1. Disaster Recovery Strategy

1.1 Summary

Disk crashes, power outages, communication loss-are all minor disasters that happen on an occassional basis - and most of us have a back-up plan ready to put into effect.

We are dependent on computers to run our business units. But rather than just looking at getting the computer system set up, we need to concentrate on how to continue the business.

There is a need to build comprehensive, effective, Disaster Recovery Plans (DRPs) to cope with major disasters (e.g. fire, flood).

1.2 Scope

This document proposes how we could record business unit contingency and IT capability, giving responsibility of local management of DRPs and at the same time providing an effective mechanism to deliver a centralised DRP in the event of disaster.

1) Proposed structure of DRPs

2) Proposed strategy to evaluate business unit contingency – objectives:

    - review products / services or critical applications
    - critically analyse and prioritise operational functions
    - review exposures for each cost center
    - establish recovery priorities
    - determine feasible recovery options
    - determine facility needs and floor space requirements

3) Proposed procedures to collate data

    - DRP Template
    - IT Inventory

4) Role of the ‘Central Emergency Disaster Recovery Group (CEDRG).

1.3 Not in Scope

As this is a framework document the following is not included:

- Information related to any contingency plans beit technical / non technical
- Suggestion for who should be members of CEDRG
- Proposal for testing DRPs or ‘structured post disaster meetings’.
- Timescales

1.4 Proposed structure of DRPs

It is proposed that each business unit be required to produce its own DRP, which will be integrated with the overall DRP managed by CEDRG. All recovery plans will need to take account of the role of the police in a disaster situation and make provision for a disaster occurring outside normal working hours. The integrated plan should ensure a swift and smooth recovery for a business unit from a disaster situation through effective co-ordination with the external emergency services and Cap Gemini's own support services.

To enable CEDRG to make a rapid assessment of a disaster situation and initiate the correct responses, each business unit DRP should be structured in the same way. The following sequence is proposed:

1.4.1 Executives:

- Work and Home telephone numbers of the persons responsible for executive decisions following a disaster. The business unit manager will be expected to liaise with CEDRG.
- Location of the business unit, together with an alternative location in the event of extensive damage to the building.

1.4.2 Staff Lists:

- lists should indicate next-of-kin and, ideally, persons to be contacted in the event of an accident, where these differ.
- identify the location of lists of persons in the business unit (in hard copy form - business unit plans to be held at an accessible point in the building and at an alternate location away from the building in which the business unit is located)
- identity of the person(s) responsible for keeping the lists updated.
- identity of the person(s) responsible for providing the police and/or CEDRG with such lists in the event of a disaster. The police take on the responsibility for notification of next-of-kin or other identified persons to be notified.

1.4.3 Damage and Salvage

- list of persons responsible for assessing the extent of the damage, once permitted back into the building and determining the business unit's needs for resumption of normal activities.
- list of persons responsible for identifying equipment which can be salvaged, its location and possible relocation.
- location of the business unit inventory (paperwork copy if the IT Log is unavailable).

1.4.4 Business unit Files

- location of back-ups of business unit computer files (ideally another building or Cap Gemini site)
- identity of person(s) responsible for updating back-ups and frequency of updating and the system for replacing former back-ups held outside the business unit.

1.4.5 Notification

- person(s) responsible for liaison with PR/Press Office (business unit representatives should not deal with the media direct).
- procedure for notification of staff at home in the event of a disaster out of hours or concerning resumption of work, if sent home following a disaster.
- checklist of organisations (suppliers, funding bodies etc) to be notified together with telephone numbers and names of persons responsible for carrying out the notification.

1.4.6 Inter-business unit Arrangements

- details of any reciprocal arrangements made with other business units for location of essential staff to initiate recovery process, re-commence essential work.

1.4.7 Other Arrangements

- details of any other arrangements not covered in the above

1.4.8 Disaster Recovery Plan

- details of where copies are held and who is responsible for keeping them updated.

1.5 Reviewing business unit contingency

To support a business unit DRP, each business unit will need to review contingency plans. Once completed this information would be managed centrally and related directly to the IT inventory system. This will aid the CEDRG, not only in developing the central DRP, but in provision of cost-benefit and risk analysis data.

1.5.1 Review products / services or critical applications

- Business units, processing cycles, peak seasons
- Minimum requirements to get the unit back up
- Time taken to get the unit back up
- How long can the unit afford to be out of action.
- What is the most likely 'Hot Site' location.
- Inventory lists (PC, Voice, infrastructure, staff, notifications, maintenance).
- Maintenance Support.

1.5.2 Analyse Risks and Exposures

The unit may have several contingencies built into their DRP plan for how it would take recover at different times of the year, depending on its peak season. We need to critically analyse and priortise operational functions.

- If the unit fails to bring a particular function up, what does it stand to lose?
- Determine communications needs - how many voice lines and data lines does the unit need?
- What will it take to get an application / system up and running?
- Determine in advance how big the communication network is, and how much of it the unit has to have up.

1.5.3 Define the Recovery Strategy

When disaster strikes:

- Determine where the unit is in its processing cycle
- Which application is the most critical at that time.
- Determine what the unit needs to do to be in compliance.

1.5.4 Develop Detailed Recovery Plans

This will include as bare minimum:

Contingencies:

- repairing or replacing existing equipment (hardware, software, telephones, cable, etc.),
    - Contingency for telephone failure (e.g. switch, network)
    - Contingency for network failure (e.g. site to site connectivity)
    - Contingency for infrastructure failure (e.g. power)

- locating facilities within the building if it's a limited disaster
- locating facilities to a temporary location within a three-mile radius
- locating facilities to 100-mile radius (in case of a regional disaster).

Building:

- Room dimensions
- Floor space requirements
- air conditioning,
- communication,
- parking requirements,
- controlled access;
- supplies (all needed on a day to day basis)

Technical
Hardware platform requirements
Software requirements
Location of files

Note:
When disaster strikes floor space requirements is critical because the first requirement in housing the unit at a temporary location will be square footage, number of outlets, air conditioning, etc. In most cases the floor space needs will be smaller. The unit may not be able to source hardware with exactly what it had at the time of the disaster.
The hardware platform at the temporary site may be different. It is important that the applications will run on that platform or operating system.

1.5.5 Primary Vendors and Contacts

This must include full address with home / work telephone, mobile, fax and if available, e-mail address.

- Hardware Vendors
- Software Vendors
- Third Party Vendors
- Telephone services support (critical).
- Building services support
- Cabling services
- Network services

1.5.6 Potential Vendor Contact List

If it is a regional disaster, there is no guarantee that current vendors will be able to supply. A back- up list of potential vendors in other areas of the country is suggested to follow in the same format proposed in paragraph 1.4.5.

1.5.7 Test, Evaluate and Revise Recovery Plans

Disaster recovery is a journey with no destination as things are constantly changing. The list is endless of what could have changed since your disaster recovery plan was written-and all of them impact on the ability to recover after a disaster.

Plans will have to be continually tested, evaluated and revised as situations change.

1.6 Collating data

It is vitally important that the collection of data is followed in a structured format. A proposed format to carry this out is as follows:

- Each business unit is reviewed following the strategy outlined in section 'Reviewing business unit contingency', data to be computerised *
- Each business unit also builds their DRPs as outlined in section 'Proposed structure of DRPs', this data is also computerised *
- The current IT inventory is centralised and reviewed by Technical Services and relevant business unit managers.

1.6.1 DRP Template

This template is used to record information critical to the CEDRG in the event of a disaster so that recovery for the business unit(s) can be managed.

For more information on the structure of this template, see the section 'Proposed structure of DRPs'

1.6.2 IT Inventory

IT equipment and notification information will be recorded in an IT Inventory.

The objective of this system is to centralise recordings of all known equipment including maintenance information. Each item of equipment can also be marked as critical and/or sharable. This means that in the event of disaster it is possible to identify equipment, which could be moved without major impact to its business unit to support another business unit affected by disaster.

The procedure in collating information for the IT Inventory is proposed as follows:

1) IT equipment is received by local technical services and installed for the related business unit.
2) The asset information form is completed and passed to Technical Services Inventory.
3) Information is then recorded into the relevant section of the IT Inventory.
4) The business unit manager is informed that the relevant IT equipment is recorded.

1.7 Role of CEDRG

In any disaster situation the Central Emergency Disaster Recovery Group (CEDRG) will be assembled to determine the strategy to be adopted and, where necessary, initiate the Central

Administration Disaster Recovery Plan. This will mobilise the provision of such central services as are needed to support stricken business units.

It will set out the arrangements to be made by:

- Security
- Building services (telephones, power, heat and light)
- Transport
- Site clearance
- Salvage, etc.
- Personnel (staff details)
- Finance (pay, insurance)
- Technical Services
- Marketing (press and PR)