



AIMA's Guide to Sound Practices for Business Continuity Management for Hedge Fund Managers

June 2006



Guide to Sound Practices for Business Continuity Management for Hedge Fund Managers

Table of Contents

1.	Introduction.....	5
1.1	Ownership.....	5
2.	Management & Control.....	6
2.1	An Overview of Management Requirements.....	6
2.2	Event Stages.....	6
2.3	Risks.....	7
3.	Business Impact Analysis and Inventory.....	9
3.1	Current systems and processes.....	10
3.2	Relationship network.....	11
4.	Protection and Recovery Plans.....	12
4.1	Crisis management.....	12
4.2	Recovery.....	13
4.3	Resumption.....	16
5.	Testing.....	17
5.1	Desk walk-through.....	17
5.2	Communications test.....	17
5.3	Evacuation.....	17
5.4	Recovery to offsite.....	18
6.	Updating.....	19
	Appendix - Check Lists.....	20
	Check List 1 - RFP questions.....	20
	Check List 2 - Disaster information file.....	22
	Check List 3 - Disaster preparation kit.....	24
	Check List 4 - Frequently found problems.....	25

Foreword

In the modern age, the importance of sound practices in the area of business continuity has never been greater. The increased use of the hedge fund industry by institutional investors requires all participants to build, test and review their contingency plans having identified any threats to the smooth operation of their business.

Managers have to demonstrate to investors and regulators that they are able to manage investors' money effectively, prudently - and reliably. Vitally for hedge funds, major incidents in financial centres are often accompanied by big market moves. Just when you want to trade, you may not be able to.

Business Continuity Management is the process of identifying threats to the smooth operation of a business or similar organisation and preparing plans to:

- reduce the likelihood of a major disruption; and
- respond effectively to an emergency should one occur.

Such a plan aims to ensure timely and orderly resumption of the business cycle with minimal or no interruption to time-sensitive business or service operations. It goes well beyond the traditional "disaster recovery" activities, which were essentially focused on technology recovery, to plan the management of the entire business during, immediately following, and long after a potential disaster.

This is increasingly being mandated by regulators. As an example, article 5.2 of the draft Level 2 of MiFID (the European Commission's Markets in Financial Instruments Directive) states:

"Member States shall require investment firms to establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the preservation of essential data and functions, and the maintenance of investment services and activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their investment services and activities."

Cont./

Business continuity management is therefore vitally important for hedge fund businesses, and requires a higher level of attention and preparation than for most businesses of similar sizes. For this reason, AIMA's Sound Practices Committee has prepared this set of principles which are specifically designed for the small- to medium-sized hedge fund management company.

We would like to thank and congratulate the members listed below, all of whom have volunteered their time and worked extremely hard to produce this valuable Guide. We intend to revise the Guide as and when developments or additional material appear.

Florence Lombard
Executive Director, AIMA

June 2006

The Guide is not to be taken or treated as a substitute for specific advice, whether legal advice or otherwise.

This guide was drafted by Catherine Doherty from Investit, revised by Mark Paton from JP SA Consulting Limited. Other contributors were:
Paul Mack, Arundel Iveagh Investment Management Ltd
Paul Parkins-Godwin, Financial Risk Management (FRM)
Steve McGuinness, HedgeSupport
Tom Brown, KPMG
Graham Phillips, PricewaterhouseCoopers
Florence Lombard, AIMA

© The Alternative Investment Management Association Limited 2006

All rights reserved. No part of this publication may be reproduced in any material form without written permission of The Alternative Investment Management Association Limited. Full acknowledgment to authors, publisher and source must be given.



1. Introduction

This Guide considers the planning and arrangements which should be made to ensure a hedge fund manager can continue to operate effectively under a wide range of circumstances.

It looks at operational risk management and considers impact of non-trading-related criminal activity. It does not cover the management of portfolio or market risk, or extreme market events, which are considered to be part of routine effective fund management and are therefore covered in the relevant AIMA Guides to Sound Practices for Hedge Fund Managers.

The Guide covers the following key topics:

- identification of risk events;
- identification of the system, process, information and relationship network which make up the enterprise;
- definition of recovery requirements;
- development of protection and recovery plans;
- testing and proving the plans work;
- maintenance and updating of the plans.

This Guide is written for a hedge fund manager with 5-50 employees. Larger companies will find that the basic principles still apply but they may require more rigorous preparations.

1.1 Ownership

For a business continuity plan to be effective, it must be owned and supported by a senior company official, who would usually be the Chief Operations Officer and who should hold director or similar status.

It is unlikely that this ownership can be provided by a more junior role. If the plan is to be owned by a role such as the IT Manager, it is very important to provide substantial proof that the business aspects have not been neglected.



2. Management & Control

2.1 An Overview of Management Requirements

A serious business disruption needs to be managed through its entirety in a structured and controlled manner to ensure consistency of decision making and communication.

A Crisis Management Team made up of senior managers who represent the whole organisation should manage the organisational issues of an event. This team must be responsible for the evaluation of the event and the response to it until full resumption is achieved.

2.2 Event Stages

The three recognised stages of an event are Crisis, Recovery and Resumption.

The **Crisis Management** phase handles the immediate aftermath of the event and addresses the initial evaluation and risk mitigation actions deemed necessary:

- the wellbeing of staff;
- effective and controlled communication;
- evaluating the impact of the event;
- deciding what must be done and initiating the response;
- executing predefined functional Crisis Management plans; and
- protecting the company's franchise.

The **Recovery** phase looks to the medium term response to an event, ensuring the key business functions can continue and an adequate service is provided to the clients:

- carefully migrating work done during Crisis phase to core systems;
- performing additional tasks with reduced resources;
- controlling updates to data and systems with a view to full resumption;
- communicating with staff and external parties about what can and cannot be achieved during this phase;
- allocating resources to facilitate a sustainable work flow which may mean flexible working from staff; and
- using some staff to prepare for full resumption.



The **Resumption** phase addresses the return to full operation once the event has ended and the effects are fully understood and have been overcome:

- validating data captured during previous phase;
- ensuring core systems fully aligned;
- producing any reports or other deliverables that have been missed during Crisis and Recovery; and
- updating business continuity plans to reflect any changes to premises or procedures after the event.

Each of these stages needs to have a plan. In addition a general communications plan should be developed to ensure the right internal and external messages are delivered in a consistent and coherent manner.

2.3 Risks

Planning starts by considering the range of risks that the company is exposed to. There are four key types of risk which any event can bring:

- Loss of access to the building, eg:
 - Catastrophic failure of office premises (fire, terrorist attack);
 - Denial of access to office premises (bomb alert, biological or chemical threat, local flooding);
 - Non-working of office premises (electricity failure, telephone systems failure, burglary).
- Loss of staff, eg:
 - Multiple key staff losses (epidemic, accident in or near your premises or during a company visit);
 - Death or incapacity of "key man" e.g. founder, principal(s) or chief executive officer.
- Loss of systems, eg:
 - Failure of internal company systems;
 - Failure of external systems or interfaces;
 - Criminal corruption of company data.
- Loss of suppliers, eg:
 - Failure of critical third party e.g., prime broker or fund administrator;
 - Failure of service providers.



Companies may find it helpful to consider disaster scenarios, each of which will involve some or all of these four risks. The range and scale of these will depend on the location of the company - there is a recent trend for "one-in-200-year" events to happen much more frequently, so it is worth being alarmist at this point. A hedge fund manager based in the centre of London or New York should be prepared for at least the following scenarios:

- A major terrorist incident which makes a large area of the city unusable for several days;
- The office building catching fire and being severely damaged by the water used to extinguish the fire;
- A local terrorist incident or health-related scare which means that you cannot get to your building for a few days;
- Substantial travel-related problems which keep many key employees away from the office;
- A power cut lasting several hours;
- Burglary of all the computer equipment in the office, including laptops;
- Computer virus corruption of key spreadsheets.

The following scenarios should also be considered:

- Loss of any two key people at the same time;
- If you live close to the office, a disaster which affects both your home and your office.

And depending on local geography:

- Major destruction of local area (freak weather, earthquake, etc).

Each scenario should define the size of zone which could be affected, remembering that disasters can result in huge no-go zones while emergency systems coordinate their first response.



3. Business Impact Analysis and Inventory

The first stage is to identify the business critical activities across the whole organisation. This provides a structured focus that will allow decisions to be made about what is the priority during each phase of a crisis event.

The plan should not get bogged down by becoming an exercise that writes down day-to-day procedures or gathering huge amounts of information about who usually does what and how in business. These are important but Business Continuity should not be the platform for that work.

For every area of the business the company should identify:

- key activities;
- the impacts and the affect if that key activity cannot be performed;
- recovery time objectives (how quickly each task must be done);
- deadlines (internal/external/hard/soft);
- key internal dependencies on that function;
- key external dependencies upon which that function relies;
- system and technical requirements.

From this the senior management can agree what the most critical tasks are in a Business Continuity context. For example, FX hedging may be deemed so important that plans need to be made to ensure that it can happen instantly even in the most severe disruption. Whilst client reporting is important it may be able to be delayed for a day or two.

Each key activity is agreed and designated as a “crisis” or “recovery” task. Then detailed plans can be prepared to describe how they would be performed, using what resources. The key parameter here for a hedge fund manager will be the trading nature of the funds. A fast-trading fund would have very different recovery timescales from a fund of hedge funds.

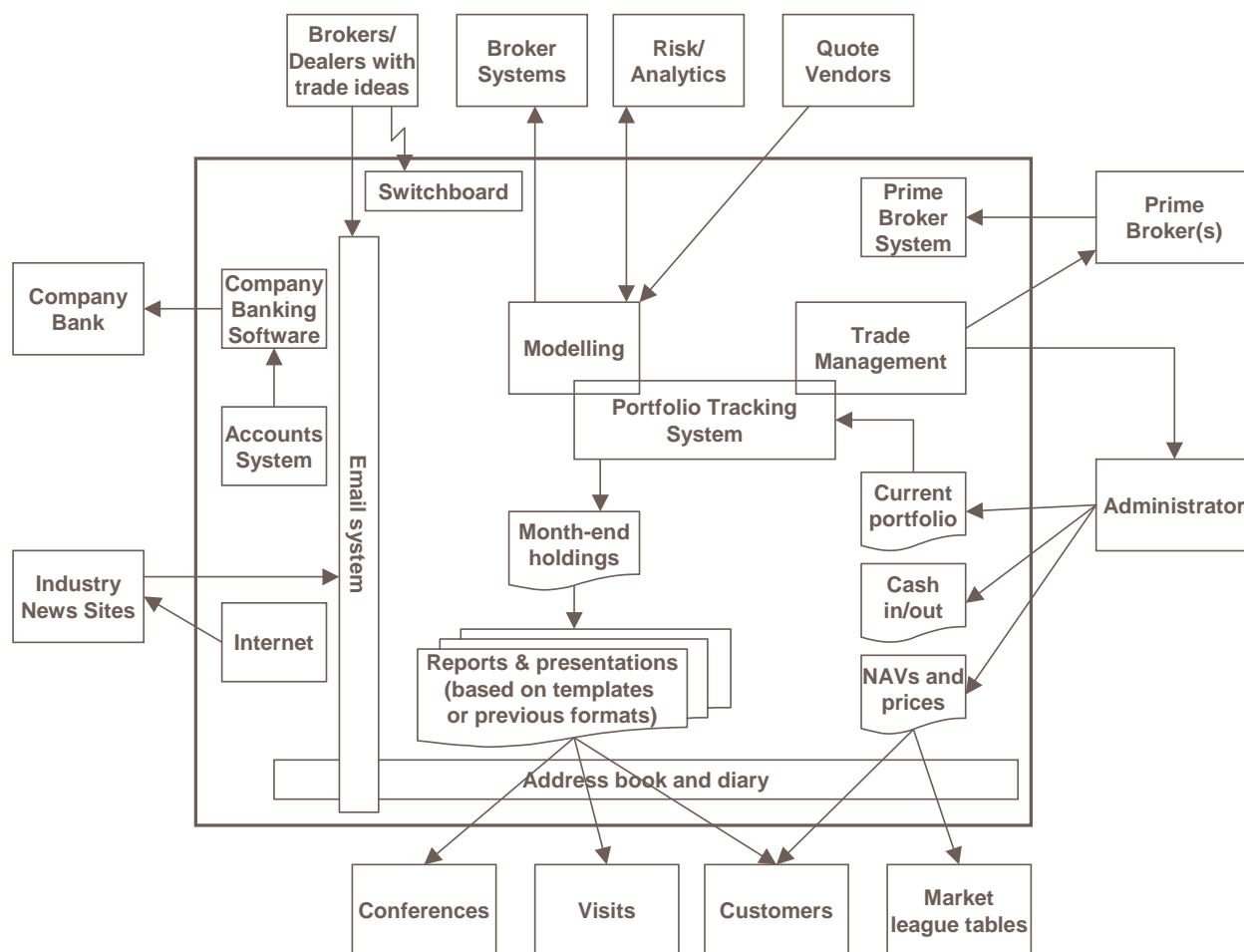
This has to be a comprehensive exercise so to get a complete picture, several different people in the company should contribute, including representatives from:

- directors and senior management of the company;
- fund management, dealing and treasury/financing;
- operations;
- compliance;
- client management and sales;
- IT support;
- finance and business administration.



3.1 Current systems and processes

It may be helpful to build up a picture of the company's systems and information flows. A simple schematic can be used, for example:



This diagram can then be used to drive a more detailed inventory as required:

- For each item entering or leaving the hedge fund company, what additional pieces of information are involved: contact names, fax/phone numbers, passwords or other security devices, special file formats or specific web addresses?
- How critical is each system, interface or service and how quickly does it need to be recovered?
- What is required to reconstruct each system, interface or service somewhere else?
- Is there any other paper-based information which does not appear on the diagram e.g. statutory books and records?

This will give an overall understanding of the scale and amount of systems and links which need to be rebuilt in order for the company to function fully.



3.2 Relationship network

No hedge fund is a single stand-alone enterprise. As illustrated in the previous diagram, a typical network of relationships will include:

- prime brokers;
- fund administrators;
- clients;
- accountants, auditors, lawyers and bankers;
- other trading counterparties;
- market information providers;
- system hosting services;
- off-site storage or archive providers.

For each relationship in this network the company should assess:

- how key their service is;
- what arrangements need to be made to re-establish links;
- what arrangements are in place by the service provider for their own recovery from failure and how their replacement service can be interfaced.

Suppliers should be considered both as part of the solution and as part of the problem:

- the administrator can contact registered investors and can restore portfolio positions;
- the company bank, lawyers or accountants can store key corporate documents;
- but a locally-based prime broker may be affected by the same scenario;
- and service interruption from a single key market information provider might be a disaster scenario that the company needs to plan for.

Managers should make sure that key suppliers have their full contact details.



4. Protection and Recovery Plans

The business inventory has now identified vital business areas to be recovered, and the requirements have shown what needs to be recovered and when. This information can now be used to plan for recovery.

- Planning should start by considering the disaster scenario which has greatest impact without being completely catastrophic. This could be a terrorist or natural disaster where the office and its surrounding area are destroyed and some key staff from the company have been lost.
- Once these plans are developed, they can be modified for the lower-impact scenarios.
- Plan should be made for activation during office hours and if a disaster occurs outside office hours.
- In the event of a complete catastrophe, involving the loss of all key staff, the plans should include arrangements to liquidate the funds and return the assets to the investors with no intervention from any senior employees. This would apply especially to a small single-office company.

Plans should cover:

- How to activate and manage the recovery process;
- Arrangements for technology recovery;
- Arrangements for premises recovery;
- Management of communications with staff, clients and suppliers.

4.1 Crisis management

Because recovery plans can be complicated and costly to put into effect, the company must decide who can declare that contingency arrangements should start. A clear chain of command is required, with at least two and preferably more people able to take control.

A crisis management team must be defined. This team needs to meet very early on, to agree that a crisis is occurring (in some cases of creeping failure this can be a difficult decision) and to take the initial decisions on which type of plan to put in place. There must be a one-to-two page checklist supporting this: "What to do in a crisis".

The key roles/responsibilities to be played in the recovery should be identified, and more than one person should be able to fill each key role (especially the IT system administrator role). Note that the people filling these roles need not be the same as the crisis management team. These roles would include:

- Recovery co-ordinator;
- Technology recovery manager;
- Premises recovery manager;
- Communications manager.



Checklists should be developed for each role showing what should be done immediately, after one hour, and in later phases. It is also useful to have some people designated as “runners”.

The plans should include a list of locations where this team should assemble if an incident occurs, and a way to agree on which location to use. Locations should include:

- a site 100-250m away from the office as primary assembly point;
- a site over 500m away from the office as secondary assembly point;
- a much more distant location, which could be a home or a remote office.

4.2 Recovery

4.2.1 Technology recovery

Technology recovery plans should include:

- workstations (with information about all workstation specifications required to undertake all critical tasks);
- network servers and tape drives (or equivalent methods of restoring backed up information);
- printers and printer drivers;
- interfaces to key service providers;
- telecommunications, especially if multiple voice or data lines are required;
- internet access.

There are many specialist technology recovery companies who offer services in this area, and the company’s prime broker may be able to help with the selection of one. Technology recovery services can include:

- storing and retrieving backup data (on a server or on tapes);
- keeping full copies of working systems, either during the day or overnight;
- being able to provide replacement computers;
- providing a full standby network which is ready to use.

If a third party supplier is used to support any part of the recovery, it is important to check how many similar businesses they are supporting and make sure they have sufficient capacity to handle the key disaster scenario. Hedge fund businesses tend to be concentrated in small areas of the city, so many similar businesses could be affected by even a mid-scale disaster.



4.2.2 Premises recovery

The company may need to have fast access to a new office to allow investment management to continue, although this could just be for a few key investment staff. Recovery plans could make use of:

- one or more home offices;
- a “warm” or “hot standby” arrangement where desks and key systems will be quickly available;
- a “cold standby” arrangement where desks could be made available after a defined period of time;
- agreements with key suppliers or even clients to use an area of their offices.

4.2.3 Communications management

The company will need to get in touch quickly with staff, suppliers and clients.

As general principles for communications:

- Plans should not rely completely on mobile telephones or via Blackberry: most major cities can reserve the mobile networks for emergency service use only in times of crisis, as was demonstrated during the London bombings in 2005.
- It is acceptable to rely on the internet being available as long as key supplier elements are considered (the company’s internet access provider, web site hosting service provider, access rights and knowledge to update the company web site, power for laptops, network communications not being routed through a powered switchboard).
- The plans must not rely on any one person being available.

The company should be able to divert incoming telephone calls to the recovery site or to put a forwarding message onto the incoming lines. Recorded messages on a pre-agreed number, or private internet chat sites could be useful for staff and client communication.

Staff communication

- Each member of the company must know what they do by default in an emergency (go home, try to assemble at a defined location, go to the disaster recover site, etc). Some staff roles may be changed or be suspended; for example, sales may stop and staff could be reallocated to client communications;
- A routine must be established to spread the news about changed arrangements, which could use a call tree structure and/or web communications through email or web site updates. A call tree defines a cascade of phone calls so that each person calls a few other people, rather than one person having to make calls to the whole company.



Building Manager and Insurer communication

- Where hedge fund managers rent office space and facilities including building services management, recovery plans should be co-ordinated with and evaluated by the building owner/manager.
- The company's insurers should be included in the plans, although the level of immediate practical help they will be able to give will depend very much on the scale of the disaster.

Supplier communication

- The plans should show which suppliers need to be informed of the changed arrangements and in which order, and they show the role that key suppliers are planned to play in the recovery. There may be multiple contacts within some suppliers; their different roles should be documented in case the person running the recovery is not familiar with that supplier.
- Voice, fax and email communications should be covered.

External/Public communication

- External communication must be very carefully controlled. Investors and intermediaries need to know what is happening to the fund and any changes planned to the management or dealing arrangements, and they need to be kept updated as the recovery progresses. Companies with a high public profile should include a media communication plan.
- The fund's administrator could assist with investor communications.
- Regulators, auditors and lawyers should also be kept informed about any changes.



4.3 Resumption

As the company switches to crisis and recovery level systems and processes, it is vital to plan for the return to business as usual. During the early stages of an event certain processes may be performed off-line or in some cases not at all. The Management team needs to keep a very careful check on what has been done and to what level during the Crisis Management and Recovery phases of the event so that the Resumption phase can be correctly delivered.

What a Resumption plan looks like depends heavily on the extent of change resulting from the event. Once the Recovery phase has been started a dedicated group should be tasked with creating the detailed Resumption plan.

Here are some areas to consider when planning the move from the Recovery Phase into full Resumption:

Have staff or roles changed?

- What impact has the event had on staffing?
- Have staff been fully briefed on their role in the Resumption phase, i.e. will they be focussing on new business or working through the backlog of work?

How do we become compliant again?

- Have client files been updated for transactions or conversations that may not have been captured via the normal method (i.e. recorded phone lines)?
- Have investment decisions been correctly documented and passed by the appropriate Investment Committees, etc?
- Have clients and other related parties been informed that we are changing our mode of operation, ensuring they have full contact details and are ready to resume full business with us?
- If some functions were not performed during previous phases has a plan been agreed with external parties to deliver missing information, reports or services?

Do systems need rebuilding?

- Are there plans to complete the upload of all data that was amended or kept on spreadsheets during the Crisis Phase or Recovery Phase into business as normal systems?
- Is there a data synchronising test to ensure there is a clear and agreed starting point for business resumption?

Will the company have a new office?

- Which contracts, stationery or other documents need to be updated?
- Have staff been fully briefed on the health and safety aspects of the new office?
- Has the Business Continuity Plan been updated to cover the new building? Lightning sometimes does strike twice.....



5. Testing

The plan cannot be claimed to be effective until it has been tested. The following tests should be carried out routinely:

- A desk walk-through of the plans;
- A full test of the communications tree;
- A basic building evacuation drill;
- A full or partial recovery to the offsite facility.

5.1 Desk walk-through

Once the plans are developed and whenever there is a significant change, there should be a dry-run of the recovery. The key recovery roles should be assigned and the recovery should be acted out. Business staff from each section - investment, investment support, client communication - should go through their activities and make sure that the right systems and information are in place at each step.

These dry-runs could be done with different key staff "unavailable".

5.2 Communications test

The communications tree should be tested regularly. During these tests some key staff could deliberately be made unavailable to check that alternative communication routes work - exactly as might happen in a real disaster.

5.3 Evacuation

Staff should regularly perform a full evacuation from the offices assuming that the primary exit route is blocked, and meet in the primary assembly point which is usually around 100-250 metres away from the building. Staff should also be clearly aware of a secondary assembly point which should be over 500 metres away from the building.

Because on the day there will be a lot of different companies evacuating and the area will become crowded, many companies have signs which can be held up to help teams meet up.



Check: At this point you will be outside the building, hopefully with a BCP file in someone's hand. Could you perform a full recovery from this point?

5.4 Recovery to offsite

The full plan should be tested, at least to cover:

- the first 6-12 hours of the IT recovery, and IT recovery of all key data;
- involvement of key, but not necessarily all, staff.

The frequency of testing depends on how dependent the company is on its systems. For a company with a high dependency on IT systems then it may be appropriate to hold a full test each year. For a company with lower dependency on IT systems the full plan may only be tested once every two years. Different systems can be tested at different frequencies. This is up to the company to define for itself.

Because the company will need to balance the desire to continue trading with the requirement to test the plans, it may be most efficient to test this at a weekend. If a home office is used as part of the plan, it could be regularly tested by detaching it from the company network.

At a minimum the company should test:

- that it can restore an adequate view of the current portfolios and can continue to manage the funds;
- that it has established links with key people in the supplier chain;
- that it has contact information and details necessary to continue with further recovery activities;
- that it has established communications with all company staff.



6. Updating

The company needs a clear plan for keeping BCP arrangements up to date. There needs to be clear ownership of the plan and regular review cycles.

The company should be able to demonstrate that four review cycles exist and are effective. Each of these cycles should be clearly owned by a member of the company:

- For **ad-hoc changes**: regular updating of all information held on- and off-site such as staff contact information and key password changes. Also each business process needs to be owned and refreshed regularly by team leaders as business processes can change very quickly, especially in the early stages of a company's life.
- For **general updating**: a review every 12-18 months of the provisions, the risks considered and the overall adequacy of the plans made.
- For **major business changes**: a reconsideration of the plans whenever a major business change occurs, such as appointment of a new key supplier, creation of an additional office or launch of a new investment strategy.
- When a major **new potential risk** is identified (9/11, Avian flu, etc): a re-examination of the plan for its ability to handle the new risk events which could result.

Appendix - Check Lists

Check List 1 - RFP questions

The company should be able to answer the following questions:

Overall plans

- ✓ Do you have a business continuity plan (BCP)?
- ✓ Within your company, who is the owner of the BCP? If this is not a board-level person, why not?
- ✓ When did you last test your business continuity plan? How often do you test it?
- ✓ What did you learn from the last test of your BCP?
- ✓ Have you needed to activate recovery plans within the last three years? If so, please give details.
- ✓ What is your policy for when to activate your BCP arrangements?
- ✓ How often do you review your BCP? When did you last review it?
- ✓ How often do you update the details of your BCP? Who is responsible for these updates?
- ✓ Which events are specifically considered in your business continuity plan?

Specific arrangements

- ✓ Where are your back-up trading desks situated? How many other companies share this facility?
How far away are these desks from your main office? How do you plan to get there?
- ✓ Do you have backup power supplies in place? When did you last test them?
- ✓ Who in the company is in charge in the time of a crisis? Who is their back-up person if they are not available?
- ✓ Do you have any particular staff with critical and unique skills? What arrangements do you have if two or more such staff are suddenly unavailable?
- ✓ Where and how is your proprietary data backed up?
- ✓ Which information do you keep in paper format, and what arrangements do you have to protect it?
- ✓ What arrangements have you made in the case of service failure from your key suppliers - prime brokers, administrators etc?
- ✓ Which are your key systems? Do you have a backup arrangement for them with a third party supplier, if so please give details?
- ✓ What is your timetable for recovering IT functions? When did you last do a full recovery of IT systems?

Security questions

- ✓ What is your computer security policy?
- ✓ What virus protection arrangements do you have in place? When were they last updated? What is the policy for updating them?
- ✓ What is your policy on checking staff references before joining?
- ✓ What is your security policy for dealing with “bad leavers”?
- ✓ What security do you have on your laptop computers?

Check List 2 - Disaster information file

The following information must be held in a file which is held in multiple places outside the normal office. It is critically important to ensure that password security is maintained and that the disaster recovery plan does not become a potential source of disaster.

Personnel-related

- ✓ Recovery roles and management
- ✓ Recovery locations
- ✓ Staff contact tree
- ✓ Home addresses, landline and mobile numbers and next of kin details for all staff

Checklists and recovery plans

- ✓ Activation plans
- ✓ Damage assessment checklists
- ✓ Checklists for each role
- ✓ Technology recovery plans
- ✓ Premises recovery plans
- ✓ Communication plans
- ✓ Systems/process diagram and relationship network

Support information

- ✓ Contact details for prime broker and administrator - name, phone numbers, email, fax numbers
- ✓ Web addresses and up-to-date passwords for any systems accessed over the internet
- ✓ Market data provider contact names and access codes
- ✓ Key customer contact details
- ✓ Insurance company contact details, policy number and out-of-hours phone line
- ✓ Office landlord contact details and out-of-hours phone line; office floor plan
- ✓ Contact details for any market participants (brokers etc) who regularly call and will need to be told a new number
- ✓ Administrator log-on and network access details
- ✓ IT provider details, location of backup tapes/servers and method for getting them back
- ✓ Remote access details for email hosting service
- ✓ Recovery guidelines for key IT systems

Additionally the following items should be stored in at least two places off-site:

- ✓ Spare hardware “keys” (dongles, passcode generators, etc) to access systems, or methods of getting new ones
- ✓ Spare company chequebook
- ✓ Copies of any important company certificates
- ✓ Software master disks and access codes (these may be impossible to duplicate, but at least the collection of disks could be split up)

Check List 3 - Disaster preparation kit

Governments usually issue specific information on preparing for a civic disaster, and the company should be aware of and follow local guidelines.

The following list would form the basis of an employee kit for a disaster such as a dirty bomb, earthquake or local flooding, where staff may be confined to the office afterwards or where a substantial amount of the city's infrastructure becomes unusable:

- ✓ Radio and spare batteries
- ✓ Torch
- ✓ Safety light stick
- ✓ Alert whistle
- ✓ Dust and toxic fume masks
- ✓ Disposable overalls, disposable gloves, sponges for washing, survival blanket
- ✓ Disposable camera
- ✓ Building plan with water/electricity/other services marked
- ✓ Drinking water
- ✓ Food (for morale and shock prevention purposes rather than long-term nutrition)
- ✓ Up-to-date copy of the disaster information file
- ✓ Printed copy of the local government guidelines, and contact information for services
- ✓ First aid kit (wound dressings rather than sticking plasters), painkillers and first aid manual
- ✓ "Old fashioned" phone handset to plug into the fax line
- ✓ Pack of cards!

Your arrangements must assume that the mobile phone networks are not available and that power is at best unreliable.

Check List 4 - Frequently found problems

This list contains some of the typical unpleasant surprises found by similar companies when testing or using their business continuity management plans:

Systems-Related

- cross-linked spreadsheets which do not work when restored to a different drive/directory
- internet passwords which have been stored as “cookies” and forgotten
- hardware-protected systems which require “dongles” or pass code generators
- fax numbers which have been coded into a button on the fax machine
- absence of diary and contact information
- loss of key historic emails which are being used as a secret filing system
- forgetting to make plans and information available from outside the main office/network.

Premises-related

- signing up for a multi-use facility shared by very similar businesses, and finding that they have got there first
- finding that the desks have been rearranged in the DR facility and you are now “sitting” in a corridor
- finding that your DR facility is inside the exclusion zone of the disaster
- finding that the rooftop evacuation route is difficult to use in business clothes, or that staff have vertigo
- not having transport to get to the DR site.

Other

- finding that your very obvious rendezvous place has also been selected by every other firm in the area.



The Alternative Investment Management Association Ltd
Meadows House, Queen Street, London W1J 5PR
Tel. +44 (0)20 7659 9920
www.aima.org

