reviewed and should be in place from September 2011. *Risk:* Staff are not fully aware of their responsibilities in respect of the use of USB data drives.	As planned, HPC 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.	Housekeeping	A review of the IT Policy is scheduled for 2012-13 financial year. These updates will reflect changes in technology that are rolled out to the organisation over then next few months.	2012-13 Financial year Director of HR / Director of IT

Risk 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.2	*Observation:* A report was provided by the Head of Business Process Improvement which detailed a review of the Payment Card Industry (PCI) process. One of the weaknesses identified was where data was taken over the telephone, it was not secure enough to ensure personal data could not be copied. There were also concerns over the security of the PDQ machine for walk in applicants and the arrangements around the collecting of the Section 10 on the International Application Forms which contain credit card details. HPC is investing in Semafone in September 2011 which will provide an automatic third party process which will remove any staff needing to take responsibility for taking credit card details. The PDQ machine is also going to be moved into a more secure area, and Section 10 details will be held more securely in the interim, but it is intended that this transaction will be dealt with by Semafone also. *Risk:* Loss of bank and credit card details.	HPC should continue to address the issues identified in the recent PCI report.	Housekeeping	This project is in progress, and is currently awaiting action by utilities to transfer specific telephone numbers to new services.	End of year Director of Finance

Risk 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.3	*Observation:* Through discussion with the HR Manager, the Director of Operations and the Head of Business Process Improvement there tended to be a view that HPC did not have a formal leavers checklist in place which ensured that all issued items, such as Blackberry's , ID cards, etc were returned and all appropriate departments such as IT, Payroll , etc were informed in a timely manner. At the debrief, this was questioned by the Chief Executive and a copy of a checklist was provided which covered most key areas, though it was felt it would benefit from a more formal list of all potential items that should be returned to ensure that nothing could be missed off. *Risk:* Failure to ensure that Leavers do not take away items which contain personal information.	The HR team should review and update the Leaver's checklist to ensure that it covers off all key areas and items that need returning. Once reviewed this should be communicated to managers across the organisation so that they are fully aware of the checklist.	Housekeeping	The list will be reviewed and updated where required. The list will be circulated to all EMT, CDT and line managers.	November 2011 Director of HR / HR Manager

Risk 2: Paper record Data Security (Data Security – Risk No 17.2).					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.4	*Observation:* Locked document destruction bins were observed as being in place within each department visited. A bag is suspended in each of the bins and confidential documentation is placed in the locked bins and emptied on a weekly basis by Iron Mountain. The service level agreement with Iron Mountain specifies the responsibilities of both parties. It was noted however that this states that HPC staff are responsible for the tying up and sealing of the bags, but having spoken with staff this part of the process is performed by Iron Mountain. At the time of the audit we did not witness the Iron Mountain process in practice. *Risk:* Confusion over the responsibilities of both parties in the agreement, which could be problematic in the event of any data security issues arising.	HPC should revisit the service level agreement with Iron Mountain and ensure this is updated to reflect current roles and responsibilities in respect of tying and sealing of the bags.	Housekeeping	The current method of collection used by IronMountain utilises a large blue "wheelie bin" transported around the office buildings to each location, where the bins contents are emptied directly into the blue bin. Bag securing is no longer required. The Facilities Manager will attempt to have the SLA updated, although it is believed to be generic across all clients, and resistance may be incurred	December 2011 Facilities Manager

Risk 2: Paper record Data Security (Data Security – Risk No 17.2).

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.5	*Observation:* The Director for Fitness to Practise provided us with a document retention policy which is used within their team and clearly sets out the timescales for retaining different documents. HPC also has a Destruction (and Retention) Policy which was created in 2005, when the Freedom of Information Act came into force. Whilst it provides a high level list of documents held and retention dates it has been accepted by management that there is a need to develop a more comprehensive retention policy on a similar line to the Fitness to Practise document. *Risk:* Failure to comply with the Data Protection Act by keeping personal information beyond timescales which the Act deems appropriate.	As planned HPC should look to expanding and enhancing their current Destruction (and Retention) Policy to match the style of the document retention policy in place with Fitness to Practise Once completed this policy should be agreed with all departments and then communicated to all parties. In addition, consideration for encompassing the FTP document already in existence into this document.	Housekeeping	A high level organisation wide destruction / retention table has existed since 2005 A scheduled updating of policies will produce a document similar to the FTP Retention policy. Individual departments are aware of the retention requirements relating to their own areas	Next 6 months Director of Operations

Risk 2: Paper record Data Security (Data Security – Risk No 17.2).

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.6	*Observation:* Section 8a of the Employee handbook provides explicit detail on the Office Security Policy. Whilst it contains a summary of some of the key measures such as locking all room, not divulging access codes etc., it did not include ensuring that sensitive information is securely locked in cabinets when the office is unmanned. It was also noted that there is currently no 'clear desk policy' in place. *Risk:* Loss of personal data due to failure to ensure effective office security processes in place.	HPC should consider updating the Office Security Policy within the Employee Handbook to make explicit reference to ensuring that all filing cabinets are locked when the section is unmanned. When practical the organisation should look towards introducing a 'clear desk policy' to ensure that all sensitive and personal data is locked away at the end of each day. Once implemented this should be detailed in the Employee Handbook.	Housekeeping Housekeeping	Departmental guidelines require confidential material to be secured overnight, however we will look to update the employee handbook	By April 2012 Head of BPI & Facilities Mgr (Director of HR)

Risk 2: Paper record Data Security (Data Security – Risk No 17.2).					
	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.7	*Observation:* The Employee Handbook includes a section on crime and data protection. In review of this we noted that it did not explicitly explain the importance of data protection to staff, nor detail the responsibilities of the Council or staff in respect of use of and security over personal data . The Secretary to the Council later provided us with the Freedom of Information/Data Protection HPC Policy and Procedure which gave a brief guide on data protection and subject access requests. *Risk:* Misleading or inadequate information detailed within the Employee Handbook on data protection.	Consideration be given to including the Freedom of Information/Data Protection HPC Policy and Procedure document within the Employee Handbook to ensure that staff are fully aware of the responsibilities regarding data protection and the process for subject data access.	Housekeeping	The current handbook content will be reviewed and ensure it matches other more detailed guidance elsewhere	April 2012 Director of HR / Secretary to Council

Risk 4: Loss of physical data despatched to and held by third party for the delivery of their services (Data Security – Risk No 17.5).

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.8	*Observation:* Applications are entered on to the NetRegulate system on arrival. Once entered the hard copy applications are picked up by Service Point who will scan and copy the documents with one copy being sent back to HPC and an electronic copy being sent on disk. A copy of the paperwork will be sent on to assessors for evaluation. Through discussion with the Head of Registration he confirmed that the current process is not ideal and informed us that HPC are currently looking at a project to consider introducing online applications. Whilst there would still be a requirement for certain proof of identity documents to be sent through the post, this would significantly reduce the current process which in turn would reduce the risk to potential information security breach. *Risk:* Ineffective processes resulting in an increased risk of information security breach.	As planned, HPC should consider the introduction of online applications.	Housekeeping	Online Applications are already on a project list, and will be prioritised when a suitable window in the projects schedule allows. However, we are legally required to provide a paper application route.	Ongoing Director of Operations / EMT

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
Full Assurance:	There is a sound system of control designed to achieve the system objectives.	All controls operate effectively promoting the achievement of system objectives.
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.
No Assurance:	No controls are in place	Controls are ineffective or it is not possible to assess their effectiveness.

Recommendation Grading	Definition
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose HPC to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose HPC 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.