Health Professions Council
Audit Committee Meeting – 27th March 2007

PKF AUDIT PLAN 2007/08 FINAL - PUBLIC PAPER

Executive Summary and Recommendations

1. Introduction
The PKF Audit Plan was presented to the last Audit Committee Meeting. Since then, the IT and FTP Audit Reports have been received from PKF. In light of the findings, the proposed Audit Plan is being re-submitted in case the Committee wants to amend the emphasis in the Plan.

2. Decision
The Committee is requested to review the IT and FTP Audit Reports and make any amendments to the latest PKF Audit Plan for 2007/08, as it sees fit.

3. Background information
Nil.

4. Resource implications
Nil

5. Financial implications
Nil

6. Background papers
Nil

7. Appendices
PKF Audit Plan for 2007/08 (amended for changes from the last Audit Committee meeting)

8. Date of paper
16th March 2007

hpc health professions council

INTERNAL AUDIT SERVICE

Final

AUDIT PLAN 2007/2008

PKF

Accountants &
business advisers

INTRODUCTION

1.1 The purpose of this paper is to summarise the planned areas for internal audit coverage for the 2007/08 financial year. The draft plan was considered by the February meeting of the Audit Committee and this version includes the changes agreed at that time.

AUDIT STRATEGY

1.2 This Audit Programme has been based on our proposed Strategic Audit Plan for 2006/07 to 2008/09. We have considered the overall risk position of Health Professions Council and are satisfied that the rationale underpinning the original strategy is unchanged and therefore no significant revision is required to the audits scheduled for the forthcoming year.

1.3 Our proposed 2007/08 Audit Plan comprises the following core strands:

Review of governance – assessment of the governance arrangements including planning, decision making and reporting taking account of the risk management arrangements and best practices.

Assurance to support the Statement on Internal Control and the Accounting Officer – programmes of evaluation and testing of controls of existing systems and transactions in order to provide assurance that internal control is adequate in the current year and to enable the Accountable Officer to make a declaration on financial and operational control for the financial statements.

Review of the core processes – programmes of evaluation and testing of controls of existing systems and transactions in order to provide assurance that internal control is adequate in the current year across the core processes within the HPC.

Review of divisions - programmes of evaluation and testing of controls of existing systems and transactions in order to provide assurance that internal control is adequate in the current year across the divisions within the HPC.

Supporting the strategic plan – consideration of risks and other issues involved in the delivery of the strategic plans, the management of changes and the scope for making efficiency or quality improvements. These can only be set each year based on the priorities for that year and in subsequent years an allowance is made for such projects only.

1.4 In practice these objectives will not necessarily be met by discrete reviews, with some reviews potentially contributing to all three objectives.

1.5 In 2007/08 the aim will be to provide assurance over the key systems and processes needed to support the statement of internal control. Total assurance effort will be maximised by co-ordinating fully with the in house Quality Auditor and the external ISO auditors where appropriate.

1.6 We will also liaise with the NAO and Baker Tilly to ensure that they can place reliance on our work.

1.7 A summary of the proposed 2007/08 Audit Programme is set out as Appendix A. This includes the provisional timings proposed for the year by quarter.

1.8 The extent to which the Audit Programme addresses the Health Professions Council risks is summarised in Appendix B and C.

APPENDIX A AUDIT PROGRAMME 2007/2008

Corporate governance:

SYSTEM	REVIEW OUTLINE	DAYS	TIMING
Corporate Governance and Risk Management	Annual assessment of the corporate governance arrangements for the Health Professions Council. This year's review will focus on the development and use of risk management and follow up of action on the issues identified in the year one review.	5	Q 4
Planned Input		**5**	

Core Processes and Functions:

SYSTEM	REVIEW OUTLINE	DAYS	TIMING
Financial Systems	Review and testing of the controls over the main financial systems and follow up of agreed actions from the 2006/7 review. This will cover the core areas of: • Payroll; • Budgetary control; • Ledger management; • Asset management; • Income, including forecasting, billing, recovery and recognition; • Purchasing and payments; • Travel and subsistence; • Cash management including cash flow management, banking and reporting.	13	Q 3
External Communication	Assessment of the arrangements for managing the quality, timeliness and consistency of external communications, focusing on communications professional bodies and with the public (under Article 13(3)). This will consider the risks involved, how the required communications are delivered and the effectiveness of the monitoring of performance in these areas.	6	Q 2
Planned Input		**19**	

Operational Functions:

SYSTEM	REVIEW OUTLINE	DAYS	TIMING
Fitness to Practice – Phase II	Follow up of audit recommendations from 2006/07 review and specific consideration of the management of the new FTP database, APU.	3	Q 2
Registrations	Review and testing of the controls within the Registrations function. This will cover the risk management arrangements, performance management arrangements and operational controls relating to registrations.	5	Q4
Business Continuity Planning and Disaster Recovery Planning	Assessment of non IT business continuity arrangements and disaster recovery arrangements with a focus on premises and staff availability issues and the ability to respond to major incidents. The review will examine: • Risk assessment process for business-critical elements at a corporate level; • Adequacy of response planning; • Adequacy of testing.	3	Q1
Planned Input		**11**	

Change Projects:

SYSTEM	REVIEW OUTLINE	DAYS	TIMING
New Building Project	The review will revisit the arrangements for managing the project and seek to confirm that the key project controls are continuing to operate. Note: This assumes that the 2006/7 review does not identify any significant issues. If this is not the case the scope of this review may need to be revised and the audit contingency utilised.	2	Q 3
Planned Input		**2**	

IT Systems:

SYSTEM	REVIEW OUTLINE	DAYS	TIMING
IT review – Laptop controls	Assessment of arrangements for laptop encryption and anti theft arrangements and software licensing.	2	Q 3
Planned Input		**2**	

Planning/Management Reporting:

SYSTEM	REVIEW OUTLINE	DAYS
Planning	Development of the Annual Plan through a reconsideration of audit risks and developments and the associated discussions.	1
Management	Overseeing the delivery of audit work and conducting detailed reviews. Liaison with managers in order to keep up to date. Liaison with the External Auditor. Consideration of the results of other quality assurance work.	2
Reporting	Attendance at Audit Committee. Keeping senior management informed of audit progress and key issues. Production of the Annual Report.	3
Planned Input		**6**

Contingency:

SYSTEM	REVIEW OUTLINE	DAYS
Contingency	Area to be audited at the direction of the Audit Committee.	2
Indicative Input		**2**

Total Expected Input for 2007/08 - 47 days

Total Fee for 2007/08 - £24,168

APPENDIX B AUDIT PROGRAMME – LINKS TO STRATEGIC RISKS

Audit Coverage in 2007/08	Strategic Risk – referenced to HPC risk register at appendix C
Corporate Governance and Risk Management	Corporate Governance - 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11
Financial Systems	Financial – 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10, 15.11, 15.12, 15.13, 15.14, 15.15, 15.16, 15.17, 15.18
Communications	Communications – 3.1,3.2,3.3
Registration	Registrations 10.1,10.2,10.3,10,4,10,5
New Building Project	Operations - 2.1, 2.7
Business Continuity and Disaster Recovery Planning	IT - 5.1, 5.2

APPENDIX C HPC Risk Register

Ref	Category		Description
1	**Strategic**	1.1	HPC fails to deliver OIC
		1.2	Unexpected change in UK legislation
		1.3	Incompatible OIC and EU legislation
		1.4	CHRE conflict
2	**Operations**	2.1	Inability to occupy premises or use interior equipment
		2.2	Rapid increase in registrant numbers
		2.3	Unacceptable service standards
		2.4	Postal or telephone disruption
		2.5	Public transport disruption
		2.7	Inability to accommodate HPC employees
3	**Communications**	3.1	Failure to inform public Article 3(13)
		3.2	Loss of support from professional bodies
		3.3	Inability to inform stakeholders following crisis
4	**Corporate**	4.1	Council inability to make decisions
		4.2	Council members conflict of interest
		4.3	Poor decision-making e.g. conflicting advice or conflicting advice & decisions
		4.4	Failure to meet Council and Committee quorums
		4.5	Members' poor performance
		4.6	Poor performance by the President
		4.7	Poor performance by Chief Executive
		4.8	Improper financial incentives offered to Council members/employees
		4.9	Health and Safety of Council Members
		4.10	Member recruitment problem (with the requisite skills)
		4.11	Expense claim abuse by members
5	**IT**	5.1	Software Virus damage
		5.2	Technology obsolescence, hardware and software
		5.3	IT fraud or error
6	**Partners**	6.1	Inability to recruit and/or retain suitable Partners
		6.2	Incorrect interpretation of law and/or Sis resulting in CHRE reviews
		6.3	Health & Safety of Partners

Ref	Category		Description
7	**Approvals &**	7.1	Non-detection of low education providers standards

	Monitoring & CPD	7.2 Education providers refusing visits or not submitting data 7.3 Inability to manage Education Provider (EP) visits 7.4 Loss of support from EP 7.5 CPD processes not operational by July 2008
8	**Project Management**	8.1 CPD processes not operational by July 2008 8.2 Fee change processes not operational by June 2007 8.3 Professional Qualification Directives processes not operational by October 2007 8.4 Failure to regulate a new profession or a post-registration qualification as stipulated by legislation
9	**Quality Management**	9.1 Loss of ISO 9000 Certification
10	**Registration**	10.1 Customer service failures 10.2 LISA Registration system failure 10.3 Inability to detect fraudulent applications 10.4 Backlogs of registration and GP applns 10.5 Failure to meet the Registration Dept merger project timetable
11	**HR**	11.1 Loss of key HPC employees (person cover risk) 11.2 High turnover of employees 11.3 Inability to recruit suitable employees 11.4 Lack of technical and managerial skills to delivery the strategy 11.5 Health & Safety of employees 11.6 High sick leave levels 11.7 Employee and ex-employee litigation 11.8 Employer/employee inappropriate behaviour 11.9 Non Compliance with Employment legislation
12	**Legal**	12.1 Judicial review of Rules, Standards and Guidance

Ref	Category	Description

13	**Fitness to Practice**	13.1	Legal cost over-runs
		13.2	Legal challenge to HPC operations
		13.3	Tribunal exceptional costs, FTP, Registrations and CPD Appeals
		13.4	Rapid increase in the number of tribunerals and resultant legal costs
		13.5	Witness non-attendance
		13.6	Employee/Partner physical assault by Hearing attendees
		13.7	Registration Appeals
14	**Policy and Standards**	14.1	Incorrect process followed to establish stds/guidance/policy eg no relevant Council decision
		14.2	Inappropriate stds/guidance published eg stds are set at inappropriate level, are too confusing or are conflicting
		14.3	Changing/evolving legal advice rendering previous work inappropriate
		14.4	Inadequate preparation for a change in legislation (Health Professions Order, or other legislation affecting HPC)
15	**Finance**	15.1	Insufficient Cash to meet commitments
		15.2	Unexpected rise in operating expenses
		15.3	Large Capital Project Cost Over-runs
		15.4	Loss in value of investment portfolio
		15.5	Inability to pay creditors
		15.6	Inability to collect from debtors
		15.7	Registrant Credit Card record fraud
		15.8	Total receipt of correct fee income
		15.9	Mismatch between Council goals & approved financial budgets
		15.10	Unauthorised payments to organisations
		15.11	Unauthorised payments to personnel
		15.12	Unauthorised removal of assets (custody issue)
		15.13	Mis-signing of cheques (forgery)
		15.14	Tax law non compliance
		15.15	Non compliance with Privy Council/Treasury Guidelines/UK GAAP/IFRS
		15.16	Qualified opinion received by the Auditors on the Annual Financial Statements
		15.17	Late submission of the Financial Statements/Annual Report, beyond sector standards
		15.18	Fund Manager or Money Market provider insolvency
16	**Pensions**	16.1	Under-funded pension liabilities (CPSM Retirement Benefits Scheme*)
		16.2	Flexiplan funding liability resulting from new Scheme Specific Funding Standard (SSFS) and insufficient Pensions Capital to meet fund obligations
		16.3	Significant costs incurred to adopt changes to existing HPC (Capita Flexiplan) pension scheme

Audit Scope Area	Work Carried Out	Findings
Strategic approach to IT development and acquisition	Review of IT strategy for fit with the corporate objectives, appropriate span of coverage and compliance with best practice.	The network comprises approximately 9 servers. There is an IT Strategy in place covering the period 2006 – 2011. There are three full time members of the IT team. They are responsible for Network support and IT security, Back office system development and IT support. There are a number of IT projects in progress and these are managed in house by the IT Director.
IT Security Policy	Review of IT security policy for the appropriateness of content.	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; • Incident response procedures
Physical access controls over PC and network equipment	Assessment of physical controls by visiting the HPC premises.	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. 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.

Audit Scope Area	Work Carried Out	Findings
Logical access controls including remote access to the network	Review of arrangements for protecting logical access against standard practices. Note: This has not been tested.	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. There are also approximately 20 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.
IT support for users	An examination of the arrangements in place for IT support.	Covered in detail as part of the IT Service Level Agreement review
Hardware and software maintenance	An examination of the arrangements in place 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.	All hardware and software are purchased and installed by IT. The maintenance of the main systems was covered in detail as part of the IT Service Level Agreement review
Backup and restoration procedures	An examination of the backup and disaster recovery procedures for appropriateness for the level of risk. Consideration of testing arrangements. Note: The backup and disaster recovery arrangements were not tested as part of this audit.	Covered in detail as part of the IT Service Level Agreement review

Audit Scope Area	Work Carried Out	Findings
Network resilience	Review of Firewalls and penetration testing arrangements. Note: These were not tested.	Firewall software called Watchguard is used to protect the HPC network and is fully managed by Star. A periodic PC audit is performed by Planet Sun. In addition penetration testing is carried out on the network to check the robustness of the firewall security on an annual basis.