Audit Committee – 9 December 2009

Internal audit report – Online Renewals IT Project Review

Executive summary and recommendations

Introduction

PKF has undertaken a second review of the online renewals IT project in line with the 2009-10 internal audit plan. The report is attached as an appendix to this paper.

Decision

The Committee is asked to discuss the report.

Background information

At the Audit Committee meeting in February 2008 the internal audit plan for 2008-09 was agreed. This included an audit of the on-line renewals project. This initial audit was conducted in February 2009, and the report was discussed and approved by the Audit Committee on 19 February 2009.

At the Audit Committee meeting in February 2009 the internal audit plan for 2009-10 was agreed. This included a second audit of the online-renewals project.

This audit was conducted in October and November 2009.

Resource implications

None.

Financial implications

None.

Appendices

Online renewals project review 2009/10

Date of paper

9 December 2009

Health Professions Council

Online renewals project review

2009/10

Final November 2009

Confidential

Accountants &
business advisers

Contents

Project timescales

Date project commenced	29/10/09
Date field work completed	25/11/09
Date draft report issued	26/11/09
Date management comments received	27/11/09
Date final report issued	27/11/09

1 Introduction and scope

1.1 In accordance with our 2009/10 internal audit programme that was agreed with management and the Audit Committee in February 2009, we have undertaken a second review of the Health Professions Council's ("HPC's") on-line renewals project as it progresses during 2009. Our work specifically focused upon the system testing and implementation phase of the project. The audit supports the annual statement on internal control required by HM Treasury and was carried out in accordance with Government Internal Audit Standards.

Scope of our work

1.2 As specified in our audit programme, the aim of this project was to provide assurance to the HPC that the planning and management controls over the on-line renewals project testing and implementation were adequate and operating as expected. We reviewed the management arrangements over the risks identified by the HPC in relation to this area, including IT risk management and project management and progress reporting arrangements.

1.3 Specifically we have not commented upon the viability of the proposed IT solution, which would be beyond the scope of our internal audit programme. As we have noted in the following sections of this report the HPC has taken specialist technical advice from other parties in respect of this matter.

1.4 The work was carried out primarily by holding discussions with relevant staff and management and reviewing the relevant documentation in relation to the specification of the system and project planning and reporting. The audit fieldwork was completed in October and November 2009.

1.5 This report has been prepared as part of the internal audit of the Health Professions Council under the terms of our engagement letter 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 over the HPC's on-line renewals project. The work was performed as part of our agreed internal audit plan for 2008/09.

Background

2.2 The HPC is seeking to improve the service it provides to its registrants when they renew by giving them the opportunity to make their declaration and payment via the Internet. The on-line renewals project was formed to develop this new service offering to the HPC's registrants. The design of the system was largely undertaken during 2008/09. The focus of the Project Team for 2009/10 was therefore primarily upon the system build, testing and implementation.

Our assessment

2.3 Based on the audit work carried out we have concluded that the HPC's controls over the implementation of the new on-line renewals system were sound and have been operating effectively to date, although there remains some further work and system testing to be undertaken before the system becomes operational.

2.4 We noted that many of the key risks associated with the project, notability in relation to usability scalability and security issues were addressed in detail through the design of the system, drawing upon specialist technical advisors to ensure that best practice in these areas was followed. Our review work has indicated that technical advisors have continued to be used to undertake the testing and implementation phase of the project. We understand that the support of these advisors will continue until the implementation is completed.

2.5 Nevertheless, whatever protection an organisation puts into place, there will always remain a danger that an expert and determined hacker could access its data or the credit/ debit card details of registrants. There is also the threat of phishing through which a fraudster could set up a duplicate of the HPC's portal and convince unsuspecting registrants to provide the fraudulent site with their personal details and the HPC needs to have agreed contingency plans with their internet service provider for dealing with the consequences of this.

2.6 However, in our view the HPC has taken the appropriate advice and built the security measures suggested by professional specialists into the design of the system accordingly.

2.7 We noted that the Project Team has adopted the HPC's highlight reports format for reporting as the project has progressed and that the project has been included in the HPC's major projects score card report which is presented to EMT every two weeks.

2.8 The Finance and Resources Committee has also received regular updates on the project during 2009/10, through the Operations report and Information Technology reports presented to each meeting.

2.9 In spite of these arrangements, we noted that the project has slipped by thirteen weeks in total and is now expected to be completed in mid-December. We understand that the various reasons for the delays were as follows:

- DSL delivered the user acceptance testing late by two weeks;
- User acceptance testing results being addressed and recalculation of production preparation time extended the project by six weeks;
- Installing the leased line caused two weeks of delays; and
- A further three weeks of delays in the load balancer/ leased line configuration.

2.10 However, the project management arrangements were operating effectively and enabled the delays to be highlighted and action to be taken by the HPC on a timely basis. This matter has now been resolved. There still remains some further testing to be undertaken and the implementation needs to be completed. We understand that the project management and reporting arrangements will continue to operate until the project is finalised.

2.11 Going forward as the system becomes operational it is planned that on-line renewal will be optional and registrants will still have the opportunity to follow the HPC's existing registration procedures. A communications and marketing programme is to be developed to raise awareness of the new on-line renewal service and to progressively encourage health professionals to renew their registration on-line reducing the pressure on the Registration Department at peak times for professional renewals in the future.

2.12 We have not therefore raised any recommendations in relation to this area. The detailed findings of our work are set out in the following sections of this report.

2.13 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
November 2009

3 Detailed findings

Background

3.1 The HPC is seeking to improve the service it provides to its registrants when they renew by giving them the opportunity to make their declaration and payment via the Internet. The on-line renewals project was formed in 2008/09 to develop this new service offering to the HPC's registrants.

3.2 The new system needs to enable registrants to access a hosted Internet web portal, to log in and be authenticated securely, to renew their application and to initiate payment of their registration fees by accessing a secure credit/debit card payment facility or downloading the necessary direct debit mandate forms.

3.3 As part of the planning for this project the HPC defined the following key objectives for the on-line renewals solution:

ON-LINE RENEWALS SOLUTION- KEY OBJECTIVES
• Usability - the system needs to be easy to use to ensure registrants continue to use this service channel;
• Security - since the HPC is a public body, storing 180,000 individuals' personal details, it is paramount that the system is safe and secure to use; and
• Scalability - the system needs the ability to increase the amount of current users to the system quickly and efficiently.

3.4 The high level aims specified for this project are to:

- Increase customer services;
- Reduce telephone calls from registrants about process;
- Provide a "24/7" service online / self service;
- Cope with future increase of registrants;
- Provide future additional services more easily;
- Reduce renewal calls and paper – resulting in potential cost savings;
- Communicate better with registrants – a more transparent process; and

- However, it must be a proportional solution to HPC's revenue.

3.5 The HPC was aiming for this system to be operational as quickly as possible to meet the demands of the next round of renewing registrants, with renewals beginning in June 2009, with the higher volume professions renewing by February 2010.

Key risks

3.6 The key risks included in the HPC's risk register in relation to the on-line renewals project are as follows:

- (5.1) Software virus damage;
- (8.6) on-line renewals project;
- (17.1) electronic record data security;
- (17.3) data held by third parties; and
- (17.4) data received from third parties.

Principal management controls

3.7 At the time of our last review of this project in 2008/09, we noted that the principal management controls through which the HPC was seeking to manage these risks were as follows.

3.8 Management had engaged the necessary technical advisors to support the implementation and to provide the expertise necessary to manage the risks of software virus/ IT fraud threats and reduce the risk of error.

3.9 We also noted that each stage of the process had been undertaken methodically and reviewed by management and appointed technical specialists when necessary. We concluded that these controls were sound at that stage of the project. Fuller details of the operation of these controls are set out in our report dated February 2009.

3.10 The project has continued into 2009/10 as planned and has been subject to similar controls. Now that the system design and development phase has been completed, the main elements of the project to be undertaken during this financial year involve:

- Completion of the system build;
- Integration of the system with the external credit card handler;
- Testing;
- Training; and

- Roll out.

3.11 The key project milestones scheduled for 2009/10 are as follows:

Project milestones	Planned timeline
Selection of load testing provider	March 2009
Integration of system with credit card handler	May 2009
Design of user acceptance test scripts	May 2009
Complete system build	June 2009
Installation of leased line between Kennington and online system	June 2009
User acceptance testing	June/ July 2009
Obtain analytics tool to analyse web site usage and user experience	September 2009
Load testing	August/ September 2009
Training and implementation and roll out	September - 1st November 2009

3.12 The principal management controls through which the HPC is seeking to manage its risks during this period of the project continue to be the:

- Engagement of experts in usability, scalability and security to support specification design, implementation and quality assurance testing; and
- Project progress monitoring following the HPC's project management methodology.

3.13 Our findings in relation to these controls are as follows:

Findings

Usability, scalability and security controls quality assurance

3.14 Digital Steps Limited ("DSL") was appointed as the HPC's registration system software developer and responsible for delivering the online renewals system to the specified requirements and architecture design.

3.15 NCC Group was engaged by the HPC to provide advice on system scalability and security.

3.16 DSL developed a software architecture document ("SAD") in partnership with NCC Group setting out the following information regarding the delivery of the on-line renewals project:

- An outline description of the software architecture required, including major software components and their interactions;
- Common understanding of the architectural principles used during design and implementation;
- Description of the hardware and software platforms on which the system is built and deployed; and
- Explicit justification of how the architecture meets the HPC's non-functional requirements.

3.17 A Software Network Architecture Document ("SNAD") was also prepared setting out a description of the network hardware architecture. Additional design documents were also written by NCC Group to validate the HPC's authentication model and the revised disaster recovery capabilities required.

3.18 At this stage NCC Group undertook a detailed analysis of the system network architecture and the software architecture options to assess the potential threats of software virus damage or IT fraud.

3.19 DSL then prepared three key documents setting out how they would implement the proposed solution as follows:

- Functional design specification. This describes the functional solution for the Online Renewals project based on the functional requirements described in the HPC document;
- Functional implementation. This describes how the system was to be functionally implemented; and
- Deployment document. This describes the tasks necessary to take the design functionality and deploy it into the production environment.

3.20 Etre was engaged to provide usability and accessibility advice and knowledge to ensure the system can be easily used by registrants. They developed the usability requirements (a set of requirements the system needs to meet to ensure it abides by industry standards and best practises), wire frame diagrams (low fidelity screen snaps shots of the system) and designed a working prototype of the online renewals system.

3.21 This work was based upon the functional and non-functional requirements previously developed by the project team with specialist consultancy support from NCC Group, particularly the usability and accessibility design considerations.

3.22 As was reported to the Finance & Resources Committee meeting in March 2009 the working prototype was tested with ten registrants under laboratory conditions, the results of the testing were then analysed and a list of improvements were produced, which resulted in modifications to the prototype.

3.23 DSL began to build the system to the design specification in January 2009. At March 2009 it was reported to the Finance & Resources Committee that following two iterations of the agreed build programme a demonstration of the system was provided to the Project Team.

3.24 By progressively reviewing the system as it is developed the HPC sought to ensure that the risk of misunderstandings in the implementation of the specification was minimised. We noted that the Project Team was satisfied with the demonstration of the system at the time of the second iteration. As the system build has progressed, we noted that a further demonstration was provided to the project team of iteration four of the system in April 2009.

3.25 User acceptance testing then began of the system to confirm that it operated in accordance with the specification and to identify any additional design enhancements necessary to meet the requirements of users. The testing team therefore included four members the Registrations Team.

3.26 We noted that the tests to be undertaken were detailed and designed to consider every aspect of renewing registration on-line. Over 1,300 test cases were to be evaluated and signed off by the users.

3.27 In accordance with best practice, we noted that the tests, the results and user sign off have been clearly documented on an Excel spreadsheet. Any areas where the results were not immediately satisfactory have been logged for action before the test can be signed off as cleared. We noted that the user acceptance testing had been completed to the HPC's satisfaction.

3.28 Due to the nature of the HPC environment and the on-line renewals process the new website will be handling credit card data. The solution proposed uses a 3rd party payment gateway, and the user will be redirected to their site to make the payment.

3.29 This means that no credit card data will touch the HPC environment. Furthermore, HPC has selected an ISP that is PCI DSS certified as a level 1 service provider.

3.30 Several options were considered by management through the preparations for the tender process but ultimately it was decided that the solution with the least risk would be to appoint a new ISP to host the new web portal.

3.31 Following a tendering process, Rackspace Limited was selected as the internet hosting provider for the online renewals system and to build the hosting environment. A leased line was to be installed to link the online system to Kennington enabling the service to be operational. Upon delivery we noted that the connectivity of the leased line was tested by the provider. Some issues arose from this testing, which required some amendments to the configuration of the infrastructure. We understand that these issues have now been addressed.

3.32 Load testing is being undertaken to confirm that the system including the hosting environment will be able to cope with the expected levels of demand from the various groups of health professionals. Rackspace Professional Services were commissioned following a tender exercise where four suppliers were invited to submit proposals to undertake this specialised work on behalf of the HPC. The methodology followed is to build up the number of users incrementally to first establish the failure load of the system. Changes will then be made to the system by DSL or Rackspace Limited to address any potential bottlenecks that may have caused the system to crash.

3.33 The load will continue to be increased and the system enhanced until the system is sufficiently resilient to cope with the likely volumes of registrants that will be using the system. Rackspace Professional Services have been used to run the load testing phase. Advice from NCC Group has been sought to determine the appropriate load levels to be tested. At the time of our review the load testing was still being completed, although no insurmountable issues appear to have arisen to date.

3.34 We noted that the HPC conducts regular penetration testing as part of their operational risk security control measures. Before the system goes live, we are advised that it will be penetration tested by a third party

3.35 Throughout the project the HPC has engaged technical specialists to support the design, testing and implementation of the new system. Based on our review of the project to date the input of these specialists and the results of their work has been clearly documented, considered by the HPC and any issues resolved before the next stage of the project is undertaken.

3.36 We have therefore concluded that the controls over usability, scalability and security have continued to operate effectively over the project to date.

Project progress monitoring and quality assurance

3.37 In accordance with best practice, a Project Sponsor (Chief Executive & Registrar) was identified, together with a Project Manager (HPC Project Manager) and a Project Lead (Director of Operations).

3.38 The Project Team includes these individuals and other key managers from the departments within HPC who would be affected by the outcomes of the project, including for example Registration, Communications and IT together with technical advisors as they are appointed by the HPC throughout the duration of the project to date.

3.39 The overall approach to the project was set out in a Project Brief. Our review work indicated that this document included the business case for the project, together with its objectives and scope. Further analysis and planning was undertaken and a detailed project plan was developed during 2008, including costs and benefits and a detailed timeline. This has been progressively refined as decisions have been made regarding the design and the likely costs of the project have become more certain.

3.40 During the course of implementation phase of the project, the HPC Project Team has met with DSL at least on a monthly basis (generally weekly) and a progress report has been prepared by DSL setting out the various tasks that they have been required to undertake and their status, together with any agreed further actions.

3.41 We noted that the Project Team has adopted the HPC's highlight reports format for reporting as the project has progressed and that the project has been included in the HPC's major projects score card report which is presented to EMT every two weeks. A risk and issues log has been maintained throughout the project and has been actively used to highlight issues and to agree remedial actions. The Finance and Resources Committee has also received regular updates on the project during 2009/10, through the Operations report and Information Technology reports presented to each meeting.

3.42 In spite of these arrangements, we noted that the project has slipped by thirteen weeks in total and is now expected to be completed in mid-December. We understand that the various reasons for the delays were as follows:

- DSL delivered the user acceptance testing late by two weeks;
- User acceptance testing results being addressed and recalculation of production preparation time extended the project by six weeks;
- Installing the leased line caused two weeks of delays; and
- A further three weeks of delays in the load balancer/ leased line configuration.

3.43 However, the project management arrangements were operating effectively and enabled the delays with the leased line to be highlighted and action to be taken on a timely basis. This matter has now been resolved. There still remains some further testing to be undertaken and the implementation needs to be completed. We understand that the project management and reporting arrangements will continue to operate until the project is finalised.

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.