

Audit Committee, 28 November 2013

Internal Audit Report – Disaster Recovery / Business Continuity Planning

Executive summary and recommendations

**Introduction**

As part of the Internal Audit Plan for 2013-14, Mazars have undertaken a review of the Health and Care Professions Council's disaster recovery and business continuity planning.

**Decision**

The Committee is asked to discuss the report

**Resource implications**

None

**Financial implications**

Mazars' fees £27,000

**Appendices**

Internal Audit Report – Disaster Recovery / Business Continuity Planning

**Date of paper**

18 November 2013



Internal Audit Report

**Disaster Recovery / Business  
Continuity Planning (03.13/14)**

**October 2013**

**FINAL REPORT**

## CONTENTS

1. Introduction	Page 1
2. Background	1
3. Scope and objectives of the audit	1
4. Audit Findings: One page summary	3
5. Summary of findings	4
6. Action plan agreed with management	5

### Appendix 1 – Definitions of Assurance Levels and Recommendations

#### AUDIT CONTROL SCHEDULE:

<b>Client contacts</b>	Greg Ross-Sampson: Director of Operations  Roy Dunn: Head of Business Process Improvement	<b>Internal Audit Team</b>	Peter Cudlip: Partner  Graeme Clarke: Director  James Sherrett: Assistant Manager  Neil Belton: IT Audit Manager
<b>Finish on Site \ Exit Meeting:</b>	3 October 2013	<b>Management responses received:</b>	24 October 2013 29 October 2013
<b>Draft report issued:</b>	21 October 2013	<b>Final report issued:</b>	29 October 2013

In the event of any questions arising from this report please contact Graeme Clarke, Director, Mazars LLP [graeme.clarke@mazars.co.uk](mailto:graeme.clarke@mazars.co.uk)

#### **Status of our reports**

*This report has been prepared for the sole use of the Health and Care Professions Council.*

*This report must not be disclosed to any third party or reproduced in whole or in part without the prior written consent of Mazars LLP. To the fullest extent permitted by law, no responsibility or liability is accepted by Mazars LLP to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.*

## 1. INTRODUCTION

- 1.1 As part of the Internal Audit Plan for 2013/14, we have undertaken a review of the Health and Care Professions Council's (HCPC) disaster recovery and business continuity planning processes. The audit was included in the Plan owing to the number of risks identified in HCPC's Risk Register relating to disaster recovery and business continuity.
- 1.2 The last internal audit review of HCPC's overall Disaster Recovery and business continuity arrangements was undertaken by the previous internal auditors in 2010/11 and provided a 'Sound to date' opinion.
- 1.3 We are grateful to the Head of Business Process Improvement, the IT team, and other members of staff for their assistance during the course of the audit.
- 1.4 This report is for the use of the Audit Committee and senior management of HCPC. The report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Such matters have been discussed with the relevant staff.

## 2. BACKGROUND

- 2.1 Business continuity planning identifies an organisation's exposure to internal and external threats and establishes mechanisms to provide effective protection and recovery for the organisation's facilities and services whilst maintaining business operations. A business continuity plan is a roadmap for continuing operations under adverse conditions such as a flood, fire or pandemic.
- 2.2 Any event that could have a significant impact on continued operations should be considered within a business continuity plan (BCP) such as loss of, or damage to, critical infrastructure including computing / network resource, buildings or facilities. As such, risk management must be incorporated into any BCP.
- 2.3 BCPs and disaster recovery measures should be subject to regular review and test to ensure they remain appropriate, effective and to ensure management are fully aware and understand their responsibilities in the event of an incident occurring.
- 2.4 HCPC's primary mitigation in the event of a sustained disaster recovery / business continuity issue / event is to relocate operations to a disaster recovery company, Phoenix (formerly ICM), in Uxbridge. This provides 10 seats, with telephones, PCs, internet communications and access to replicated data at the Internet Service Provider (Rackspace in Reading) hosting HCPC data.

## 3. SCOPE AND OBJECTIVES OF THE AUDIT

- 3.1 Our audit considered the following risks relating to the area under review:
  - "Interruption to electricity supply" (*HCPC Risk Register, Ref 2.7, September 2013 - Residual Risk High*);
  - "Basement flooding" (*HCPC Risk Register, Ref 2.11, September 2013 – Residual Risk Medium*);
  - "Failure of IT Continuity Provision" (*HCPC Risk Register, Ref 5.4, September 2013 – Residual Risk Low*);

- Inadequate or untested procedures in place for dealing with emergencies, resulting in potential inability to continue in the event of loss of systems / staff etc.; and
- Losses of key financial and operational data, due to failure to ensure adequate back-up arrangements are in place.

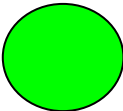
3.2 In reviewing the above risks, our audit considered the following areas:

- Disaster Recovery/ Business Continuity Plan;
- Assessment of operations and systems and prioritisation / importance to HCPC;
- Assignment of responsibilities for dealing with disasters and communication of respective roles and responsibilities of individuals;
- Testing, review and updating of the DR / Business Continuity Plan;
- Stand-by disaster recovery services and arrangements including periodic testing to ensure that they are effective, workable and current;
- Back ups – including frequency, adequacy, testing and secure storage;
- Arrangements with third parties –for provision of recovery sites / services / equipment; and
- Monitoring and reporting of incidents / near misses to Executive Management Team / Committee.

3.3 The objectives of our audit were to evaluate the adequacy of controls and processes for disaster recovery and business continuity planning in the areas under review, and the extent to which controls have been applied, with a view to providing an opinion on the extent to which risks in this area are managed. In giving this assessment, it should be noted that assurance cannot be absolute. The most an Internal Audit service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control.

3.4 We are only able to provide an overall assessment on those aspects of the controls and processes for disaster recovery and business continuity planning that we have tested or reviewed. The responsibility for maintaining internal control rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy of the internal control arrangements implemented by management and perform testing on those controls to ensure that they are operating for the period under review. We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone are not a guarantee that fraud, where existing, will be discovered.

#### 4. AUDIT FINDINGS: ONE PAGE SUMMARY

Assurance on effectiveness of internal controls	
	<b>Substantial Assurance</b>

Recommendations summary	
Priority	No. of recommendations
1 (Fundamental)	None
2 (Significant)	None
3 (Housekeeping)	1
<b>Total</b>	<b>1</b>

Risk management
<p>Operational, financial and reputational risks which could arise in the event of a business continuity incident occurring can be considerable. As referred to in 3.1 above, HCPC's Risk Register contains specific risks associated with disaster recovery and business continuity planning.</p> <p>Testing undertaken as part of this audit has confirmed the mitigating actions in respect of the areas reviewed as part of this audit are in place and operating effectively.</p>

Value for money
<p>Value for money considerations can arise in this area through the costs involved in designing, testing and maintaining the various methods of business continuity and disaster recovery. Efficient and effective recovery in the event of a disaster occurring is vital due to the importance of maintaining core business services.</p> <p>HCPC are benefiting from the establishment of a business continuity framework, supported by effective and tested recovery plans covering the range of the organisation's operations.</p> <p>No specific value for money issues were highlighted in our review.</p>

## 5. SUMMARY OF FINDINGS

### Overall conclusion on effectiveness and application of internal controls

- 5.1 Taking account of the issues identified in paragraphs 5.2 to 5.4 below, in our opinion the control framework for disaster recovery and business continuity planning for the areas reviewed, as currently laid down and operated at the time of our review, provides **substantial** assurance that risks material to the achievement of HCPC's objectives are adequately managed and controlled.

### Areas where controls are operating effectively

- 5.2 The following are examples of controls which we have considered are operating effectively at the time of our review:

- The organisation has a fully defined Business Continuity Plan including IT Disaster Recovery plans;
- Core IT Services are hosted onsite but replicated offsite to provide redundancy and recovery measures. Failover procedures between the two sites have been implemented and tested;
- Services and departmental functions have been assessed for their importance and all services are covered by the recovery plans;
- A third party support contract for Disaster Recovery services is in place with Phoenix, previously known as ICM;
- Responsibilities are clearly assigned and established for both the response to a disaster occurring and maintenance of the existing plans;
- Invocation responsibility is clearly defined;
- Plans cover an appropriate variety of scenarios;
- Annual test exercises are carried out based on a variety of detailed scenarios and a further test is planned for November 2013; and
- A process for reporting incidents and near misses to senior management is in place.

### Areas for further improvement

- 5.3 We identified one area where there is scope for further improvement in the control environment. The matter arising has been discussed with management. The recommendation has been, or is being, addressed as detailed in the management action plan (Section 6 below).
- 5.4 As part of discussions over risk management at the Audit Committee, there has been considerable debate around the relative risk scoring after mitigating for various BCP individual risks as well as discussion over consolidating the individual risks into one overall BCP related risk. At the Audit Committee on 26 September 2013, Management presented additional detail in respect of the current status of Top risks including a number related to BCP.

6. ACTION PLAN

	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
6.1	<p><i>Observation:</i> The Business Continuity Plan is centrally controlled and managed by the Head of Business Process Improvement but is distributed as a paper document to 52 different people or locations.</p> <p>This makes it possible for uncontrolled documentation that may be outdated to still be held. Anecdotal evidence suggests that this has been the case on a number of occasions.</p> <p>There would be benefits with using an alternative method for managing how the plan is accessed such as improved version control and distribution. Potential alternatives include managing access via a central storage point i.e. secure internet or intranet location, cloud-based service or distributed by secure USB device.</p> <p><i>Risk:</i> Plans may lack effective version control which may cause people to refer to old or outdated version of the Business Continuity Plan causing delays in recovery.</p>	<p>HCPC should consider alternative methods of version control and distribution for the BCP, i.e. via secure internet/intranet, cloud service or secure USB key.</p>	3	<p>The Executive consider technology based solutions for the update and distribution of the BCP every year as part of the project prioritisation process and budget discussions. To date other statutory requirements have reached a higher priority than this project.</p> <p>This item remains on the long list of important projects until actioned.</p> <p>This project will be considered again in the project prioritisation process and budget discussions taking place in December and February for the forthcoming (2014/15) budget year.</p>	Dec 2013 / Feb 2014



## Appendix 1 – Definitions of Assurance Levels and Recommendations

We use the following levels of assurance and recommendations in our audit reports:

Assurance Level	Adequacy of system design	Effectiveness of operating controls
Substantial Assurance:	While a basically sound system of control exists, there is some scope for improvement.	While controls are generally operating effectively, there is some scope for improvement.
Adequate Assurance:	While a generally sound system of control exists, there are weaknesses which put some of the system objectives at risk.	While controls are generally operating effectively, there are weaknesses which put some of the system objectives at risk.
Limited Assurance:	Control is generally weak leaving the system open to significant error or abuse.	Control is generally weak leaving the system open to significant error or abuse.

Recommendation Grading	Definition
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose, HCPC to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose, HCPC to a moderate degree of unnecessary risk.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.