Finance & Resources Committee 31st July 2008

Business Continuity Management – lessons learned from May 28th exercise

Executive summary and recommendations

Introduction

On the 28th of May 2008 part of HPC took part in a simple Disaster Recovery exercise, to test existing mechanisms that are in place to assist our response to unforeseen events. This included establishing remote access to replicated IT systems for the whole organisation.

HPC will continue to build capacity and flexibility in this area.

For the sake of brevity the report uses expanded bullet points wherever possible.

Decision

The Committee is requested to note the document. No decision is required.

Background information

HPC has an ongoing Disaster Recovery / Business Continuity plan, that is updated on a regular basis. Small tests of individual system restorations have taken place in the past. A company wide test has taken place for the first time.

Resource implications: None

Financial implications: None known at present

Appendices: None

Date of paper 21st July 2008

Business Continuity Lessons learned

Content

The scenario

On the morning of May 28th the EA building burned, damaging the HPC building and preventing access…how would HPC cope?

- On May 28th Marc Seale, Chief Executive & Registrar and Roy Dunn, Head of Business Process Improvement, intercepted members of EMT as they entered Park House and informed them that an exercise of the Disaster Recovery / Business Continuity plan was underway.
- The exercise scenario was that an adjacent building had been destroyed in a fire outside normal business hours 8 am – 6 pm and that HPC premises were damaged and not available. Two early start HPC employees were not accounted for.
- EMT members were not allowed to go to their desks, but only allowed to employ the resources they had immediately to hand.

HPC employees and Council members taking part or observing

Employee, Contractor or Council member	Business Area
Marc Seale	CER
Greg Ross-Sampson	OPS
Simon Leicester	Fin
Larissa Foster	HR
Guy Gaskins	IT
Niamh O’Sullivan	Sec
Tyrone Goulbourne	IT
Manj Cheema	Fin
Shellagh Gillick	Fin
Ebony Gayle	Comms
Cherise Evans	Journalist
Anna van der Gaag	President / Cnl Mbr

Neil Willis	Cnl Mbr (F&R Comm)
Tony Hazel	Cnl Mbr (Audit Comm)
Jonathan Bracken	Parliamentary Agent
Tony Glazier	Remote Web site updates
Roy Dunn	BCM Observer only

Analysis of the response took place based on detail captured as the event took place. All of these recommendations are summarized over the rest of the paper.

1- Modifications to the plan as a result of the exercise

- The sequence of IT system restoration will be reviewed, with restoration of the HRInfo system taking priority. This will enable HR to contact employees next of kin more easily if required.
- Loading the NetRegulate registration data to allow the on-line register to function can occur concurrently with other systems restoration. This is carried out by a third party in most instances.
- The readability of the paper plan was a concern. The overview table was skipped and the detailed response was followed. Instructions need to be more implicit.
- Using the overview document may have enabled the Incident Management Team (IMT) to split up and cover more activities more efficiently.
- More detail is required about how to select which part of the plan must be used in different situations, or under different scenarios. A simple flow diagram will be considered for this – but this will not be easy to design.
- The remote editing of the HPC website requires an additional back up should the web master and Reading Room website designers (current fall back) be unavailable.
- Determine a list of essential supplier phone numbers and email addresses to be loaded onto IMT members mobile phones. (in progress)
- Modify the content in the Communications plan for internal and external use.
- Encourage IMT members to think of non-obvious solutions
- Determine if further IT systems are essential for HPC DR operations, their position in the order of restoration, and any situations where that system may not be required.
    - These systems include;
        - ALBACS system for collecting direct debits
        - Call recording system,
        - ICR scanning and processing of renewals
        - Blackberry server for additional communication mechanism.
        - Reporting database – registrations reports
        - HPC's web server for www.hpc-uk.org. This server is physically located in a Docklands data centre, is backed up there and replacement hardware components stored. Do we need to enable additional capacity for restoration ourselves?

2- Improvement to response

- Members of EMT did not have copies of the DR Plan with them as they came into the building – and they are not required to carry such a bulky item with them. It also contains confidential employee and Council member information.
- When the new version of the plan is rolled out, a single page sheet (Incident Management Plan) will be provided with all essential details required for an immediate response.
- For the purposes of this test the decision to relocate to the NDR site in Uxbridge was made but not instigated immediately. Under real life conditions HPC would begin relocation of key Incident Management Team employees to the NDR site as soon as possible.
- Consider redirecting Incident Response team members direct to the recovery site. This is likely to happen in a real invocation by default and would save considerable time.
- There was no move to inform Fire/Police/Ambulance services that two employees were potentially missing. This may be down to the scenario not being clear about where the information concerning their status originated.
- Use of the new Incident Management Plans (IMP) listing essential contact details, with initial response information would provide sufficient instructions to commence activation of the BCM without referral to external sources of information.
- Many members of HPC have laptop computers with the VPN client enabling them to work remotely. For those that did not have their encrypted laptops with them at home standard build laptops need to be made available via the DR company, (under investigation).

3-Areas for development

- Complete the migration to the new Business Continuity plan from the previous version by 1st August 2008. This will include;
  - Incident Management Plan (A4, carried at all times within reason)
  - Business Impact Assessment across HPC – ongoing
  - HPC Business Continuity Plan response to incident pack*
  - Business Continuity Glossary of terms
  - Key documents and items to be recovered from HPC campus in a disaster recovery situation

(*Critical document to enable management of a major incident.)

- Move to a BS25999 compliant Business Continuity plan and maintenance system. – underway, due for completion December 2008
  (Note this does not indicate we are attempting to achieve BS25999 certification.)
- Follow the Gold, Silver, Bronze model deployed by the Emergency services and Military. See attached page, Explanation of new Business Continuity / Disaster Recovery Terms.
- Gold should be concerned with stakeholders and strategy, Silver should be involved in restoration, Bronze assists in restoration and catch up.
- More information has been requested to be included in the IT section of selected DR plan copies. Copies of key system passwords need to be

stored in a location that is highly secure but available. Monthly updates to the war boxes has been instigated.

- Continue developing the scenarios that we have specific planned responses to.- ongoing.
- The Suppliers System listing essential and non essential suppliers needs to be updated more regularly, and forwarded to all users of the BCM plan.
- Investigate electronic means of updating all members, whilst retaining a paper version of equal value.

4-Implications and effects of the scenario used

- With the scenario used, the decision making process was mostly limited to EMT members. This is less realistic than we would like and future exercises may include a wider spread of employees.
- The combination of EMT, MMT and Council members present may not be realistic under true invocation / non exercise conditions
- Marc Seale is frequently off site along with other EMT members being unavailable on a less frequent basis. ACE position or BCM must be able to take appropriate decisions.
- Under the Gold Silver Bronze model, Gold members would be solely involved in strategic issues including communicating with major specific stakeholders.
- Often the best people to restart operational processes and overcome the issues surrounding their restoration are those running the services day to day, as evidenced in the IT activities. Thus the Silver members would be carrying out these activities.

IT Systems restoration

Restoration of IT services took place in the following sequence from 12.00 hrs onwards.

(Note the on-line register was theoretically accessible from the website from 10.38 hrs onwards).

Time to restoration of access to update system data from within the Disaster Recovery space at NDR	Time to availability once HPC on site at NDR	Functionality	Business area
12.12 hrs	[+12 minutes elapsed time]	Basic desktop functionality; Word Processing, spreadsheets & web access	All HPC / Core requirement
12.15 hrs	[+ 15 minutes elapsed time]	G: & N: drives	All HPC access to network stored information
13.00 hrs	[+ 1 hr elapsed time]	Lotus / Domino	Web based Lotus email (Domino)
13.15 hrs	[+ 1hr 15 minutes elapsed time]	NetRegulate (LISA)	NetRegulate (LISA) access to update register
14.35 hrs	[+ 2hrs 35 minutes elapsed time]	HRInfo / PPWin	HR & Partner information
		Sage data Data restored but client required to be installed	Finance data

- This used the existing data replication technology, but a new version of the Virtual Private Network (VPN) client not tried from NDR before (but used regularly from mobile users).
- The Finance system has just migrated to the upgraded MS SQL based version in SAGE 200. The web access version had not yet been completed.
- The NetRegulate system was upgraded to new hardware and software in use at Park House. The project to install the same version at Star Gloucestershire is yet to complete. The previous version of NetRegulate is currently in use at Star.

Summary

- The exercise involved most of the EMT, some Council members and suppliers in a test of our response mechanisms. Those involved have visited the DR site, and understand the facilities we are likely to have available.
- Restoration of IT systems has been proven with the exception of those systems undergoing modification and upgrade at the time of the test. The priority for restoration will be revisited.
- Whilst the decisions made were tempered by the need to keep day to day operations running back in the live environment discussions around our freedom to react are highly beneficial. Amendments to allow suspension of Council standing orders and financial regulations were discussed. Council standing orders have since amended in line with this.
- The response highlighted the requirement to work as teams focused on individual tasks, suggesting the proposed Gold Silver Bronze model is likely to work for HPC. This is currently under discussion.

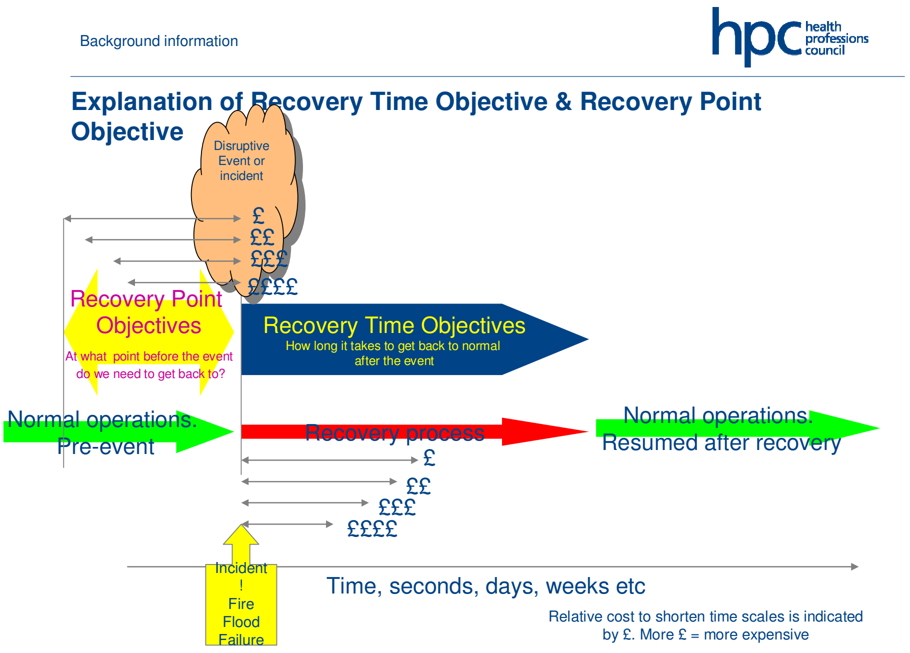
Background Information

For each of our systems and services, we determine what we are aiming for? The smaller each of these parameters is, the more costly to implement.

- Recovery Time Objectives (RTO) = How long to get back to normal?
    - Can you be down for seconds, a few minutes, an hour or two, days, weeks, months? What is the impact on the public if HPC is not working for hours, days, weeks?

- Recovery Point Objectives (RPO) = Where are you trying to get back to?
    - What point in time are you trying to get back to? End of business last night, lunch time today, a minute ago, now? How much work can we afford to loose?

Graphical explanation of Recovery Time Objective & Recovery Point Objective



Background information

Explanation of Recovery Time Objective & Recovery Point Objective

Disruptive Event or incident

£
££
£££
££££

Recovery Point Objectives

At what point before the event do we need to get back to?

Recovery Time Objectives

How long it takes to get back to normal after the event

Normal operations: Pre-event

Recovery process

Normal operations: Resumed after recovery

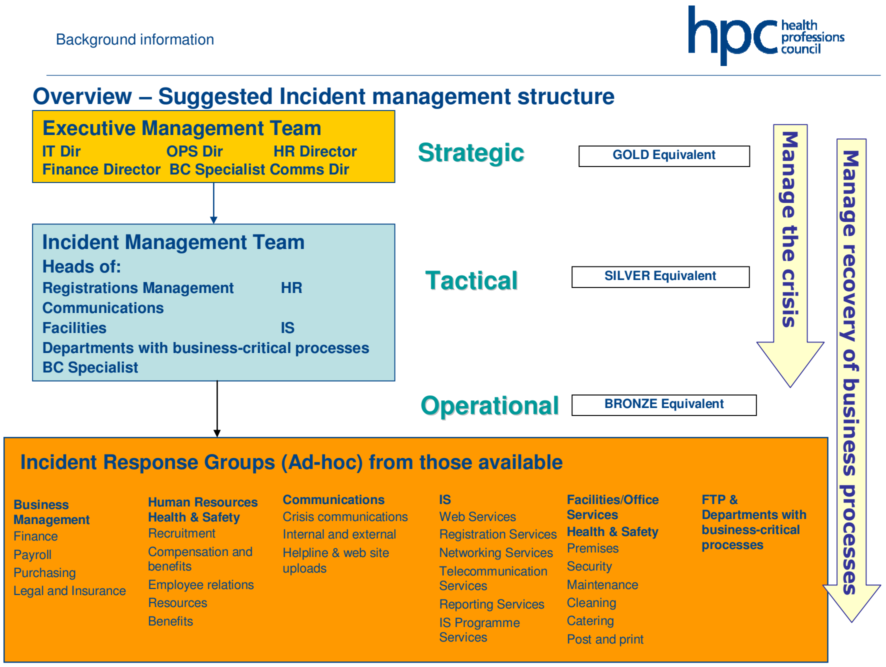
£
££
£££
££££

Incident
!
Fire
Flood
Failure

Time, seconds, days, weeks etc

Relative cost to shorten time scales is indicated by £. More £ = more expensive

Overview – Suggested Incident Management Structure



Background information

Overview – Suggested Incident management structure

Executive Management Team

IT Dir OPS Dir HR Director
Finance Director BC Specialist Comms Dir

Strategic GOLD Equivalent

Incident Management Team

Heads of:

Registrations Management HR
Communications
Facilities IS
Departments with business-critical processes
BC Specialist

Tactical SILVER Equivalent

Operational BRONZE Equivalent

Manage the crisis

Manage recovery of business processes

Incident Response Groups (Ad-hoc) from those available

Business Management
Finance
Payroll
Purchasing
Legal and Insurance

Human Resources
Health & Safety
Recruitment
Compensation and benefits
Employee relations
Resources
Benefits

Communications
Crisis communications
Internal and external
Helpline & web site uploads

IS
Web Services
Registration Services
Networking Services
Telecommunication Services
Reporting Services
IS Programme Services

Facilities/Office Services
Health & Safety
Premises
Security
Maintenance
Cleaning
Catering
Post and print

FTP & Departments with business-critical processes