## Finance and Resources Committee 16 March 2009

## Online Renewals & applications update

## Executive summary and recommendations

### Introduction

Since April 2008, the Online Applications & Renewals project has been led by Greg Ross-Sampson (Director of Operations and Project Lead) managed by Claire Reed (HPC Project Manager), with Marc Seale (Chief Executive & Registrar) as the project sponsor.

The purpose of the attached paper is to inform the committee on the progress of the Online Applications & Renewals project.

### Decision

The Committee is asked to agree the attached paper.

### Background information

See attached paper.

### Resource implications

See attached paper.

### Financial implications

See attached paper.

### Appendices

See attached paper.

### Date of paper

16 March 2009

# Online applications & renewal project update 5 March 2009

Greg Ross-Sampson

## Index

## Introduction

The Online Applications & Renewals project has been led by Greg Ross-Sampson (Director of Operations and Project Lead) managed by Claire Reed (HPC Project Manager), with Marc Seale (Chief Executive & Registrar) as the project sponsor.

The **objectives** of the on-line systems service is to:-

- Be Useable – the system needs to be easy to use to ensure registrants continue to use this service channel;
- Be Secure - being a public body and storing 180,000 individuals' personal details, it is paramount that the system is safe and secure to use;
- Be Scalable – the system needs the ability to increase the amount of current users to the system quickly and efficiently

The **high level aims** of the project are to:-

- Increase customer services
- Reduce calls about process. E.g. non-value added calls
- Provide a "24/7" service online / self service
- Cope with future increase of registrants
- Provide future additional services more easily
- Reduce renewal calls & paper – cost saving
- Communicate better with registrants – transparent process
- However, it must be a proportional solution to HPC's revenue

## Comments from PKF internal audit

In accordance with Audit Committee's 2008/09 internal audit programme, PKF undertook a review of the planning and management controls over the on-line renewals 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. The audit report is in appendix B.

PKF concluded that the controls over the implementation of the new online renewals system were **sound** and **have been operating effectively** to date. They concluded that management have 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. They also concluded that at each stage of the process had been undertaken methodically, reviewed by management and the appointed technical specialists when necessary.

They do also comment that there remains a considerable amount of work to be undertaken before the project is completed and management recognise the need to continue to exercise a high level of scrutiny as the implementation progresses.

In PKF's view the HPC's arrangements are what they would expect for an organisation with the risk profile of the HPC and have been designed to meet payment card protection standards. To heighten security still further would be likely to be an even more expensive option.

PKF's review of the various project reporting documents indicated that the project spend forecasts have been progressively refined as management have become more certain of the costs.

## Engagement of specialist suppliers

The project team has engaged the services of different third party suppliers to provide technical and expert advice and skills to deliver this service offering.

Etre were engaged to provide usability and accessibility advice and knowledge to ensure the system can be easily used by registrants

NCC Group was engaged to provide security and scalability advice and knowledge to ensure the system will cope with the projected volumes in a secure manner.

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

## Progress to date

## Scalability and security

Scalability is the term used to describe how well a solution will work when the demand increases. HPC want to ensure that the online renewal system performs adequately when a large number of registrants access it concurrently and that we can more easily "scale up" to meet excessive demand.

Security is the term used to describe protection against unauthorised access to, or alteration of, information and system resources such as CPUs, storage devices and programs. Security includes:-

- Confidentiality - preventing unauthorised access; integrity - preventing or detecting unauthorised modification of information.
- Authentication - determining whether a user is who they claim to be.
- Access control - ensuring that users can access the resources, and only the resources, that they are authorised to.
- Nonrepudiation - proof that a message came from a certain source.
- Availability - ensuring that a system is operational and accessible to authorised users despite hardware or software failures or attack.
- Privacy - allowing people to know and control how information is collected about them and how it is used.

In order to define the measures that need to be met to achieve scalability and security, two documents were created, the functional requirements (what it does) and the non-functional requirements (how it does it).

The non-functional requirements broadly explain:-

- performance metrics
- channel of delivery
- service delivery
- usability
- security
- technical requirements

NCC Group worked with HPC to define our non-functional requirements.  These have been approved and signed off.

The functional requirements broadly explain and define:-

- the actions of the process, creating or modifying data
- reporting requirements
- how data or information is held but not the delivery channel

NCC Group, DSL and Etre contributed to the validation of HPC's functional requirements. These have been approved and signed off.

The design definition of the system is split into two sections, the Software Architecture Document (SAD) and the Software Network Architecture Documents (SNAD).

Software Architecture Document (SAD) outlines a description of the software architecture, including major software components and their interactions, a common understanding of the architectural principles used during design and implementation, a description of the hardware and software platforms on which the system is built and deployed, explicit justification of how the architecture meets the non-functional requirements.

This document was developed by DSL, in partnership with NCC Group.  This has been approved and signed off.

Software Network Architecture Document (SNAD) is a description of the network hardware architecture.

These documents were developed by NCC Group, in partnership with DSL. These documents have been approved and signed off.

Additional design documents were also written by NCC Group to validate our authentication model, and to validate the revised disaster recovery capabilities.

Three design specification documents have been completed by DSL to deliver to these requirements.  They are the Functional design specification (FDS), the Functional Implementation and the Deployment document.

The Functional design specification (FDS) describes the functional solution for the Online Renewals system based on the functional requirements.  The Functional implementation describes how the system will be functionally implemented and the deployment document describes the tasks necessary to take the design functionality and deploy it into the production environment.

## Alternative Oracle solution

As mentioned in the update in November 2008, the system network architecture design (SNAD) was reliant on the validation of a solution that would keep our existing externally hosted services with the current service provider and host the new online renewal service at a new hosting provider.  Specific design consultancy was sort from Oracle [1] Consulting to detail the options available to HPC to ensure a reliable and performant database architecture.  This was an important element to the success of the design.

A formal analysis report was received from Oracle and all parties were satisfied that there were a number of relevant achievable options for HPC to create an appropriate solution. The conclusion from our security and scalability experts, NCC Group and the project team was that the multiplaced platform solution proposed would deliver our requirements.

Following on from this advice, our software developers investigated this solution and found that the proposed tool that Oracle suggested would carry out the required function was not available on the software platform that runs the existing Oracle database.

Subsequently, Oracle provided a revised documented solution with written assurance that this alternative solution would be suitable.  The overall conclusion from NCC Group and the project team was that this solution, although different, would be meet HPC's requirements.

## Usability

Usability is a term used to describe the effectiveness, efficiency, and satisfaction with which users can achieve tasks in a particular environment of a product. High usability means a system is easy to learn and remember, efficient, visually pleasing and fun to use and quick to recover from errors.

Using the functional and non-functional requirements, particularly the usability and accessibility design considerations, HPC's usability and accessibility experts, Etre, have developed a prototype environment in which the proposed solution was tested by registrants i.e. “real life” users. Usability results and recommendations ascertained from the laboratory testing of the working prototype, wiring diagrams  (the diagrammatical “look and feel” explanation of what the graphic user interface (GUI) will look like) , process flows explaining how each web page will function from the perspective of the user and the HTML ( Hypertext Mark Up Language) web pages of the system.

[1] Oracle is a powerful relational database management system that offers a large feature set. Oracle is widely regarded as one of the two most popular full-featured database systems on the market today and is the database that HPC's core application Net Regulate utilises.

These project work packages have incorporated the usability requirements defined in the non-functional and functional requirements pertinent to them. They have also taken into consideration the improvements ascertained from the laboratory testing of the working prototype.[2]

## Hosting services

A tender process has been held for the provision of internet hosting services for the online renewals system.

A new internet hosting provider was needed because the incumbent could not support an architecture design to the level of security and scalability the project team had specified.

A Request For Proposal (RFP) was sent to eight suppliers and following a thorough tender review process, Rackspace Ltd was selected as the internet hosting provider for the online renewals system.

Rackspace is currently building the hosting environment and is planned to be implemented by March 2009.

## Software build development

DSL have commenced the build of the system. At time of writing, 2 of the anticipated 6 iterations of their build programme have been completed. A demonstration of the system following iteration 2 was given to the project team for review.

This approach of reviewing work completed at particular build iterations ensures that the system is being developed as specified and mitigates the possibility of any misinterpretations or misunderstandings of the design specification.

The project team was satisfied with the demonstration of the system.

[2] The working prototype was tested with 10 registrants under laboratory conditions, the results of the testing was analysed and a list of improvements was produced.

## Current project forecast

Following on from the completion of the design phase, the project has revised the project spend forecast.

| | | November 2008 | | | February 2009 | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2008/09 | 2009/10 | Total | 2008/09 | 2009/10 | Total | Differential |
| CAPTIAL EXPENDITURE | Usability and accessibility analysis, design, test and web page development | £ 77,970 | £ - | £ 77,970 | £ 65,917 | £ - | £ 65,917 | -£ 12,053 |
| | Architecture analysis and design, ISP analysis, tender expertise | £ 66,499 | £ - | £ 66,499 | £ 60,428 | £ 1,234 | £ 61,661 | -£ 4,838 |
| | Requirements capture, FDS, design documentation, build & deployment | £ 87,688 | £ 56,289 | £ 143,977 | £ 197,931 | £ 144,213 | £ 342,144 | £ 198,167 |
| | Load & penetration testing , software system development | £ - | £ - | £ - | £ - | £ 155,035 | £ 155,035 | £ 155,035 |
| | New ISP | £ 76,258 | £ - | £ 76,258 | £ 18,657 | £ - | £ 18,657 | -£ 57,601 |

| | | |
|---|---|---|
| TOTAL CAPITAL EXPENDITURE | £ 342,932 | £ 300,481 |
| CAPITAL BUDGET | £ 300,000 | - |

| | | November 2008 | | | February 2009 | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2008/09 | 2009/10 | Total | 2008/09 | 2009/10 | Total | Differential |
| OP EX | Operational costs - legal advice, training | £ 5,500 | £ 18,810 | £ 24,310 | £ 12,767 | £ 61,574 | £ 74,341 | £ 50,031 |
| | ISP hosting service cost | £ 37,806 | £ 37,806 | £ 75,611 | £ 21,993 | £ 65,978 | £ 87,970 | £ 12,359 |

| | | |
|---|---|---|
| TAL OPERATING EXPENDITURE | £ 34,760 | £ 127,552 |
| OPERATING BUDGET | £ 21,000 | - |

This project spend forecast has been budgeted for in the revised 2008/2009 budget re-forecast and in the 2009/2010 budget.

## Capital investment

### Usability and accessibility analysis, design, test and web page development

Project spend is below forecast. This is due to previously forecast usability work not being required.

### Architecture analysis and design, ISP analysis, tender expertise

Project spend is below forecast. This is made up of an underspend and an additional new spend for the development of a load test plan.

### Requirements capture, Functional Design Specification (FDS) and design documentation

Project spend is above forecast. Although the complexity created by having to host the on-line renewal service away from our existing hosted internet services has created delay and subsequent additional spend, the biggest increase has been due to the final estimate to build the underlying software being higher than the project had previously anticipated. This consists of an additional spend for the system build, for load testing support, for a replica of the system for training and support purposes and for the mocking up of testing screens to assess the usability of the revised authentication model.

This increase in the system build and other work packages have come to light immediately after the development of the functional and non-functional requirements, usability testing and the consequential development and sign off of the hardware and software architecture design and associated security configuration of the system.

The project team investigated the option of reducing the scope of the project deliverables to reduce spend however, this was not considered a viable option. At the beginning of the project, the project team took the MuSCoW[3] approach to the requirements prioritisation of the system. As a consequence the build programme is only building the bare minimum requirements (MUST and SHOULD components). The project has since re-assessed the requirements and losing any existing functionality will make the system less usable, less accessible, less secure and incapable of taking the anticipated loads.

### 3rd parties

Project spend is above forecast. It was anticipated that the project team would use the existing quarterly penetration testing regime to prove the security of the design. Due to the architecture of the solution and the complexity of the design an additional amount has been allocated for penetration testing by a 3rd party.

An allocation has been made for potential changes or modifications to the solution during the build and deployment phase.

Due to revised advice from Oracle Consulting on the synchronisation solution between the hosted on-line renewal service and the Kennington site, a less automated solution will now be used in the solution. This will require Oracle-specific expertise to configure. An additional project spend is forecast.

### New ISP (Internet service provider)

Project spend is below forecast. A below forecast spend in the set up costs is due to a significant reduction in the anticipated cost from the ISP. A project spend over forecast is due to an increase in the lease line set up costs, as a result of hosting the on-line renewal service away from our existing hosted internet services.

### Depreciation

In compliance with HPC's depreciation policy, the capital expenditure of the project will be capitalised on the balance sheet and depreciated (written off over the 3 year useful commercial life) from November 2009 onwards and a small portion will impact the Income and Expenditure Account for the 2009/2010 financial year.

[3] MuSCoW is a method used in business analysis and software development to reach a common understanding with stakeholders on the importance they place on the delivery of each requirement (of any type) - also known MuSCoW prioritisation or MuSCOW analysis. The letters in MuSCoW stand for Mu - MUST have this, S - SHOULD have this if at all possible, Co - COULD have this if it does not affect anything else, W - WON'T have this time but WOULD like in the future.

It is anticipated that the capital expenditure will be depreciated as follows:-

| **2009/2010 (5 months)** | **2010/2011 (12 months)** | **2011/2012 (12 months)** | **2012/2013 (7 months)** |
|---:|---:|---:|---:|
| £89,363 | £214,471 | £214,471 | £125,108 |

**Operational expenditure**
In the 2009/10 round of budgeting, in order to more accurately reflect the overall cost of projects, HPC has been more rigid in ensuring that all costs associated with a project, whether they are directly or indirectly related to the project, are loaded into the respective 2009/10 project budget rather then allocating the cost to the budget of the respective department. As a result of this approach, the project's "operational costs" line item has seen an increase in forecast.

**New ISP – ISP hosting service cost**
Project spend is above forecast. All of the spend in this line item is due to having to host the online renewal service away from our existing hosted internet services. A project spend was forecasted in November 2008 however this has increased due to the more rigid project cost policy to allocate all associated costs to the project budget, in this case, the cost up until "go live" of hosting the on-line renewals.

**HPC - other operational costs**
Project spend is above forecast. This is for the additional contract negotiations with the new ISP. This overspend would not have occurred if the hosting of the on-line renewal service were to occur with our current ISP.

An amount has been allocated for leased line rental and maintenance. For the service to be operational, a direct connection needs to be established between the Kennington office and the remotely -hosted on-line renewals system. The cost for rental and maintenance of this connection until the system goes "live" has been allocated to the on-line renewals project.

Due to the more rigid project cost policy to allocate all associated costs to the project budget, an amount has been allocated for a communication plan to promote the on-line service in its first year of operation.

UAT testing for the on-line service will be carried out by employees from the Registration (and other) teams. They will, in turn, be backfilled by temporary workers for the duration of the testing. Due to the more rigid project cost policy, an amount has been allocated to the online renewals project for this.

## Current project timetable

The estimated project roll out date is scheduled for 18 September 2009, with the project completion, including lessons learnt review, and project closure complete by 1 November 2008.

The high level project delivery plan is in appendix A.

## Key milestones for the next project reporting period

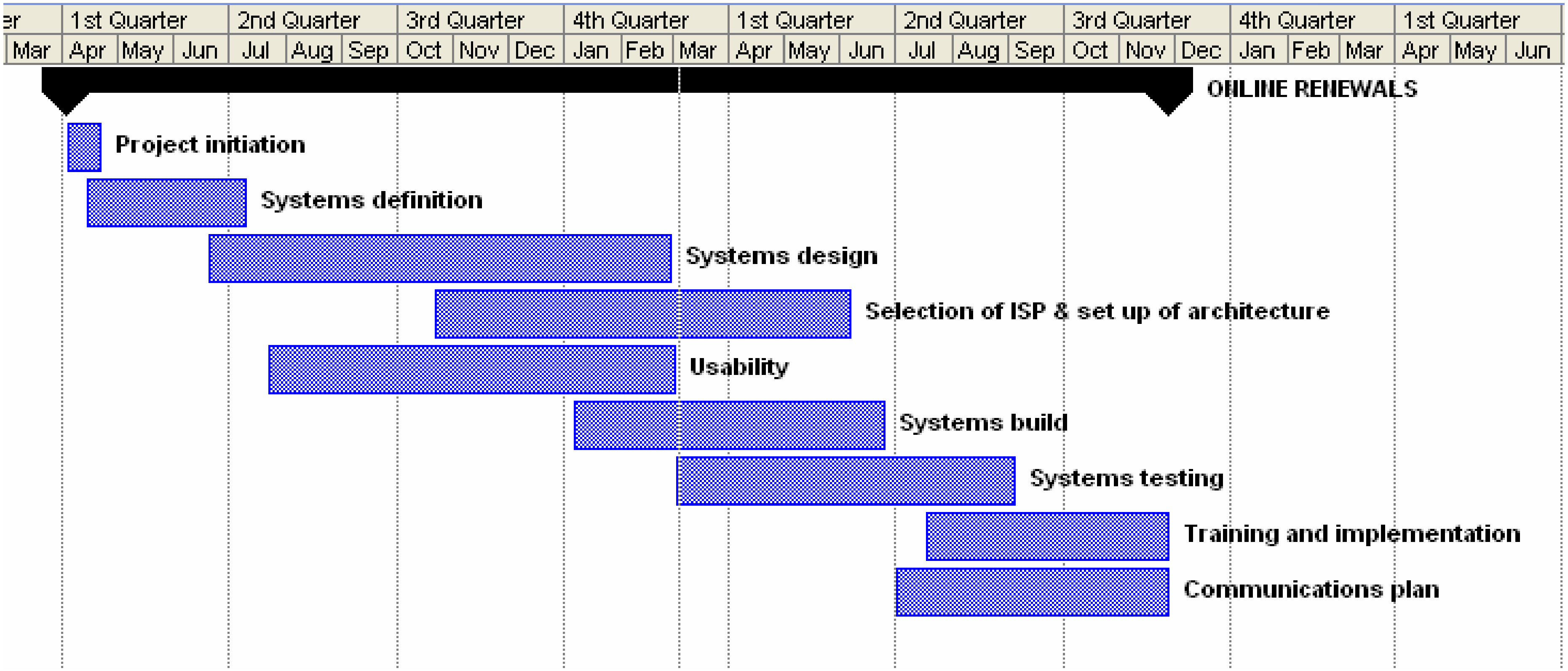
| Key milestones | Date |
|---|---|
| Selection of load testing provider | March 2009 |
| Integrate system with external credit card handler | May 2009 |
| Design of User Acceptance Test (UAT) scripts | May 2009 |
| Complete system build | June 2009 |
| Install leased line between Kennington and online system | June 2009 |
| Obtain analytics tool to analyse web site usage and user experience | September 2009 |
| User acceptance testing (UAT) | June/July 2009 |
| Load testing | August/ September 2009 |

## Challenges over the next reporting period

Apart from DSL delivering the build phase by June 2009, the next project challenge will be the load testing of the system. The project team have worked hard to ensure that the system architecture, design, implementation and system code will ensure the system is scalable and resilient however, it will not be until the system load testing phase that we can validate this. The system load testing is scheduled August/September 2009. Following the load testing, if it is concluded that the system is not meeting the system requirements or throughput targets then the system build or system architecture will need to be modified to address these performance issues. The length of the load testing period is dependant on the issues identified in the load testing cycle. The approach to testing is a cycle of, build, load test, assess results, and address any issues, next iteration, until the system is functioning as expected. The more cycles required, the greater the potential project spend and impact to the “go-live” date.

**Greg Ross-Sampson**
**Director of Operations and Project Lead, Online Applications and Renewals Project**

# Appendix A – high level project delivery plan



# Appendix B – PKF audit report of the planning and management controls over the on-line renewals project

# Health Professions Council

# Online Renewals IT Project

# Review 2008/09

Final February 2009

Confidential

Accountants &
business advisers

# Contents

| **Project timescales** | |
|---|---|
| Date project commenced | 05/02/09 |
| Date field work completed | 09/02/09 |
| Date draft report issued | 11/02/09 |
| Date management comments received | 17/02/09 |
| Date final report issued | 18/02/09 |

# 1 Introduction

1.1 In accordance with our 2008/09 internal audit programme that was agreed with management and the Audit Committee in February 2008, we have undertaken a review of the Health Professions Council's ("HPC's") planning and management controls over the on-line renewals 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 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 February 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.

## 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 a considerable amount of work to be undertaken before the system becomes operational.

2.4 We noted that management has 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.

2.5 We also noted that each stage of the process has been undertaken methodically and reviewed by management and appointed technical specialists when necessary.

2.6 Nevertheless, there remains a considerable amount of work to be undertaken before the project is completed and management recognise the need to continue to exercise a high level of scrutiny as the implementation progresses.

2.7 A key element of this will be the testing programme that is included in the project plan from May to September 2009 and will include, system testing, user acceptance testing and load and security testing.

2.8 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.  However, in our view the HPC's arrangements are what we would expect for an organisation with the risk profile of the HPC and have been designed to meet payment card protection standards. To heighten security still further would be likely to be an even more expensive option.

2.9 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).

2.10 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

2.11 Detailed planning was undertaken by the Project Team to specify the requirements of the HPC for each aspect of the project and to clarify precisely the key milestones.

2.12 We understand that those members of the Project Team who are actively involved with the project at this stage meet twice weekly. Progress reports have been presented to the Executive Management Team ("EMT") and the Finance and Resources Committee throughout the duration of the project to date.

2.13 From our review of the reports provided to the Finance and Resources Committee, we noted that the Committee was provided with a detailed analysis of the cost assumptions and explanations for any increases in the forecast costs of the project. We understand that the decisions to accept cost increases to date have been taken on the basis of the need to deliver the priority objectives of usability, scalability and security. For example, the need to appoint a new ISP was not foreseen in the original project plan and the timelines and cost forecasts have therefore needed to be adjusted accordingly.

2.14 We noted that the current financial forecast for the project includes around £640,000 of capital expenditure (capex) and just under £150,000 of operating expenditure (opex) including indirect overheads spread over two financial years - 2008/09 and 2009/10. Our review of the various project reporting documents indicated that the forecasts have been progressively refined as management have become more certain of the costs. We understand that these matters will continue to be discussed by the Finance and Resources Committee as the project progresses so that the impact on the HPC's overall finances can be monitored effectively.

2.15 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.

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

**PKF (UK) LLP**
**February 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 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 & 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 noted that it is crucial for this system to be operational as quickly as possible to meet the demands of the next round of renewing registrants, who will begin to renew in June 2009, with 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:

- Software virus damage, IT fraud or error;
- Technology obsolescence; and
- Failure to deliver the on-line renewals project as planned.

3.7 The principal management controls through which the HPC is seeking to manage this risk include:

- System specification and design including the use of third party contractors and advisors;
- Project implementation planning and management, including quality assurance; and
- Progress reporting.

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

## Findings

### System specification and design

3.9 This is a relatively technical project and for this reason the HPC engaged specialist advisors to develop the software, deliver usability and to advise on scalability and security issues.

3.10 NCC Group was engaged by the HPC to advise on system scalability and security and to develop the functional and non-functional system requirements with management.

3.11 We noted that a software architecture document ("SAD") was then prepared by the company that was to code and develop the software, Digital Steps Limited ("DSL") 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.

3.12 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.

3.13 Throughout the design the HPC has sought to employ mainstream technology that remains readily accessible and has recognised support and maintenance agreements. This protects the organisation against the risk of obsolescence and facilitates enhancements to the system in the immediate future.

3.14 Based on these specifications 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.

3.15 Etre was appointed to develop 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. This work was based upon the functional and non-functional requirements, particularly the usability and accessibility design considerations.

3.16 We understand that this working prototype was tested with 10 registrants under laboratory conditions, the results of the testing were then analysed and a list of improvements were produced.

3.17 We are advised that Etre has now implemented these improvements and modifications into the prototype and has finished creating a functional specification and a working functional user interface.

3.18 Our review of the reports prepared by NCC indicated that they 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. The principal threat is likely to come from a hacking attack. The system software design therefore incorporates best practice counter-measures to address this threat as advised by NCC.

3.19 NCC provided the HPC with a number of options but recommended that the organisation should adopt a site access password requirement of eight characters alphanumeric together with additional Registration and authentication numbers on the basis that this would make such attacks difficult and time-consuming and provide adequate security for the specified usage profile of the service. This protection is to be underpinned by further counter-measures built into the software design, which prevent other commonly used hacking methods.

3.20 Some examples of the counter-measures built into the design specification are set out in the table below;

| Description | Requirement |
|---|---|
| Login reporting | Log failed authentication attempts |
| Communication security | Disable weak SSL ciphers and only supporting SSLv3.0 and/or TLS1.0 |
| HTTPS | Consider forcing all authenticated users to use a HTTPS connection |
| Error Handling | Ensure that it is not possible to solicit any verbose error messages from the application |
| Cross Site Scripting | Prevent Cross Site Scripting |
| HTTP Methods | Disable unnecessary and insecure HTTP methods |
| Robots | Avoid using Robot.txt file for indexing sensitive directories |
| Comments in Source code | Use comments only in development web sites and not productions ones |
| Session ID | The application should remove any processes that place the users JSESSIONID value in either the referrer field or the URL |
| Prevention of system attacks | System must be secure enough to prevent attacks that would compromise the security of the system or its performance |

| Description | Requirement |
|---|---|
| Security standard | All credit card handling must be PCI DSS compliant |
| Session Management | Ensure that authenticated users have a robust and cryptographically secure association with their session |
| Session time-out | Set server sessions time out |
| Prevent SQL injections | Implement measures to protect the WS against SQL injections |

3.21 As part of the analysis, doubts were raised about whether the HPC's current Internet Service Provider (ISP) could meet the system requirements and ensure the system would be secure and scalable.

3.22 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. This means that no credit card data will touch the HPC environment. However, to ensure the security of this platform the ISP needs to be PCI (DSS Payment Card Industry Data Security Standard) Service Provider compliant.

3.23 Further analysis indicated that the HPC's current ISP could not provide management with a satisfactory level of assurance and decision was taken to seek to appoint a new ISP through a tender process. Through our review of the Executive Management Team minutes for February 2009 we noted that the new ISP has recently been appointed.

3.24 Our review indicated that 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 but to retain the existing ISP to host the HPC's current websites (www.hpc-uk.org / www.hpcheck.org / www.healthregulation.org).

3.25 This also has the advantage that the current HPC websites remain separate from the new development, at least for the time being, ensuring that they remain subject to the tried and tested security controls that have been in place for some time.

3.26 Based on our review of the steps that have been taken to date, we have concluded that management has 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.

3.27 We have noted that each stage of the process has been undertaken methodically and reviewed by management and appointed technical specialists when necessary.

3.28 Nevertheless, there remains a considerable amount of work to be undertaken before the project is completed and management recognise the need to continue to exercise a high level of scrutiny as the implementation progresses.

3.29 A key element of this will be the testing programme that is included in the project plan from May to September 2009 and will include, system testing, user acceptance testing and sign off and load and security testing.

### Project planning and reporting

3.30 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). 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.

3.31 The overall approach to the project was set out in a Project Brief. Our review work indicated that his 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.

3.32 The current key milestones for the project are set out in the table below:

| Project milestones | Timeline |
|---|---|
| Project initiation and information gathering | April - July 2008 |
| Conceptual architecture and application design | July- November 2008 |
| ISP tender exercise and appointment<br>Systems build | November 2008- February 2009 |
| Testing | March - September 2009 |
| Training and implementation and roll out | September - 1st November 2009 |

3.33 We understand that at this stage of the project the only individuals in the Project Team involved on a regular basis are the Project Manager, the Director of Operations (senior business user) and the Director of IT (IT expert).

3.34 Although we are advised that it is the intention of the Project Team to adopt the HPC's highlight reports format for reporting where this is useful as the project progresses, reporting is currently undertaken through meetings between those actively involved in the project at present on Wednesdays and Fridays. We noted that progress with the project has been reported more formally through the HPC's major projects score card report which is presented to EMT every two weeks.

3.35 The Finance and Resources Committee has also received two papers on the project during 2008/09. The most recent paper presented was to the November 2008 meeting. This included the following matters:

- a detailed update on the work undertaken to date during 2008;
- the current timetable;
- explanations of the reasons behind the appointment of the various technical advisors;
- revised budget and financial report; and
- detailed cost/ benefit analysis.

3.36 From our review of this document we noted that the Finance and Resources Committee was provided with a detailed analysis of the uncertainties inherent in some of the cost assumptions and the reasons why the budget for the project has increased. For example, the need to appoint a new ISP was not foreseen in the original project plan and the timelines and costs have therefore needed to be adjusted accordingly.

3.37 A further paper is scheduled to be presented to the Finance and Resources Committee in the near future. We noted that the current financial forecast for the project includes around £640,000 of capital expenditure (capex) and just under £150,000 of operating expenditure (opex) including indirect overheads spread over two financial years - 2008/09 and 2009/10.

3.38 Our review of the various project reporting documents indicated that the forecasts have been progressively refined as management have become more certain of the costs. We understand that these matters will continue to be discussed by the Finance and Resources Committee as the project progresses so that the impact on the HPC's overall finances can be monitored effectively.

# 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. |