Audit Committee Meeting 15 March 2017

Business Continuity test using Shadow Planner / Plan in Your Pocket.

Executive summary and recommendations

Introduction

HCPC carried out its annual Business Continuity test in November 2016

Rather than use the traditional red folder DR / plans, most EMT members used the Shadow Planner / Plan in Your Pocket app on Samsung smartphones.

A high level over view of the scenario is provided in the report. Suggestion on how to improve use of ShadowPlanner are included in the report.

Decision

The Audit Committee is asked to discuss the report, in Appendix 1.

Background information

None

Resource implications

None known

Financial implications

None known

Appendices

Appendix 1 Business Continuity test report

Date of paper

22 February 2017

Internal Audit

1. Audit overview

1.1	Audit Date or Incident Date	11/11/2016
	Auditor	Kayleigh Birtwistle / Roy Dunn (James Wilson & Emily Watkins, observers) Jamie Hunt, mock tabloid journalist.
	Last audited date	16/10/2015
	Date report was issued	23/12/2016
	Internal Audit ISO9001	☒
	Internal Audit ISO27001	☒
	Internal Audit ISO10002	☐
	Department	All departments- Business Continuity plans
	Processes or tasks being audited	Use of Shadow-Planner / Plan in Your Pocket App
	Process owner	Greg Ross-Sampson (Dir of Ops)
	People audited	All of EMT, + Office Services Mgr
1.2	Reason or aims of audit - Summary	Test use of Plan in Your Pocket by EMT under DR conditions
1.14	Nonconformities issued	0 (Quantity)
1.15	Observations made	0 (Quantity)
1.16	Signature and date of person being audited and in receipt of report including non-conformities	Signature:_____ Date:_____

1. Summary of Audit

The Business Continuity / Disaster Recovery plan is tested on an annual basis. The BPI dept maintain the plan, and develop scenarios to test the response of EMT and or CDT, or individual departments to potential events. Some business continuity expertise is retained within the department, by virtue of ISO27001, ISO9001 and the Risk Management function. The tests do not always include a switch over to BCM/DR servers due to the excessive time required to roll back and redo work.

2. Previous audit areas / subjects for resolution

Previous actions around Business Continuity / Disaster Recovery were based around adopting a mechanism to update the plans on a more reliable basis, rather than relying on sealed envelopes, passed to the relevant parties on a monthly basis. This has been completed with the roll out of Shadow Planner / Plan in Your Pocket App.

2. Opportunities for improvement, observations and nonconformities

Seven Opportunities for Improvement were highlighted.

1. Plans should be reviewed to ensure new systems, functionality and access models are accommodated.
2. Determine if the current estate of three buildings allows for greater resilience.
3. Maintain a synchronised paper / pdf version of the plan for ease of use.

4. Determine how EMT and CDT level employees can be trained to maintain the plans for their departments.
5. Determine if any additional personal information should be stored on the service to allow for no internet scenarios, whilst being aware of any potential for increased risk of information loss.
6. Re-drill the EMT on a more regular scenario once updates to the plans have been made, and familiarity with Shadow Planner / Plan In Your Pocket have been established.
7. Offer DR/BCM tests to departments, to allow them to practice with Shadow Planner functionality. Registration have already volunteered.

4. Non-conformity, Observations or Opportunities for Improvement action plan					
Recommendation	**Findings**	**Detailed Recommendation**	**Management Response**	**EMT Decision**	**Decision & Implementation Date**
1	The plans last had a major update in 2013, and a refresh of the information is advisable, in light of the plan material being available on new media.	Departments to evaluate their plans on "Plan in your Pocket" and determine what updates they would like to make.		**Depts to supply updates by Oct 2017**	
2	Determine if core functions could share available space and resources in emergency.	EMT to determine what resilience opportunities are available from use of three buildings (184 & 186 Kennington Park Rd; 33 Stannary St; 405 Kennington Rd). Plans to be updated accordingly.	**Leave plan as single site, but adjust the lead sheets to consider moving people around the buildings that are still available**		
3	Noting actions against the plan is easier on paper.	Some members of EMT would like to retain a printable version of the plan, as a file on their smartphones, for emergency printing if print functionality from Shadow Planner website is not available.	BPI – a pdf of the plan will be produced, and made available to plan users. This can be stored on secured devices.	**Have a paper copy available for MJS at Opening meeting**	

4	Content is to be mostly maintained by individual departments.	EMT & Heads of / CDT members to be trained on the updating of Shadow Planner on line.	BPI will arrange training for required users, probably around a Monthly EMT.		
5	Full employee, partner details are not available without web access to Core HR system.	Determine if additional information should be added to Shadow Planner / Plan In Your Pocket, or scenario is so unlikely additional mitigation is not required.	It is possible to update the template to include extra information, but this adds an additional (low) risk of information loss, via mobile device or make no changes?	Should additional next of kin etc info be included in Shadow Planner? NO	
6	Provide additional training to EMT ta ease familiarity with the Shadow Planner / Plan in Your Pocket app.	Re-drill the EMT on a more regular scenario once updates to the plans have been made, and familiarity with Shadow Planner / Plan In Your Pocket have been established	Training / Introduction to ShadowPlanner EMT/CDT/Hd's of etc	Introduction to ShadowPlanner before 1st Oct 2017	
7	Provide departmental opportunities for testing of the Shadow Planner / Plan in Your Pocket app.	Offer DR/BCM tests to departments, to allow them to practice with Shadow Planner functionality. Registration have already volunteered.	Registration dept test scheduled February 1st 2017	Before Nov 2018	

5. Glossary

Frequently used internal audit terms;

QMS	Quality Management System
QM	Quality Manager
QCA	Quality Compliance Auditor
ISMS	Information Security Management System
ISO9001	Quality Management Standard
ISO10002	Quality Management, Complaints Management Standard
ISO27001	Information Security Standard
ISO27002	Set of published standard controls for Information Security

6. Root cause analysis

ROOT CAUSE AT HCPC	**ROOT CAUSE WITH APPL / REG**	**NOT ASSIGNABLE**		HCPC - Human Error, requires training	HCPC-Equipment or software failure	HCPC-Lack of resources	HCPC-Supplier error	HCPC-Process failure, or lack of complete process	Other

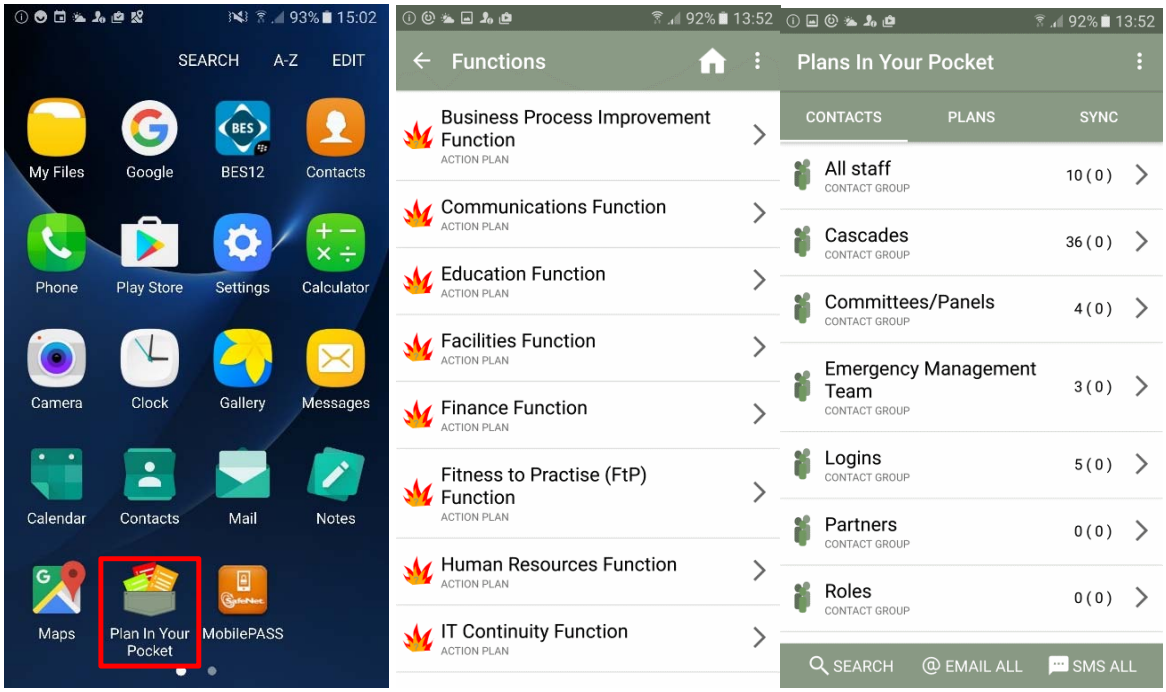
A1. Audit reason

This audit forms part of the annual cycle of internal audits, and follows a risk based approach. Key departmental business continuity plans are now available on a mobile devices (smartphone) platform. Use of the smartphone plan were tested against an impossible to immediately recover scenario over a morning BCM/DR test off site.

A2. Reference documents and data sources used in operational activity

Shadow Planner online Business Continuity system – provides content to the mobile app.

“Plan In Your Pocket” mobile app (Shadow Planner content on smartphones). Partial drill downs into functions for each dept to carry out, and PII required to contact employees and long term contractors, or Council Members.



A3. Risk Register for audit area

Category	ISMS Risk	Ref	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016
Information Security	I A6,8,9 12,14	17.1	Loss of information from HCPC's electronic databases due to inappropriate removal by an employee	EMT, Director of IT and Director of Operations	5	3	15	Access is restricted to only the data that is necessary for the performance of the services. Employment contract includes Data Protection and Confidentiality Agreement	Adequate access control procedures maintained. System audit trails. Training where appropriate.	Laptop encryption. Remote access to our infrastructure using a VPN . Documented file encryption procedure . Maintain ISO27001	Low
			Links to 5.3. Incl old 17.6								
Information Security	I A11,8, 7,15,16, 17	17.2	HCPC Document & Paper record Data Security	EMT; Head of Business Improvement	5	3	15	Use of locked document destruction bins in each dept. Use of shredder machines for confidential record destruction in some depts e.g. Finance.	Data Protection agreements signed by the relevant suppliers. Dept files stored onsite in locked cabinets. Training where appropriate (Employees & Partners)	Regarding Reg Appln forms processing, employment contract includes Data Protection Agreement	Low
			Links to 15.7								
Information Security	I A15, 8, 13	17.3	Unintended release of electronic or paper based information by external service providers.	EMT, Director of IT and Director of Operations	5	3	15	Access is restricted to only the data that is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data Processor agreements signed by the relevant suppliers. Maintain ISO27001	Low
Information Security	I A18, 15, 13	17.4	Inappropriate data received by HCPC from third parties	Director of Ops, and Director of FTP	5	2	10	Read only, password protected access by a restricted no of FTP employees to electronic KN data.	Registrant payments taken in compliance with Payment Card Industry (PCI) Security standards ie with quarterly PCI testing.	Ensure third party data providers e.g. professional bodies provide the data password protected/encrypted/door to door courier/registered mail/sign in sign out as appropriate.	Low
Information Security	I A15, 8	17.5	Loss of physical data dispatched to and held by third parties for the delivery of their services	Director of Ops and Hd of Business Process Improv	5	3	15	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Use of transit cases for archive boxes sent for scanning or copying and sign out procedures.	-	Low
Information Security	I A9, 12, 13, 15	17.6	Loss of Registrant personal data by the registration system (NetRegulate) application support provider in the performance of their support services (specific risk).	Director of IT and Director of Operations.	5	3	15	Access to and export of personal data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data processor side letter specifying obligations and granting a limited indemnity.	Low
Information Security	I A8	17.7	Incorrect risk assessment of Information Assets	Hd of Business Process Improv & Asset Owners	4	2	8	Identification and collection of information risk assets	Regular audit and review of information risk assets by Hd of BPI	Regular identification and review of information risk assets by Hd of BPI	Low
Information Security	I A6, 7, 8, 9	17.8	Loss of personal data by an HCPC Contractor, Partner, Council or Committee member.	EMT	5	3	15	Access to and export of personal data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods. Training where appropriate.	Maintain ISO27001	Low
Information Security	I A5	17.9	Loss of ISO 27001:2013 Certification	Hd of Business Process Improv & Asset Owners	5	4	20	Culture, follow procedures, report errors, training and awareness as required	Standard Operating Procedures and prevention of overwriting systems	Extend ISO systems as required	Med
Fitness to Practise		13.8	Backlog of FTP cases	FTP Director	3	4	12	Reforecasting budget processes	Monthly management reporting	Quality of operational processes	Low
			13.2 moved to 12.2								
Fitness to Practise	I A12,13, 14, 16, 17	13.10	Protracted service outage following a Case Management System failure	Director of IT	5	3	15	Effective backup and recovery procedures	Maintenance and support contracts for core system elements	Annual IT continuity tests	Low

Operations	I A11, 17.2.1	2.1	Inability to occupy premises or use interior equipment	Office Services Mgr	4	4	16	Invoke Disaster Recovery/Business Continuity plan	Commercial combined insurance cover (fire, contents, terrorism etc)	-	Low
Operations		2.3	Unacceptable service standards	Director of Operations	5	4	20	ISO 9001 Registration, process maps, well documented procedures & BSI audits	Hire temporary employees to clear service backlogs	Detailed workforce plan to match workload.	Low
			Links to 9.1, 10.4								
Operations	I A11	2.6	Inability to accommodate HCPC employees	Office Services Mgr	4	3	12	Ongoing Space planning	Additional premises purchase or rented	-	Low
			Links to 5.2								
Operations		2.14 (formerly11.5)	Health & Safety of employees	Chief Executive & Office Services Mgr	5	4	20	Health & Safety Training, policies and procedures	H&S Assessments	Personal Injury & Travel insurance	Low
			Links to 4.9, 6.3								
Communications		3.3	Inability to inform stakeholders following crisis	Director of Comms	4	1	4	Invoke Business Continuity Plan (BCP)	Up to date Comms BCP available	-	Low
Communications		3.4	Failure to inform Registrants Article 3 (13)	Director of Comms	5	1	5	Delivery of communications strategy	Delivery of aspects of communications workplan, specifically, Meet the HCPC events, campaigns, Registrant Newsletter, Profesional media and conference attendance . Publications and web.	Quality of Operational procedures	Low
IT	I A17, 14,12	5.4	Failure of IT Continuity Provision	Director of IT	4	3	12	Annual IT continuity tests	IT continuity plan is reviewed when a service changes or a new service is added	Appropriate and proportionate technical solutions are employed. IT technical staff appropriately trained.	Low
IT	I A11.2.2 A17.1.2	5.6	Data service disruption (via utility action)	Director of IT	5	1	5	Redundant services	Diverse routing of services where possible	Appropriate service levels with utility providers and IT continuity plan	Low
Education	I A12,13,1 415	7.5	**Protracted service outage following Education system failure**	Director of IT	4	2	8	Effective backup and recovery processes	In house and third party skills to support system	Included in future DR/BC tests	Low
Registration		10.2	Protracted service outage following a NetRegulate Registration system failure	Director of IT	5	3	15	Effective backup and recovery procedures	Maintenance and support contracts for core system elements.	Annual IT Continuity tests	Low
			Links to 5.1-5.3 and 17.1								
Registration		10.4	Backlogs of registration and applications	Director of Operations, Head of Registration	4	3	12	Continually refine model of accurate demand-forecasting, to predict employees required to prevent backlogs, and service failures	Process streamlining	Match resource levels to meet demand & delivery published Service Standards	Low
			Links to 1.1								

A4. Audit areas – evidence and narrative

Location: Southwark Cathedral
Date / time: 14 November 2016, 10am-12pm
Attendees: Marc Seale (MS), Guy Gaskins (GG), Kelly Holder (KH), Abigail Gorringe (AbG), Michael Guthrie (MG), Greg Ross-Sampson (GRS), Andy Gillies (AnG), Jacqueline Ladds (JL), Theresa Haskins (TH), James McMahon (JM), Roy Dunn (RD), Kayleigh Birtwistle (KB), Emily Watkins (EW), James Wilson (JW),

The scenario will not be recorded in detail as it is a viable terrorist scenario that could easily be used in live conditions.

The “terrorist activity” resulted in total loss of internet and landline connectivity within the M25 area.

Full restoration of internet and telephony services is estimated to take several months, as the expertise to connect up all of the replaced hardware is limited. Mobile communications channels will be severely overloaded in the meantime, and may be subject to periodic failure themselves.

RD, ran through the start of the scenario to get EMT up to speed on the developing theoretical situation. This listed some known events, some theoretical implications of those events, and possible reactions made as the scenario rolled out in the first few hours. This is summarized in the list Situation overview below.

Situation overview

- NetRegulate Online Register not accessible using HCPC hardware
- Not able to update remote NetRegulate implementation from Park House
- Not able to answer or make telephone calls via “landlines”
- Congested mobile networks very slow or unresponsive as all phone and web traffic goes via mobile data infrastructure. Priority given to Tier 1 responders.
- Cannot easily update www.hcpc-uk.org to inform stakeholders of issue
- Cannot easily update employees, Partners, Witnesses, Registrants and legal representatives if Hearings being cancelled or postponed in London
- Cannot replicate / back up data easily as link is down. Back up to tape and disk still possible
- Office 365, email, etc not available via PC, using HCPC network
- FTP CMS still theoretically available on site
- Core HR system not accessible from Park House (and no local copy of information)
- Cannot easily pay employees or Partners and Members
- EDU system still theoretically available on site

The time was about 8.30am, some EMT’s members were in the office, some on their way in, some stuck in transit, and some diverted to the DR site. EMT were required to work out what to do, and where to do it, as the scenario developed. Communication between EMT members would be difficult in the real version of this scenario playing out.

The EMT, commenced following the Day 1 Action Plan as listed in Shadow-Planner / Plan In Your Pocket. The Chief Executive followed the plan on paper from a “Red folder” version and a Shadow-Planner pdf version of the plan. MS tracked the response to the scenario as each piece of information was delivered. There is a slight discrepancy on the layout of the paper plan to the online version, as the Shadow planner database is limited to 256 characters per field. The Shadow Planner version tends to be broken down more. It is also designed to fit on portrait A4 and on mobile devices rather than landscape A3 as paper.

EMT determined if those in the office already, should be evacuated or it was more likely to be safe for them to remain in the office. [Decision = Employees on site should stay for now]

As the scenario had to fit in with various HCPC practices, a list of issues were provided for EMT, who split up into small virtual teams, Comms & HR Directors, Some were deemed in transit and out of contact, others still at home waiting to see how the situation developed.

hcpc health & care professions council

Do we open the Park House and 405 buildings?

If not, what will you do?

Record your decisions and actions.

Will you be able to make the call, send the email or the SMS?

Throw a prime number greater than 40 to get the connection, wait 7 minutes to try again if you get an odd number.

Decision - Office Services:
Keep Park House open at reduced hours (10am-4pm), close 405 etc, as there are no threats to the site.

hcpc health & care professions council

It is Friday 13th, payroll is about to go to Core Payroll bureau

Who is responsible?

What do you do to make sure everyone gets paid?;

List the practical steps, authorisations required etc to ensure this happens.

Do you have access to the information that you need?
Show the test team where the information is.
Record your decisions and actions.

Will you be able to make the call, send the email or the SMS?

Throw a prime number to get the connection, wait 7 minutes to try again if you get an odd number. Throw a prime number below 20 to gain Tier 1 access for a single smartphone.

Decision - Payroll run:
As access to the web hosted data was not possible, the most pragmatic solution is to rerun the previous months pay run, and sort out any discrepancies manually as communications improved. It would be necessary to email and or speak to the provider of the service. AG managed to throw a prime number combination under 20!

hcpc health & care professions council

End of the Renewal cycle at the end of the month

Online renewal will not work in the short term

Online renewals may work for some registrants outside London, if the NetRegulate infrastructure can be entirely switched over to our ISP / hosting environment Rackspace

How will you organise the appropriate technical changes?

What do you do for those not renewing online?

Record your decisions and actions.

Will you be able to make the call, send the email or the SMS?

Throw a number under 19 to get the connection, wait 7 minutes to try again if you get an odd number.

Decision - End of renewal cycle:
GRS would do nothing, waiting until the following day to make a decision on any action required (such as extending renewal deadline, making allowances for those who come off the register, etc) as online renewals would still work for registrants outside of London.

hcpc health & care professions council

Policy & Standards and Communications

Whilst no one is initially going to die if the HCPC registers are not available on line, not having a response plan would be seen as incompetent.

What do we do first to maintain public confidence whilst the register is unavailable (much of the internet is unavailable)?

How do we communicate with the public?

Record your decisions and actions.

Will you be able to make the call, send the email or the SMS?

Throw an even number to get the connection, wait 7 minutes to try again if you get an odd number.

As the website was not accessible / available from London, the Communications department were required to arrange for an internet proficient employee to travel outside the area of the connectivity issue to establish a stream of information for those outside London.

Decision - Business vs. Crisis Management

It was suggested that a decision should be made as to who would be running the crisis management, and who would be running the business (if all of EMT is in crisis management, who is running the business?). Discussion took place of appointing people to manage crisis and people to manage business on the basis of who was present and available, and their skills and capabilities.

A "journalist" from a major tabloid appeared on site with EMT to ask questions about the activities of fake Paramedics during the terrorist scenario. The questions were designed to trip up EMT, and were unreasonable in their direction.

OBSERVATIONS:

- The paper version of the plan was slightly different to the phone app version that was being used by most of the EMT, causing some confusion (there is a limit on the numbers of characters that can be displayed in any one panel = 256)
- A suggestion was made that paper and phone versions of the plan should be available in the event that phones are not accessible or useable.
- It was noted that the phone chargers in the 'war box' at Uxbridge may need to be replaced for the new work phones. Blackberry chargers seem to be compatible.
- A suggestion was made that a television should be mounted in Room N, as this would be where the EMT is likely to meet in the event of a disaster
- JL noted that the communications plan and checklists needed updating

A5. ISO 27001 audits Information Assets used

HCPC's Business Continuity / Disaster Recovery plan as replicated on Plan In Your Pocket / Shadow Planner.

Appendix 1 Recent news stories around fake Paramedics

http://www.dailymail.co.uk/health/article-3394706/Worrying-rise-fake-paramedics-patients-danger.html

https://www.thesun.co.uk/news/1345728/deluded-man-was-caught-impersonating-a-paramedic-wearing-high-viz-jacket-and-carrying-a-bogus-medical-kit-with-three-knives/

http://www.bbc.co.uk/news/uk-wales-32828441

http://www.mirror.co.uk/news/uk-news/fake-paramedic-caught-after-ambulance-4002882

Appendix 2 HCPC Intranet report on the BCM test.

EMT's disaster recovery training

Thursday, 24 November 2016
EMT recently held a 'disaster recovery' training session – essentially planning how HCPC runs in the event of a disaster, for example when we've been flooded in recent years. It's vital that even when a disaster strikes, we remain operational for our registrants.

The session was run by the Business Process Improvement team, Roy Dunn and Kayleigh Birtwistle. We developed a disaster scenario based on real life events that have happened in the last 15 years, all cobbled together to make a very difficult situation, to test our response plans.

EMT had our new 'Plan In Your Pocket' app on their phones to try out. The app is a new electronic form of our Business Continuity Plan, instead of the large red disaster recovery (DR) folder with print outs. The Business Continuity Plan is the plan we have in place to keep the business operational in the event of a disaster. It details what the organisation must consider when reacting to any event that may disrupt business on a day to day or longer basis. Various decisions are listed in the plan indicating fairly obvious ways to react; for instance "Do we stay or do we go", is to consider if the HCPC buildings are useable and safe, or do we need to relocate to our back-up site in Uxbridge? The plan also lists what individual departments must do to maintain basic levels of service if at all possible.

In the past, I have drip fed information into EMT to see how they react to ever changing information, sometimes changing the slant of the test part way through. This year, an element of chance was introduced whereby EMT could get different outcomes to their reactions to the test based on their ability to throw combinations of numbers from 20 sided gaming dice. If you don't get the numbers you require to carry out your required action, pass the dice on to the next person, and wait 7 minutes before you can try again.

James Wilson and Emily Watkins from the Registration team, acted as observers, as it is often impossible to keep track of all the decisions and run the scenario simultaneously – there is just too much going on, and often multiple conversations around what to do are occurring, and Jamie Hunt attended part way through the test as an unreasonable reporter from a newspaper.

Some of you will have seen this new application 'Plan In Your Pocket' on your HCPC Samsung smartphone.

Access will gradually be rolled out to those requiring the application, instead of the red Disaster Recovery plan folder.

CDT will be run through a similar exercise next year.

PDF versions of the plan will be produced for off-line printing as required.

A report will be produced for EMT and Audit Committee over the next month.

Department: Business Process Improvement
Group: Executive Management Team

Appendix 3 To emulate the difficulties that would be in place under this scenario EMT members were asked to throw particular combinations of numbers with the gaming dice. The call or email could only be sent if they threw the required numbers.

To gain access to mobile or networked connectivity, EMT members were required to throw combinations of numbers from 5, 20 sided gaming dice. Failure to score the correct range of digits required waiting 7 minutes before making a further attempt. This was designed to emulate the random nature of being able to make a telephone call, send a text or email whilst the communications infrastructure in London was greatly degraded.

Appendix 4 Front / Cover page of HCPC's Business Continuity Plan pdf, direct from Shadow- Planner

hcpc health & care professions council

Business Continuity Plan

Department All
Office All
Generated 11-11-2016
Version 1

This package contains a copy of the current Business Continuity Plan for the Health & Care Professions Council.

This must only be opened if you are contacted by the HCPC Business Continuity Team.

This contains confidential employee information and is thus subject to the Data Protection Act.

When this version is amended you will automatically be sent an updated version. Please return old copies to HCPC.