Audit Committee, 9 October 2014

Internal audit report – ICT Disaster Recovery NetRegulate System

Executive summary and recommendations

Introduction

Mazars have undertaken a review of the HCPC's arrangements for DR processes in relation to the NetRegulate system.

Decision

The Audit Committee is asked to discuss the report

Resource implications

None

Financial implications

This audit was undertaken as part of the internal audit plan for 2013-14. Mazars' annual fee is £27,000.

Appendices

Internal Audit Report – ICT – Disaster Recovery NetRegulate System

Date of paper

1 October 2014

Internal Audit Report

ICT – Disaster Recovery (DR)
NetRegulate System (01.14/15)

September 2014

FINAL REPORT

MAZARS

CONTENTS

AUDIT CONTROL SCHEDULE:

Client contacts	Guy Gaskins: Head of IT Jason Roth: Infrastructure Support Manager	**Internal Audit Team**	Graeme Clarke: Director James Sherrett: Assistant Manager Neil Belton: IT Audit Manager
Finish on Site \ Exit Meeting:	31 July 2014	**Management responses received:**	29 September 2014
Draft report issued:	11 August 2014	**Final report issued:**	29 September 2014

In the event of any questions arising from this report please contact James Sherrett, Mazars LLP james.sherrett@mazars.co.uk or Graeme Clarke, Mazars LLP graeme.clarke@mazars.co.uk

1. INTRODUCTION

1.1 As part of the Internal Audit Plan for 2014/15, we have undertaken a review of the Health and Care Professions Council's (HCPC) DR processes in relation to the NetRegulate system. The audit was included in the Plan owing to the number of risks identified in HCPC's Risk Register relating to DR and the importance of this system to the business.

1.2 During 2013/14, we undertook a review of HCPC's overall Disaster Recovery and business continuity arrangements and provided a 'Substantial' assurance with one Priority 3 recommendation made regarding to version control of the BCP. The status of this recommendation was recently reviewed as part of our Follow Up review; the results of which are reported separately.

1.3 We are grateful to the Director of IT, Infrastructure Support Manager and their 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 HCPC currently regulates 16 health and care professions. These include: Arts therapists, biomedical scientists, chiropodists/podiatrists, clinical scientists, dieticians, hearing aid dispensers, occupational therapists, operating department practitioners, orthoptists, paramedics, physiotherapists, practitioner psychologists, prosthetists/orthotists, radiographers, social workers in England, speech and language therapists.

2.2 NetRegulate is a dedicated system originally supplied by a third party, Digital Steps, now known as Energysys, which allows HCPC to manage its register of health and care professionals. The system allows registrants to update their own records either via the phone to the HCPC or through the internet via the HCPC web portal accessible via the HCPC website.

2.3 As a key business system it is important that in the event of an IT disaster HCPC has appropriate arrangements to ensure that NetRegulate can return to 'business as usual' in a timely, efficient and effective manner.

2.4 The live application and database is hosted on site at the HCPC offices with redundant replication to a backup database hosted by Rackspace at a remote Datacentre. The web connectivity and security environment is also hosted by Rackspace through industry standard IIS Web server devices. To maintain the service there is also redundant internet connectivity between HCPC and Rackspace.

3. SCOPE AND OBJECTIVES OF THE AUDIT

3.1 Our audit considered the following risks relating to the area under review:

- Malicious damage from unauthorised access *(HCPC Risk Register, June 2014, Ref 5.5)*; and

- Protracted service outage following a NetRegulate Registration system failure *(HCPC Risk Register, June 2014, Ref 10.2).*

3.2 The focus of our work was on the NetRegulate and Online Renewals systems. There was no specific coverage of the Education database as this is subject to internal review as part of an internal project within HCPC.

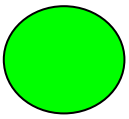
3.3 In reviewing the above risks, our audit considered the following areas:

- Back-up and recovery arrangements for the Net Regulate Registration system;
- IT Disaster Recovery Plans;
- Periodic testing, review and updating of IT Disaster Recovery Plans to ensure that they are effective, workable and current;
- Assignment of responsibilities forming part of Plans for dealing with disasters and communication of respective roles and responsibilities of individuals;
- Back up Strategy;
- Review of back up processes to include assessment of adequacy for HCPC's needs; and
- Restorations resulting from incidents and testing undertaken.

3.4 The objectives of our audit were to evaluate the adequacy of controls and processes for DR of the NetRegulate system 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.

3.5 We are only able to provide an overall assessment on those aspects of the controls and processes for DR of the NetRegulate system 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	
	**Substantial Assurance**

Recommendations summary	
Priority	**No. of recommendations**
1 (Fundamental)	None
2 (Significant)	1
3 (Housekeeping)	None
Total	**1**

Risk management
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 of the NetRegulate system. 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 largely operating effectively with the exception of the issue identified in the Action Plan in Section 6 below.

Value for money
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 also vital due to the importance of maintaining core business services. HCPC is benefiting from the establishment of a business continuity framework, supported by effective and tested recovery plans covering the range of the organisation's operations. No specific value for money issues were highlighted in our review.

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 5.3 below, in our opinion the DR arrangements for the NetRegulate system, 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 NetRegulate Backup and Recovery Strategy;
- NetRegulate is hosted onsite but replicated offsite to provide redundancy and recovery measures. Failover procedures between the two sites have been implemented and tested;
- The system and database is also backed-up to tape on a daily basis and recovery from tape is regularly tested;
- Web services have been subject to penetration testing and no outstanding issues were identified with access or security;
- There are two factor authentications through registration number and separate access codes required for the user to access and amend their data;
- Any changes made to a user's information are subsequently emailed to the user's registered email account for confirmation;
- Data changes are logged and periodically reviewed for anything unusual. The logs can also be used reactively should an unauthorised data change be reported;
- Test restorations of the database from either tape or standby facilities are made to the test system on a regular basis; and
- The system code is held in Escrow to limit the impact of Energysys removing support for NetRegulate. It should be noted that Energysys no longer promotes NetRegulate and HCPC is its only user.

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).

6. ACTION PLAN

	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
6.1	*Observation:* On the day of our audit review we requested evidence that the live replication of the NetRegulate database from the main site at HCPC to the standby site at Rackspace was operating as expected. On investigation it was identified that the live replication had not worked for a period of around 5 days. Whilst this does not mean that the system was without backup, it does mean that the frontline method, for both continued operation in the event of a disaster and the prime recovery method, were not operating. The lack of reporting of a failure around this service was noticeable. Tape backups of the database remained operational and available which would provide restoration of services which should limit any data loss to a maximum of 24 hours. It should also be noted that subsequent to our visit the live replication is now working again. *Risk:* Primary recovery and continued service are not available or working as expected.	HCPC should ensure that alerts that warn the ICT Team when backups fail are established.	2	The technical team are working with the technical support team at Oracle to create a mechanism for effective alerting from the synchronisation software. The technical implementation is now in the user acceptance test system for validation and a formal change request is being written to promote it to the production environment as soon as the tests are completed successfully. In the interim the synchronisation manager console is being manually checked daily to affirm continued protection. The change is expected to be made into the production environment by December 2014.	December 2014 Director of IT

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.