YOUR LOGO

NAME COMPANY OR DEPARTMENT

BUSINESS CONTINUITY PLAN

Good business continuity plans will keep your company up and running through interruptions of any kind: power failures, IT system crashes, natural disasters, supply chain problems and more.

Document Control Sign-off Process

Document Details	
Document Owner	<name>
Contributors	<names>
Review Schedule	6 months / yearly
Testing Programme	May 2012
Associated Documents	• Pandemic Plan • Other plans

Approval		
Version No.	**Date Issued**	**Reviewed/Authorised By**
1	May 2012	Cloud Solutions

Table of Contents

1 Contingency planning

A contingency plan is an impact-reduction measure. It should describe in detail what you and your staff will do if a particular problem occurs.

You may need a contingency plan when:

- you **identify** a risk that you think has a high chance of happening and will have a high impact
- you try to find ways of **reducing** the likelihood of the event, but you cannot reduce the risk to an acceptable level
- the residual risk is still so large that you need to take a **structured approach** to reduce its likely impact

The **main considerations** that you should address in a contingency plan are:

- **scope** - what particular risk the contingency plan is designed for
- **initiation** - how you will know when to put the plan into action
- **actions** - what sequence of actions you will take in order to control the problem and minimise its impact
- **roles and responsibilities** - who will do what and when

Good contingency plans are usually based on the shared experience of managers working together.

An important form of contingency plan is a **business continuity plan** (BCP). This is typically created to cover the most serious of problems, such as the complete loss of all your servers and network infrastructure due to a fire.

Such plans may involve planning for the rapid acquisition of temporary buildings, reciprocal arrangements with other organisations, special staffing arrangements, etc.

BCPs should be **tested** if possible. A test could be a simple paper exercise where different parts of the recovery procedure are run through by the people involved. This is adequate for simple plans.

A full test of a BCP requires a full exercise. This will usually involve many people and significant cost because it will disrupt normal activities. Therefore, any exercise of this type should be carefully planned and budgeted.

2 IT Business continuity planning

Key steps in developing a business continuity plan

There are five key stages in developing and maintaining a business continuity plan.

Understanding your business

- Project initiation and management - get support from senior managers. Establish a management structure to develop and carry out the plan.
- Risk evaluation and control - identify the threats and the best defence. For example, with e-commerce, computer viruses might be a major threat - the appropriate defence might be regularly updated anti-virus software.
- Business impact analysis - establish your business' critical processes and identify the impact of any failures. For example, if your e-commerce website is critical to your operation, what would it cost your business if it went down for 24 hours?

Business continuity management strategies

- Develop an organisational business continuity strategy, identifying which areas you need to concentrate on. Focus on the critical operating requirements of the business, as identified above.
- Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for your e-commerce website goes down, you need a specific strategy for resuming operations.

Developing and implementing a business continuity response

- Emergency response and operations - establish a crisis management process to respond to incidents.
- Develop and implement a business continuity plan. This describes specifically how you will deal with incidents. Focus on the priorities of your overall business continuity strategy.
- Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

Developing a business continuity management culture

- Awareness and training plans - ensure all staff are aware of the importance of business continuity and can operate effectively following an incident.
- Review the effectiveness of awareness training periodically. Identify any further training needed.

Exercising, maintenance and audit

- Test the business continuity plans. Test any technical aspects - for example if you plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.
- Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.
- Regularly audit the plans - do they meet the needs of your strategy? Act on your findings.

3 Components of an IT business continuity plan

You will use information on threats to your business to create your business continuity plan.

The plan should aim to **reduce** the risks posed by disruption to your business processes. Measures that may be needed include:

- A back-up and data recovery strategy, including off-site storage.
- The development of a resilient IT infrastructure with redundancies (spare capacity) in case of failure. For example, mirrored central server computers sited in different locations, each containing the same information, so that if one goes down, the other one is available to ensure continuity of service and alternative storage facilities.
- The elimination of **single points of failure**, such as a single power supply.
- The introduction of an uninterruptible power supply for your IT systems. This is a battery-powered device that allows your systems to keep running, giving you time to save any data that you may be working on.

Even if such measures are adopted, things can still go wrong. Therefore, the business continuity plan should specify the actions to be taken in order to **recover** from any unexpected disruptive event, covering:

- people and accommodation
- IT systems and networks
- services such as power and telecommunications
- critical business processes

Methods of recovery might include:

- carrying out activities manually until IT services are resumed
- moving staff at an affected building to another location
- agreeing with another business to use each other's premises in the event of a disaster
- arranging to use IT services and accommodation provided by a specialist third-party standby site

Keep the business continuity plan short and readable. It should not duplicate other sources of information, and any other relevant documents should be referred to. Encourage staff to review the plan before it is formally issued.

4 Examples of IT related risks

Business managers are used to recognising commercial threats and taking appropriate actions - for example, dealing with a new customer who turns out to be a late payer.

However, IT-related threats in business are much newer, a lot less predictable and change much faster.

A useful way of recognising threats is to classify them as follows:

- **Physical threats** are those that result from physical access or damage to information resources such as servers, network equipment, computer rooms, etc. In some business environments it is easy to overlook these types of threats. However, if an unauthorised person - employee or not - can enter your computer room unobserved, then all your other IT security measures are essentially compromised.
- **Electronic threats** are those that aim to compromise your business information and typically come from outside your premises/network, eg a hacker accessing your network via your website. Other malicious threats can range from phishing and spoofing emails and websites to links in social networking websites that take you to websites that can steal your personal and financial details. Hackers can gain remote control of your computers through infections by viruses, worms or Trojans, turning them into 'bots' or 'zombie computers'. These groups of infected machines - botnets - are capable of a wide variety of activities, including denial-of-service attacks, click fraud and identity theft.
- **Technical failure** is a common threat for IT systems. For example, if key data is stored only on the hard disk of one server, then the failure of that hard disk would be catastrophic. Hard disks in computers will fail eventually, even in expensive servers.
- **Infrastructure failure** can be a subtle form of threat. For example, if your business relies on your internet connection to receive orders from customers, you could miss out on new purchase orders if that connection fails.
- **Human error** is a major threat. If an honest mistake by a user or system manager could cause an irrevocable loss of data, you need to take action to prevent it from happening, eg by regularly backing up data.

5 Roles and responsibilities

ROLES AND RESPONSIBILITIES - **who** will do **what** and **when**

Who	What	When
Name manager	When it should be activated	Activated as per Appendix 3.
Name 2nd in command	Who is allowed to activate it	Activate when assessment recommends
	Activation process	

6 Initial Response

#	**Action for <your company/department>**
1.	Gather at a predetermined site, plan also for a suitable alternative.
2.	Do a head count of your staff and make sure all the staff and visitors are accounted for
3.	Allocate roles – co-ordinator, back up staff, logistics, note taking, record keeping, and insurance advice. See 5 above.
4.	If land lines are out – nominate a cell phone for all incoming calls.
5.	Transport. Establish which cars are available.
6.	**Have a "emergency bag" with emergency essentials easily available.** Contents of this bag – torches, list with important phone numbers, USB data stick with critical operating data. Drink bottles with water.
7.	
8.	
9.	
10.	

7 Facility Outage Action Plan

7.1 Your offices are unavailable

Impact	Disruption to your daily activities.
Maximum Tolerable Outage	▪ 24 hours
BCP Strategy	▪ Establish reporting lines ▪ Where to go? ▪ Assess staff requirements
Responsibilities	Refer to Section 5 of this plan
Maximum Time in Alternative Operations	2 days

Alternate Site Details2	
Location	Work from home
Access	n/a
Resources	Home office, cell phones and laptop with remote access

8 System Impact Action Plan

8.1 Computer Network Down

System maximum restoration timeframe:

Impact	No email or internet or access to remote computers
Maximum Tolerable Outage	24 hours
BCP Strategy	• Ascertaining duration of impact • Description of manual workaround option/s available whilst restoring system • Communications required
Maximum Time in Alternative Operations	1 day

9 Telephony Outage Action Plan

9.1 Land Lines Down

Impact	No land line calls No fax Internet and email possibly OK (operates via fibre optic cable)
Maximum Tolerable Outage	Manual processes capable for ??? days.
BCP Strategy	Nominate a cell phone for all incoming calls
Maximum Time in Alternative Operations	1 day

9.2 Cell Phones Down

Impact	No cell phones
Maximum Tolerable Outage	1 day
BCP Strategy	Use email when email is available
Maximum Time in Alternative Operations	1 day

10 People Outage Action Plan

10.1 Key people

If individual team members are unavailable refer to section 5 of this plan to reallocate duties among those who are available.

10.2 Team/Person Down

Impact	Less people to allocate work to.
Maximum Tolerable Outage	24 hours
BCP Strategy	• Alternative staffing options if regular staff unavailable e.g. non-critical staff could perform this role easily, or request support from similar companies. • Emergency rostering • Communications required
Maximum Time in Alternative Operations	1 day

Appendix 1 - Resources

Resources available to aid in the response process	
Items	**Location**
?? Vehicles	

Equipment / information (required to be sourced on the day)	
Items	**Items**
?? cell phones	
Phone Charger, 1 per cell phone, located with the cell phone holder	
?? Torches	
2 Spare batteries per torch	
List with emergency phone numbers	Hard copy attached to this plan, pocket sized version with each team member

Appendix 2 - Glossary

Term	Meaning
Maximum Tolerable Outage	The maximum period of time that critical business processes can operate before the loss of critical resources affects their operations.
Estimated Recovery Timeframe	Estimated time taken to implement BCP strategy and re-start operations.
Maximum Time in Alternative Operations	The period of time that the business can cope using the BCP strategy/workaround solutions ie how long will the workaround last for

Appendix 3 – Risk Assessment

A risk assessment was performed as the initial stage of the BCP process:

Date: 17 March 2010

Attendees: names

Company name			
Scenario	**Likelihood**	**Consequences for Environmental health Team**	**Current Risk Rating (average event)**
Personnel down – Group/person taken out (illness, accident)	Likely	Shock, morale, reduced capacity	1
Earthquake	Likely	Cost to restore, health and safety for staff.	2
Storm – strong winds	Likely	Damages, health and safety for staff	3
Flood	Unlikely	Loss of service, cost and time to restore	4
Fire	Unlikely	Health and safety for staff Loss of facilities Revenue loss, cost to restore	5
Major accident or serious road works	Unlikely	Cost to restore	6
Eruption	Unlikely	Loss of service Loss of revenue, cost to restore	8