Health Professions Council
Audit Committee -27 March 2007

INTERNAL AUDIT REPORT – INFORMATION TECHNOLOGY SERVICE LEVEL AGREEMENT

Executive Summary and Recommendations

Introduction

As part of the internal audit programme for 2006/7 PKF undertook a review of Information Technology at HPC. The attached report which includes a management response was agreed with the Executive in February 2007.

Decision

The Committee is asked to discuss the report.

Background information

At its meeting on 28 June, the Committee approved the Internal Audit Needs Assessment and Internal Audit Plan for 2006-7. (See paper AUD 43/06).

Resource implications

None.

Financial implications

None.

Appendices

Information Technology Service Leval Agreement internal audit report.

Date of paper

14 March 2007.

PKF

Accountants &
business advisers

hpc health professions council

IT Service Level Agreement – VFM Assessment and IT Healthcheck

February 2007

Final – Confidential

Assurance Level:

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.

Staff Interviewed – Roy Dunn (Director of Information Technology), Craig Kjelvei (Support Analyst), Rick Welsby (Back Office Systems Administrator and Developer) and Tyrone Goulbourne (Network & Security Support)

Audit Team – Manju Mitra

Contents

1 Introduction

1.1 The purpose of the review was to provide an assessment of the Service Level Agreement that is in place with contractors for the support and maintenance of the IT systems at the Health Professions Council (HPC); and also to assess the effectiveness of HPC's back up and restoration procedures.

1.2 The review covered:

- An examination of the arrangements in place over IT support and for hardware and software maintenance.
- An assessment of appropriateness of the arrangements that are in place for managing contracts and the value for money implications of the proposed arrangements.
- An examination of the backup and disaster recovery procedures to ensure that business can continue in the event of a disaster with minimum disruption.

1.3 In addition a high level assessment was carried out of:

- Strategic approach to IT development and acquisition;
- IT security policy;
- Physical and logical access controls; and
- Network resilience.

1.4 Our work was carried out primarily through discussions with all key staff within IT and reviewing the underlying processes and available supporting documentation. Where possible we carried out limited testing in order to substantiate comments made. In addition we examined the following documents:

- Existing and proposed support contracts prepared by Digital Steps Limited;
- Proposal for maintenance and support of IP Telephony prepared by Universal;
- Disaster recovery (DR) plan;
- Proposed DR test plans covering a number of disaster scenarios;
- IT Strategy for the period covering 2006 and 2011.

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. The conclusions and recommendations are based on the results of the audit work carried out and are reported in good faith. However, our methodology relies 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 The purpose of the executive summary is to highlight the main findings and conclusions from our review. The detailed findings are included in the following section of the report.

Overall Conclusion

2.2 Based on the review carried out we have concluded that the adequacy of the controls over IT areas reviewed is as follows:

- IT Support Service – **Satisfactory**
- Contract Management – **Satisfactory except for LISA**
- Back up and Disaster Recovery - **Satisfactory**
- Other IT Key Controls - **Satisfactory**

2.3 The IT support for the main application software LISA is outsourced to Digital Steps Limited (DSL). The support for the current version of the Borland application on which LISA ceased in May 2006. Therefore, the HPC initiated the Borland upgrade project. HPC did not have the technical expertise in-house to determine whether the upgrade solution proposed by DSL offer good value for money and if it is the best fit for HPC requirements.

2.4 Therefore the HPC used consultants to help with technical evaluation of the DSL proposal. This process has now been completed. However, the LISA system was supported on a rolling month by month contract for a period of time. It is important that management ensure that they do not leave themselves exposed to a situation where an aspect of a key system is unsupported as this increases the risk of failure to a business critical system. A new support contract has now been signed.

2.5 The disaster recovery plan was successfully tested in February 2006 and it is planned to test the plan regularly by simulating various disaster scenarios. Back up is undertaken on a daily basis. The software for backing up the LISA system is a tool built within the SUN's operating system and for the other servers the backup software used is Backup Exec. A batch process is scheduled to automatically run the backup process overnight.

2.6 We confirmed by testing that there is a documented set of procedures for backup, storage of tapes and restoration activities and also for tape management. We further confirmed that these procedures are adhered to.

2.7 We have recommended that the following to enhance the control environment:

- The status field on the fault recording screen should be updated once the fault is fixed to reflect the current position**.** This will ensure that the helpdesk management system records accurate information and gives a true reflexion of IT department's performance; and
- It is important that the HPC ensure that they do not leave themselves exposed to a situation where an aspect of a key system is unsupported. An unsupported system increases the risk of a failure of a business critical system.

2.8 Finally, we wish to thank all members of staff at the HPC for their availability, co-operation and assistance during the course of conducting our review

PKF (UK) LLP

February 2007

3 Detailed Findings

IT Overview

3.1 The main business system is an application called LISA. This is a registration system and contains sensitive personal information about the medical practitioners. LISA is a three year old bespoke system and it was developed Digital Steps Limited. The LISA application runs on an Oracle database. This is a critical business system for the HPC.

3.2 There are currently three main IT contracts with three main IT service providers that are managed by the Director of Information Technology. The three main IT service providers are:

- Digital Steps Limited (DSL) for the LISA system;
- STAR for disaster recovery and web hosting; and
- Universal Office Automation for telecommunication facilities.

3.3 At present HPC is in the process of reviewing the IP Telephony Infrastructure support and the DSL support contracts, both of which are due for renewal shortly, in order to ensure that they are obtaining value for money for the services received.

3.4 DSL currently provides support services for the LISA application software and they will continue to provide this support as the system was developed by them and that they have exclusive rights to the software.

3.5 An IT strategy for the period 2006 – 2011 has been prepared by the Director of Information Technology. The IT team is small with many IT activities outsourced including development and maintenance of the main system LISA, firewall configuration and maintenance and web hosting.

IT Support and Maintenance Service

Our assessment

3.6 We have concluded that the controls over IT support and maintenance of IT systems are operating satisfactorily. However, there is a number of items that are over two months old, some of these have been fixed but not updated on the system.

Findings

3.7 The in-house IT department provides the first line support. Users log IT and telephony related faults using a Lotus Notes based in-house developed helpdesk management system. Once the fault is logged by completing an online form and it is submitted the system automatically sends an email alert to all members of IT. We have confirmed the operation of this system.

3.8 A nominated person in IT deals with the logged issues. We noted that a large number of faults are fixed by the first line support. When a problem is resolved the IT support person describes the resolution in the relevant section of the online form and notifies the user by phone. When the job is closed the system automatically sends an email to the user who has logged the problem and the item is archived.

3.9 By reviewing the fault log we confirmed that the logged items are suitably prioritised and action taken as appropriate within the expected time period.

IT Support - Digital Steps Limited (DSL) for the LISA system

3.10 DSL currently provides support services for the LISA application software. The HPC receives regular performance reports from DSL, making sure that regular contact is maintained with the DSL developers.

3.11 In addition, weekly meetings are held with the DSL Account Manager and the main developer working for HPC, the Director of Information Technology, the Back Office Administrator, the UK Registration Manager and a representative from Finance. In these meetings the list of issues passed to DSL is reviewed, outstanding items are discussed and the list is updated as necessary. On a monthly basis the Director of Information Technology and / or the Network & Security Support meets with the UK Registration Manager to discuss the status, progress of outstanding issues and any further user requirements with respect to LISA.

3.12 From an examination of a sample of open items that are over two months old, we noted that a number of these were fixed but had not been closed within the system. **(R1)**

3.13 There were also a number of LISA bugs and enhancements logged and these have been passed to DSL to fix. A further investigation of a sample of these indicated that the items are being progressed in accordance with the agreement reached with the users in the weekly status meetings and the delays are justified.

3.14 We understand that there has been a recent audit of the helpdesk system. It was the first time this exercise has been carried out.

3.15 The current DSL annual service cost is approximately £60,000 and this is paid in 12 equal instalments. There is a contract with STAR for web hosting and providing disaster recovery facilities and the annual cost for this is approximately £95,000.

IT Support - STAR for disaster recovery and web hosting

3.16 Once a quarter there is a formal meeting with STAR Account Manager and the Director of Information Technology and the Back Office Administrator. At present STAR does not send any performance reports to the HPC. However, we noted that it has been agreed that from September 2006 STAR will start to provide the HPC with reports that will include service breakdown which will enable more effective monitoring to take place. This will improve the performance management of the STAR contract.

3.17 All HPC servers are purchased with a three year warrantee; these are then extended or replaced as appropriate. The servers are maintained by respective suppliers. The large printers are mainly all HP and therefore these are maintained by HP. Network equipment such as routers and switches are maintained by Universal.

Contract Management

Our assessment

3.18 The terms of the old LISA SLA were not clear and this could have lead to a misunderstanding of the roles and responsibilities between the HPC IT team and DSL. We understand that the SLA between the HPC and DSL has now been reviewed and renegotiated. However, the LISA system was supported on a rolling month by month contract for a period of time. It is important that management ensure that they do not leave themselves exposed to a situation where an aspect of a key system is unsupported. This increases the risk of a failure of a business critical system. We have made a recommendation in this regard. **(R2)**

Findings

3.19 The main business system is an application called LISA. HPC had been investigating ways to manage the Borland application upgrade project for LISA and its ongoing support in a cost effective manner. We understand that this process has now been completed.

Service Level Agreement – Telephone System – Universal Office Automation

3.20 The telephone system is supported by Universal Office Automation under a service level agreement (SLA). This contract is also due for renewal in 2006/7, and therefore the management is currently reviewing and evaluating proposals from several suppliers including Universal to determine if savings may be made without compromising the quality of the service that is provided. We noted that the Council has received three proposals and the cost for the contract for all of the proposals is approximately were as follows: Actimax £7,450 plus VAT, Maintel £3,823 plus VAT, Universal £7,500 plus VAT. Maintel were the selected supplier.

3.21 We understand that an evaluation team has been considered for selecting a suitable telephony support supplier. The team comprises the Director of Information Technology, Back Office Administrator, Registrations Manager, UK Registration Manager and a representative from the Finance Department.

3.22 We further noted that the management is satisfied with the level of and the quality of services provided by Universal.

Service Level Agreement – LISA - DSL

3.23 We understand that DSL tested the latest version of BES (v6) and following this they commented verbally to the Director of Information Technology that BES v6 will not fit the HPC requirements; therefore they have recommended that the SUN version of the software is purchased. Initially the DSL proposal was to implement BES solution for £25,000, and then later they revised their proposal and suggested the SUN solution for £70,000, which will include purchasing the software and its implementation within the HPC. This cost will be absorbed in the Lisa support contract.

3.24 We noted that DSL did not provide a written explanation for rejecting the BES solution. The verbal rejection was followed by the submission of the second proposal in July 2006 offering SUN version and their ongoing support for the system.

3.25 From an examination of the proposal document called 'A managed service document for 2006 – 7' prepared by DSL in July 2006 we noted that it describes a new approach to the provision of support and maintenance services for LISA. The document lists the new benefits within the increased cost which includes first line support that is currently provided by HPC IT helpdesk and other maintenance services currently provided by the supplier / manufacturer of the respective systems, namely SUN, Oracle and Borland.

3.26 We further noted that the document specifies the service levels against the priority levels of the logged issues. DSL indicates the frequency and means of reporting the progress of support and also states that once a month all support requirements will be formally summarised.

3.27 The Director of Information Technology discussed the DSL's initial proposal document internally with the three IT staff members and the Director of Operations and rejected this based on the fact that a number of maintenance and support services they included are already covered and that HPC is not considering changing these arrangements at present.

3.28 The HPC intended to keep the first level support in house. Therefore HPC requested DSL to revisit the proposal and exclude from the proposal the services that they are currently receiving from other sources. The target date for the submission of the revised proposal was originally mid August 2006. However, they missed the deadline. This led to a delay in the process leaving the HPC further exposed. The existing contract was extended on a month by month basis as the negotiation continued.

3.29 HPC does not have the technical expertise in-house to determine whether the upgrade solution proposed by DSL offer good value for money and if it is the best fit for HPC requirements. Therefore HPC has utilised consultants from a company called NCC to help with technical evaluation of the DSL proposal. This consultation has now been carried out in full and assisted the HPC with the contract negotiation process. This has resulted in the LISA system being fully supported with enhanced levels of support in terms of the time available from DSL and n house IT support.

3.30 The support structure for LISA comprises of three lines of support. The HPC IT help desk function provides the first level support. The next level contains more specialist skills and the second line of support will be provided by DSL. DSL will then establish whether the problem can be resolved without any code changes. The third line of support is also at DSL which may result in an investigation for a software fix if the problem cannot be fixed at the second line of support.

Backup and Disaster Recovery procedures

Our assessment

3.31 The backup and disaster recovery procedures are appropriately controlled.

Findings

3.32 Back up is undertaken on a daily basis. The software for backing up the LISA system is a tool built within the SUN's operating system and for the other servers the backup software used is Backup Exec. A batch process is scheduled to automatically run the backup process overnight.

3.33 We confirmed by testing that there is a documented set of procedures for backup, storage of tapes and restoration activities and also for tape management. We further confirmed that these procedures are adhered to.

3.34 We also noted that data for the LISA system is transmitted to the Disaster Recovery site everyday; that means almost an identical image is held off site. At the time of our visit HPC was negotiating with STAR to make resources available so that HPC may transmit all data at the end of the day. Once this arrangement is in place a full data replication will be available at the disaster recovery site. This will not only enhance the backup activities it will also offer an improved contingency for the business continuity programme.

3.35 The physical and environmental controls for the computer room are appropriate to reduce the chances of need for recovery. The computer room has a smoke detector and dual, independent air conditioning units. If a fire is detected it automatically sets off the main building alarm and triggers an alert to the fire brigade. The building alarm is monitored by an external company and maintained by Secom.

3.36 There is a documented Disaster Recovery plan and a copy is with each member of the Executive Management Team (EMT) and departmental managers. All members of IT have access to an electronic copy. The Director of Information Technology, who is also the Disaster Recovery Coordinator, has a copy at home as well as at the HPC offices. The key Council members i.e. the Presidents and the Chair persons of the key committees also have a copy at home and at office. We noted that the plan includes the essential actions, staff notification procedures and the roles and responsibilities of the business continuity (BC) team in disaster situation.

3.37 In the event of a disaster outside the office hours the monitoring company calls the caretaker and in his absence his line manager. The monitoring company also has the contact details of the Director of Information Technology.

3.38 The DR site at STAR provides the backup network infrastructure and desktops and office accommodation for ten people. The key members of staff who are needed to be office based have been identified and they are familiar with their roles and responsibilities in the event of a disaster. If the DR programme is invoked then either the HR or the line managers are expected to inform the other members of staff. Most of these staff members are expected to work remotely using their laptops and the VPN connection.

3.39 We confirmed by examining relevant documentation that the DR plan was successfully tested in February 2006. This was achieved by switching off LISA at the main office and building the system at STAR. This exercise was carried out on a Friday to avoid business disruption and with the assistance of DSL to load the LISA system and relevant data from the backup tapes. The key users participated by inputting the day's transactions to confirm the effectiveness of the DR process. We understand that the next test is planned to be performed in November 2006 in full, covering Sage financial system and other less critical areas. After this test the exercise will be carried out annually.

3.40 We further confirmed by testing that lessons learnt were discussed following the last test. The future test plans contain various disaster scenarios. We were informed that it is planned to carry out dry runs in the future Executive Management Team meetings to test these scenarios. The members of the BC team are expected to participate in the full tests, this will help to keep their knowledge up to date and improve familiarity with their roles in a disaster situation.

Other IT Key Controls

Findings

3.41 The findings in relation to the other aspects included in the IT Healthcheck but not covered in the more detailed section of the report above are summarised below:

3.42 Strategic approach to IT development and acquisition – There is an IT Strategy in place covering the period 2006 – 2011. The IT team consists of four full time members of staff who are responsible for Network support and IT security, Back office system development and IT support.

3.43 There are a number of IT projects and these are managed in house by the IT Director or the Company Project Manager.

3.44 IT Security Policy - There is a detailed Information and IT security policy in place at the HPC drafted in October 2005. This is a comprehensive document including the following:

- Information policy;
- Computer use policy;
- Internet use and e-mail policy. There is also a email policy in place covering acceptable use;
- User management procedure;
- System administration procedures; and
- Incident response procedures.

3.45 Physical access controls over PC and network equipment – Physical access to HPC premises and the LAN, Servers and Back up devices are included within the Information and IT security policy. Servers are located in the server room which is locked and accessible only to IT staff.

3.46 There are physical controls in place to prevent access to the IT system through the door control at reception. There is also a 15 minute screen saving locking to prevent unauthorised access.

3.47 Logical access controls including remote access to the network – Logical access controls are in place at the HPC for access to the IT systems. New starters access rights are determined by their line manager – this access is applied for by the line manager to IT support.

3.48 There are also approximately 30 members of staff who have remote access via a Virtual Private Network (VPN). This is managed by a company called Star who are also the Internet Service Provider. There is a documented procedure in place for home and laptop working.

3.49 Network Resilience – Firewall software called Netscreens is used to protect the HPC network and is fully managed by Star. A quarterly PC audit is performed by Planet Sun examining the software held on PC's.

3.50 In addition penetration testing is carried out on the network to check the robustness of the firewall security on an annual basis. This is performed by NCC. There is also no wireless network internally at HPC.

3.51 We have no additional recommendations to raise from this work.

4 Action Plan

Ref.	Findings *Implications*	Recommendations	Priority	Management Response *Responsible Officer*	Due Date
R1	The fixed items in the outstanding faults log are not always closed promptly. *The helpdesk management system records inaccurate information and therefore it does not give a true reflexion of IT department's performance.*	The status field on the fault recording screen should be updated once the fault is fixed to reflect the current position**.**	**Low**	Tickets will be closed in a timely fashion unless being used as a means of tracking issues that may not be completely resolved. *Roy Dunn*	**Ongoing**

Ref.	Findings *Implications*	Recommendations	Priority	Management Response *Responsible Officer*	Due Date
R2	The SLA between the HPC and DSL has now been reviewed and renegotiated. However the LISA system was being supported on a monthly rolling contract for a period of time. *An unsupported system increases the risk of a failure of a business critical system.*	Management should ensure that they do not leave themselves exposed to a situation where an aspect of a key system is unsupported.	**High**	A new support contract has now been agreed. The contract was rolled on a month by month basis at the existing rate during the negotiation process. *Roy Dunn*	**April 2007**

5 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 and is operating as intended but falls short of best practice.*
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.*