Health Professions Council
Audit Committee – 26th June 2007

INTERNAL AUDIT REPORT – BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Executive Summary and Recommendations

Introduction

As part of the internal audit programme for 2007/8 PKF undertook a review of the Business Continuity Planning and Disaster Recovery Planning at HPC. The attached report which includes a management response was agreed with the Executive in June 2007.

Decision

The Committee is asked to discuss the report.

Background information

At its meeting on 27 March 2007, the Committee approved the Internal Audit Needs Assessment and Internal Audit Plan for 2007-8. (See paper AUD 22/07).

Resource implications

None

Financial implications

None

Appendices

Date of paper

13 June 2007

PKF

Accountants &
business advisers

hpc health professions council

Business Continuity Planning and Disaster Recovery Planning

June 2007

Final - Confidential

Assurance Level: Satisfactory – Satisfactory design of internal control that addresses the main risks but falls short of best practice and is operating as intended

Staff Interviewed – Roy Dunn and Simon Leicester

Audit Team – Mark Wonnacott

Contents

1 Introduction

1.1 This review forms part of our 2007/2008 internal audit, which has been carried out in accordance with the programme which has been agreed with the Audit Committee in June 2006.

1.2 The aim of the audit was the 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 audit examined :

- Risk assessment process for business-critical elements at a corporate level;
- Adequacy of response planning; and
- Adequacy of testing plans.

1.3 The work was carried out primarily by holding discussions with relevant staff, reviewing any available documentation and testing controls in place to determine their effectiveness. The audit fieldwork was completed in June 2007.

1.4 This report has been prepared as part of the internal audit of the Health Professions Council (HPC) 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 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 and our conclusions on the arrangements for business continuity and disaster recovery planning at HPC. The work was performed as part of our internal audit plan for 2007/08.

Overall Conclusion

2.2 We have carried out the audit in accordance with the programme agreed with you. Based on the audit work carried out we have concluded that the level of control over Business Continuity Planning and Disaster Recovery is **Satisfactory**.

2.3 The HPC has established and documented a Disaster Recovery Plan which outlines clear lines of authority, prioritises work efforts and acts as a comprehensive statement of consistent actions to be taken before, during and after any disaster. Our review of the business continuity planning arrangements indicated that the disaster recovery plan has been documented and contains sufficient information for staff members to resume normal processing for all critical operations within a reasonable time frame.

2.4 The disaster recovery arrangements cover all key areas and are updated and amended on a regular basis. We have concluded that the HPC have a plan that complies with best practice. However, having appropriate plans is not sufficient. They need to be communicated to all relevant people, be supported so that they can happen and tested to ensure that they work. Whilst our review has indicated that all of these are in place, testing has not been carried out to the proposed plan.

2.5 We have not identified any fundamental concerns in any of the areas covered during this audit, although there remain some areas affected by minor risks whereby further steps should be taken to strengthen the controls in order to mitigate these risks.

2.6 We have identified an area where controls could be further strengthened and have made recommendation in this regard notably in respect of:

- The Departmental Disaster Recovery testing plan should be performed and reported to the delegated committees as scheduled.

2.7 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
June 2007

3 Detailed Findings

Adequacy of Responses Plans and Risk Assessment process for business critical elements at a Corporate Level

Our assessment

3.1 Our review of the business continuity planning arrangements indicated that the disaster recovery plan had been well documented and contains sufficient information for staff members to resume normal processing for all critical operations within a reasonable time frame.

3.2 The disaster recovery arrangements cover all key areas and are updated and amended on a regular basis. In the event of a disaster occurring we have concluded that the HPC have a plan that complies with best practice.

Our findings

3.3 We confirmed that the Council has a Disaster Recovery (DR) Plan in place and in establishing the disaster recovery plan, the following factors where considered:

- Minimising the duration of a serious disruption to business operations;
- Planning and prioritisation – determination of critical and less critical business needs;
- Facilitating effective co-ordination of recovery tasks;
- Reducing the complexity of the recovery effort; and
- Communications (internal and external parties).

3.4 The DR plan that is in place has been designed to :

- Provide management with a comprehensive understanding of the total effort required to develop and maintain an effective DR plan;
- Obtain commitment from appropriate management to support and participate in the effort;
- Define recovery requirements from the perspective of the business functions;
- Document the impact of an extended loss of operations and key business functions;
- Focus appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- Select project teams to ensure the proper balance required for plan development;
- Develop a contingency planning consideration must be integrated into ongoing business planning and system development processes, in order for the plan to remain viable over time;

- Define how contingency planning considerations must be integrated into ongoing business planning and system development processes, in order for the plan to remain viable over time;
- Provide a sense of security for employee;
- Guarantee the reliability of standby systems; and
- Minimise decision-making during a disaster.

3.5 The following individuals each have a full copy of the DR plan. The heads of departments – Approvals, Communications, CE&R, FTP, Finance, Human Resources, Info & IT. International and UK Registrations, Operations, Facilities, Secretariat. In addition the President and the Committee Chairman also have a copy. Each member of the EMT has a copy of the plan in the office and additionally at their home to provide for events occurring outside of office hours. The Disaster recovery plan contains the following sections:

3.6 - Deciding on type of response to disaster. Examples of disaster types have been noted and what type of response would be made, for example whether or not to remain at Park House.

3.7 - Who does what detailing position, priority level, responsibility under disaster recovery, replaceable by, and response phase in days. This has assigned initial actions to various members of the BC team and detailed the action that will be needed on day one , then days 2 to 5, and then days six and onwards.

3.8 - How to evoke disaster recovery plan and the procedure to follow if invoking DR plan.

3.9 - Key business functions to restore. This includes the critical functions that the organisation carries out and has assessed the objective recovery time and the objective recovery point also.

3.10 - Use of disaster recovery office. The organisation utilises the services of a disaster recovery company called NDR. NDR providers the Council with off site location and can supply servers and 10 PC's. We confirmed that senior management of the organisation had visited the off site office space maintained by NDR the disaster recovery company. NDR are based in Uxbridge, Middlesex and the DR plan includes details of their location and contact details. In addition arrangements have been made at the alternate site to hold essential items for use in the event of a disaster. These are held in the "war box" and include – a cheque book to ensure that payments can be made in the short term, lotus notes security file on CD and a supply of headed HOC stationery.

3.11 - Contact details. These are updated each month using the information contained in the HR database. This includes the contact details for every staff member at HPC and is sent in a sealed envelope to each member of the Business Continuity team to ensure that contact details remain current.

3.12 - Core processes by departments and recovery time. This section of the DR plan has been completed by all of the operational areas within the HPC. Each department has assessed the critical business functions, the timescale for renewal, why the function must commence within this timescale and what critical resources are required. From our review of the DR plan we have concluded that this exercise has been done comprehensively for each department. The DR plan also includes a section detailing the key documents and items to be recovered from the HPC campus. This has also been done for each operational department.

3.13 Plan review and update process. As part of the maintenance of the DR plan the plan is reviewed twice a year at the EMT away day. This ensures that the plan is kept up to date and remains a live document that is updated for any changes that may have occurred.

3.14 Key process diagrams for core functions. For each of the key operational areas flow diagrams have been documented and included within the DR plan.

3.15 From review of the DR plan it is clear that a high level of work has gone into the preparation and updating of the document. The BC Co-ordinator and the BC team have ensured that business critical systems and functions have been identified and that the time critical factor of each of these systems and functions has been built into the DR plan.

Adequacy of Testing Plans

Our assessment

3.16 Our review of the disaster recovery testing plans indicated that there are arrangements in place but that the testing is behind the planned programme.

Our findings

3.17 From our review of the Disaster Recovery Plan we have noted that there is an annual departmental testing schedule is in place. The schedule details the department that is to be tested, the suggested date for testing and the date when the test has been completed.

3.18 The table over the page shows the departmental testing plan:

Department	Suggested Test Date
IT	February
Operations	February
Finance	January
FTP	April
Operations International	May
Approvals and Monitoring / CPD/Aspirant Groups	August
Secretariat	June
Human Resources	September
Facilities	October
Communications	November
Policy and Standards	January

3.19 IT was established that only two of the programmed annual departmental tests had been performed to date.

Recommendation

R1 The Departmental Disaster Recovery testing plan should be performed and reported to the delegated committees as scheduled.

3.20 It was established that in February 2007 a test was also conducted and was successful. The test conducted involved streamed the LISA backup data to the Councils internet service provider and showed that this can be accessed and updated from the NDR off site office space within 45 minutes of requesting the data to be loaded up. Additionally in May 2007 a Disaster Recovery test on LISA data and application were evoked and lessons learned from the exercise were also noted.

3.21 During the last year there have also been two non planned invocations. These occurred in October 2006 due to a power outage in South London and a reverse proxy unit failure after the power outage two days later. The lessons learned from these events have been recorded and reported to the Finance and Resources Committee.

3.22 Formal testing of the disaster recovery plan should be undertaken to ensure that the planned responses are adequate and appropriate for major incidents. This will also ensure that there are no additional gaps in the existing plans and allow lessons to be learned that can be incorporated into the existing plans.

4 Action Plan

Ref.	Findings	Recommendations	Priority	Management Response *Responsible Officer*	Due Date
R1	From our review of the Disaster Recovery Plan we have noted that there is an annual departmental testing schedule is in place. The schedule details the department that is to be tested, the suggested date for testing and the date when the test has been completed. We noted that the departmental disaster recovery tests were not always undertaken.	**The Departmental Disaster Recovery testing plan should be performed and reported to the delegated committees as scheduled.**	**Medium**	HPC will evaluate the recommendations of BS 25999-1:2006 concerning types and methods of exercising BCM strategies; and implement by the end of the year. This takes into account the complexity of the plan, and is designed to minimise business risk. *Director of IT*	End of 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 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.