



Alternative Investment  
Management Association

# AIMA'S GUIDE TO SOUND PRACTICES

## Business Continuity Management for Hedge Fund Managers and Funds of Hedge Funds Managers

---

June 2012



## Table of Contents

1.	INTRODUCTION.....	5
2.	MANAGEMENT.....	8
3.	PLANNING: BUSINESS REQUIREMENTS.....	9
4.	PLANNING: INFORMATION TECHNOLOGY.....	12
5.	EXTERNAL DEPENDENCIES AND CONTACTS.....	14
6.	CRISIS SCENARIOS: RISKS, MITIGANTS AND OUTCOMES.....	15
7.	CRISIS MANAGEMENT.....	21
8.	RECOVERY.....	27
9.	RESUMPTION.....	30
10.	MAINTENANCE.....	31
11.	TESTING AND TRAINING.....	32
12.	STAFF OBLIGATIONS.....	34

## FOREWORD

Since the initial version of this guide was published in 2006, the world has changed and with it so has Business Continuity Management (BCM). Among the lessons that we have learned since 2006 is that extreme events and scenarios that may have once been deemed impossible have happened and management in turn have had to react to these challenges.

The sound practices advice offered in our initial guidance still stands; indeed, the need for sound business continuity planning for hedge funds has never been greater with investors and regulators leading the calls for greater improvements to be made. As we have observed the “institutionalisation” of the hedge fund industry throughout the past decade, a more sophisticated operational framework is required to attract institutional investor capital today. Today many hedge fund investors view a Business Continuity Plan (BCP) as a prerequisite to capital allocation<sup>1</sup>.

Change too has also been driven from the continued regulation of the industry. In Europe, it is now a requirement of member states 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”.<sup>2</sup> Further, regulators in the US are also requesting that business continuity planning no longer be just a best practice for US hedge funds but also a requirement. Hedge fund managers should therefore have robust programs in place and be ready to show industry examiners that all statements in the business continuity plan are completely accurate and adhered to.

This revised guide has updated and re-sequenced the material to more faithfully reflect the structure of a Hedge Fund's typical Business Continuity Plan (BCP), so hopefully making it easier for the drafter of a Hedge Fund or Fund of Hedge Funds BCP to successfully complete their task. New material has been added setting out some of the Crisis Scenarios that may arise and what mitigations may be gainfully utilised. The sections on Crisis Management, Recovery and Resumption have been expanded as these are the key parts of the Guide while the section on Testing has been expanded and organised in the context of a testing hierarchy - which should also assist investors undertaking operational due diligence.

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

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

---

<sup>1</sup> AIMA – Guide to Institutional Investor's Views and Preferences regarding hedge fund operational infrastructures (2011)

<sup>2</sup> Article 5(3) MiFID Implementing Directive 2006/73 EC

This guide was drafted by Peter Northcott (Mako Group).

It was reviewed by:

Christopher Miller (Investment Quotient)

Mark Paton (Paton Consulting Limited)

AIMA COO/CFO Group

Coordinated by:

Tom Kehoe (Research Manager, AIMA)

Peter Northcott has prepared BCPs for four different financial services organisations and also has first-hand experience of explosions (both a bomb and an industrial accident), hurricanes and an earthquake. Peter is a member of the COO/CFO group at AIMA and has actively participated in the updating of some of AIMA's recent illustrative questionnaires for Due Diligence.

Christopher Miller and Mark Paton run consulting businesses and have extensive experience advising alternative investment firms in the area of business continuity management.

© The Alternative Investment Management Association Limited 2012

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 sets out principles a small-to-medium sized alternative investments firm should consider when developing a **Business Continuity Plan (BCP)** as part of the **Business Continuity Management (BCM)** process.

In particular, it describes the management organisation, infrastructure and processes that should be established to address a broad range of potential business disruptions, subsequent operation in Recovery mode and Resumption of normal activity. It also includes guidelines for undertaking business analysis and, importantly, Testing procedures.

Larger companies will find that the basic principles still apply but they may require more rigorous preparations.

### 1.1 Why Compile a Business Continuity Plan?

For alternative investment firms, the decision to set up a BCP is usually easy because they have very little choice in the matter. Regulators, investors, or both, generally require significant resilience in the event of business disruptions.

But there are practical reasons too. Managers with "fast" operations, which have high frequency trading, could be put out of business if they were suddenly unable to place or close out trades. This sort of manager has the most demanding requirements for business continuity. In the event of disruption, they need to be up and running with an alternative location or systems within minutes or seconds.

Managers with "slow" operations, which trade on a more extended cycle may have a less demanding timescale, but they still need to resume operations securely in the event of problems, and a loss of data could put them out of business too.

In a disaster, unprepared businesses suffer disproportionately. Estimates vary, but up to 80% of businesses involved in a major incident go out of business within a short period of time. However, with effective planning, a firm cannot only survive, but, can enhance its reputation.

### 1.2 Definitions

The Business Continuity Institute defines BCM as:

"An holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and value creating activities.

Its primary objective is to allow the top management of an organisation to continue to manage their business under adverse conditions, by the introduction of appropriate resilience strategies, recovery objectives, business continuity and crisis management plans in collaboration with, or as a key component of, an integrated risk management initiative."

Furthermore, the characteristics of a Crisis include:

- An urgent need for decisions;
- A lack of accurate information on which to base those decisions;
- An acute shortage of time;
- Insufficient resources at [the organisation's] disposal
- Uncertainty of the outcome.

A BCP is generated as part of the business continuity process. The BCP will typically incorporate the **Disaster Recovery Plan (DRP)**. The latter is purely focused on the IT recovery, whereas the BCP additionally incorporates business activities.

### 1.3 Key BCM Goals

Any incident disrupting normal business operations will require prompt, precise and decisive action. In particular, BCM should:

- Minimise the impact to staff welfare.
- Minimise the impact on physical and financial assets.
- Minimise the impact on continuing operations.
- Maintain the security of confidential information.
- Minimise the impact on, or even enhance, the organisation's public reputation.
- Ensure the organisation can continue operating as a going concern during the disruption.
- Expedite the return to normal operations.

Events requiring contingency plans can vary from a single hard disk failure to the complete destruction of a building or city. A good plan explores many scenarios, but remains flexible enough to respond dynamically to a completely new threat.

The classical sequence of phases envisaged by a plan: "Crisis -> Recovery -> Resumption" are explicitly explored in this document - a good BCM plan will prioritise tasks in this sequence and define the transition between the phases.

It is also important to note that a plan is not the same thing as a capability. A capability can only be developed through Training and Testing, which are also addressed in this guide.

### 1.4 Inclusions/Exclusions

This guide references the most feasible crises relating to business continuity interruptions. However it is important to note that in an extreme crisis, for example, one involving the destruction of the building and the death/serious injury of many staff, it may not be possible to resurrect the business as a going concern. In this instance, the limit of the recovery would be to wind up the business in as orderly a fashion as possible.

This guide also does not attempt to cover operating risk more broadly - this is outside the scope of BCM. However it is important that business continuity remains part of the Operating Risk remit in general so that it is periodically monitored along with other risks.

### 1.5 Assumptions

This Guide makes the following assumptions:

- The organisation preparing a BCP is a Hedge Fund Manager or Fund of Hedge Funds Manager (although aspects of the advice are applicable to other organisations).
- The organisation has between 5 and 50 staff. Larger organisations should have greater scope to budget for specialist advice in this area - which is recommended as organisations become more complex with size.
- The organisation has just one office (if an organisation has more than one office then this creates considerable scope for increased resilience).
- The organisation outsources the management of its IT and Telecoms Infrastructures, which in turn are structured in a traditional way. With the advent of cloud computing and serverless offices this assumption may not always be valid, particularly for newer organisations.

- The organisation is independent and fairly traditionally organised. If many functions were outsourced, for example, then this would change the nature of the risks faced and thus the planning required.
- There is no hot site - in the event of no access to the office, staff would be expected to work from home using a Virtual Private Network (VPN). However firms should be aware that regulators would not expect this to be an extended arrangement - in particular, the Resumption phase should target co-location in either the existing office or, if that is not possible, a new one.

## 2. MANAGEMENT

### 2.1 Ownership and Responsibility

The ultimate responsibility for BCM rests with the directors or partners of the business. The topic should therefore appear on a board or partnership meeting agenda at least twice a year. The subject should also be discussed by the organisation's risk committee at least quarterly.

BCM should be the direct responsibility of a director/partner - typically the Chief Operating Officer (COO), as part of their operational risk remit. Inevitably, aspects of business continuity will be delegated; nevertheless it is important that the COO maintains high visibility in this role to support the embedding of the process within the organisation. It is therefore appropriate for the COO to be the chairman of both the Crisis and BCP teams - although this does not have to be the case.

### 2.2 Crisis Management Team Composition

The purpose of the Crisis Management Team is to manage the organisation's response to a crisis and thereafter through its recovery and resumption phases. Other than for training and testing purposes, the team would generally only meet when a crisis is imminent or has occurred.

The specific composition of the team will clearly vary considerably, dependent on the size and characteristics of the organisation. Nevertheless, typically, the team would comprise the following members:

- Chief Operating Officer (Chairman).
- Delegated Plan Owner (Individual with day to day responsibility for the plan including business impact analysis, training and testing).
- Chief Executive Officer (Key role during crisis validating major decisions and communications both internally and externally. Needs to be familiar with detail).
- Head of IT (for Technology Recovery component).
- Head of HR (to ensure staff welfare is prioritised and also that plan familiarity is a contractual obligation).
- Head of Risk (to ensure investment risk is managed and contained).
- BCP Administrator (works closely with delegated plan owner - may be the Office Manager).

Consideration should be given to the co-option of other staff that are likely to be significantly impacted by a crisis, for example, the organisation's Head of Sales and Marketing to manage client communications.

Finally, depending on the size and nature of the organisation, it may also be wise to include external parties in the process (for example, the IT Infrastructure vendor, the Building Manager and the Prime Broker).

### 2.3 Business Continuity Team Composition

The Business Continuity Team is distinct from the Crisis Team. Its purpose is to prepare business continuity plans (including technology recovery) for the organisation and then embed it through training and testing.

It should comprise of a chairman, delegated plan owner and representatives from every department of the organisation. It should meet frequently during the initial preparation of the plan and then regularly thereafter to ensure the plan is maintained and organisational readiness is sustained.

### 3. PLANNING: BUSINESS REQUIREMENTS

This chapter reviews the steps that should be taken by the business, as distinct from IT, to compile a BCP.

#### 3.1 Business Impact Analysis

An important part of BCM is identifying the key business activities that must be sustained in the event of a disruption OR will become a requirement in the event of a disruption (for example, investor communication). These need to be agreed across the organisation to avoid conflict and confusion during a crisis.

The maintenance of these plans is the responsibility of the nominated BCP representative for each area, together with managing updates and coordinating testing. It is important to note that the BCP representative is not necessarily the manager or senior member of each team.

Only key activities on which the firm depends on a time horizon of a period less than one month should be included (so, for example, salary payments would be included but preparing annual financial statements would not). The assumption should also be made that the disruption occurs at an inconvenient time (for example, shortly before trades have been communicated to the administrator).

Finally, this exercise is NOT a substitute for documenting day-to-day procedures, which is outside the scope of the BCP.

The analysis should encompass:

- Organisational Areas (for example, Operations)
- Functional Areas (for example, the Risk Committee)

Organisations with multiple offices are outside the scope of this document. However, if they were within scope then geographical location would be a third dimension.

##### 3.1.1 Key Activities Template

The template should capture the following information for each key activity:

- Function
- Impact (High/Medium/Low)
- Required Recovery Time (Hours)
- Any Relevant Deadlines (Internal/External and Hard/Soft)
- Dependencies (Up/Downstream)
- IT Requirements
- Potential Workarounds
- Number of Full-Time Equivalent Staff (FTEs) required in recovery scenario.

##### 3.1.2 Hard Copy Records Required

Each area also needs to complete a template relating to hard copy records that will need to be stored offsite – either at another office location or at the relevant employee's home. These will need to be updated as required – and probably reviewed at least every quarter. This could apply to a document or another physical asset (for example SecurID card).

A more advanced plan could involve employees being given a sealed and dated envelope containing the relevant documentation. This would be exchanged every time the plan was updated.

### 3.1.3 Checklists

Each organisational area should also develop department-specific checklists for action during various outage scenarios.

### 3.1.4 Evacuation Plan

An evacuation plan, probably provided by Building Management, should be included in the BCP. This would include assembly points.

The organisation should have an appropriate number of trained emergency marshals and first aiders.

### 3.1.5 Staff Contact Details/Call Tree

A call tree should be included in the BCP. This states which staff should call which other staff in the event of a crisis being invoked. Due to both private data confidentiality issues and the challenges entailed in keeping up to date, staff personal contact details should not be published in a firm-wide BCP without staff consent.

Nevertheless, all staff should have mobile phone numbers and personal e-mail addresses of key colleagues stored at home in hard copy form and programmed into their mobile phones.

Commercial automated call tree management services are now a viable option for consideration.

## 3.2 Other Business Issues

### 3.2.1 Illness, Incapacity or Death

#### 3.2.1.1 Immediate Action

A combination of HR and trained first aiders need to be available for immediate action, depending on whether the event occurs at the office, away from the office on business, or at home.

Considerations can include the possibility of infection, and the fact that such events can be traumatic for colleagues as well.

#### 3.2.1.2 Key Person Provisions

As noted elsewhere, in the event of the death or incapacity of a “key person”, life/incapacity insurance and/or key man insurance can secure some financial recompense although this is frequently of little consolation. The precise circumstances will vary so widely dependent on the size and nature of the organisation, and the identity of the person incapacitated and the nature of the incapacitation, so that it is difficult to plan for all eventualities. However, the following should be considered.

- The lifestyle risks of the key people.
- Travel arrangements should be organised so that risk is minimised. It is wise for key staff to avoid travelling together. While air travel is relatively safe, the lack of communication can mean that no one is available to make investment decisions, should a market event occur.
- Risk appetite may vary, and while reducing exposure in a panic is rarely profitable, a fund may aim for a lower level of risk in times of uncertainty. Such strategies are best considered calmly before they are required in a crisis.

- If the incapacity is longer-term or permanent then all fund positions are likely to be unwound to cash as far as possible and investors offered the opportunity of an early redemption if feasible. The Risk Manager should supervise this process. Serious consideration should be given to winding up the business in an orderly fashion.
- Some investors may attempt to negotiate a “Key Man” clause when subscribing. This is where the impact on the plan needs to be considered at the time of subscription.
- Great care should be taken with communication - both internally and externally. Apart from the emotional impact, inaccurate communication may leave the organisation vulnerable to legal and/or reputational risk.

### 3.2.2 Insurance

Copies of insurance documentation should be held offsite.

### 3.2.3 Home working / Health & Safety / Regulatory Requirements

A fairly common contingency plan in BCPs, should the office become unavailable, is for staff to work remotely from home. Notwithstanding the obvious issues around loss of physical proximity, there are also other issues which should be considered ahead of time:

- Has the relevant regulator given any special dispensation to allow the organisation to operate in a decentralised way?
- How will requirements such as e-mail retention and telephone recording be fulfilled?
- Will employee homes be regarded as business premises by local government?
- Are there any Occupational Health & Safety issues involved with working from home?
- Do insurance policies remain valid for persons who wish to work from home?
- Will the worker be able to avoid domestic interruptions?
- Are security and confidentiality maintained?

### 3.2.4 Security

Organisations are particularly vulnerable to security problems in a crisis, and routine risk planning is inadequate, namely:

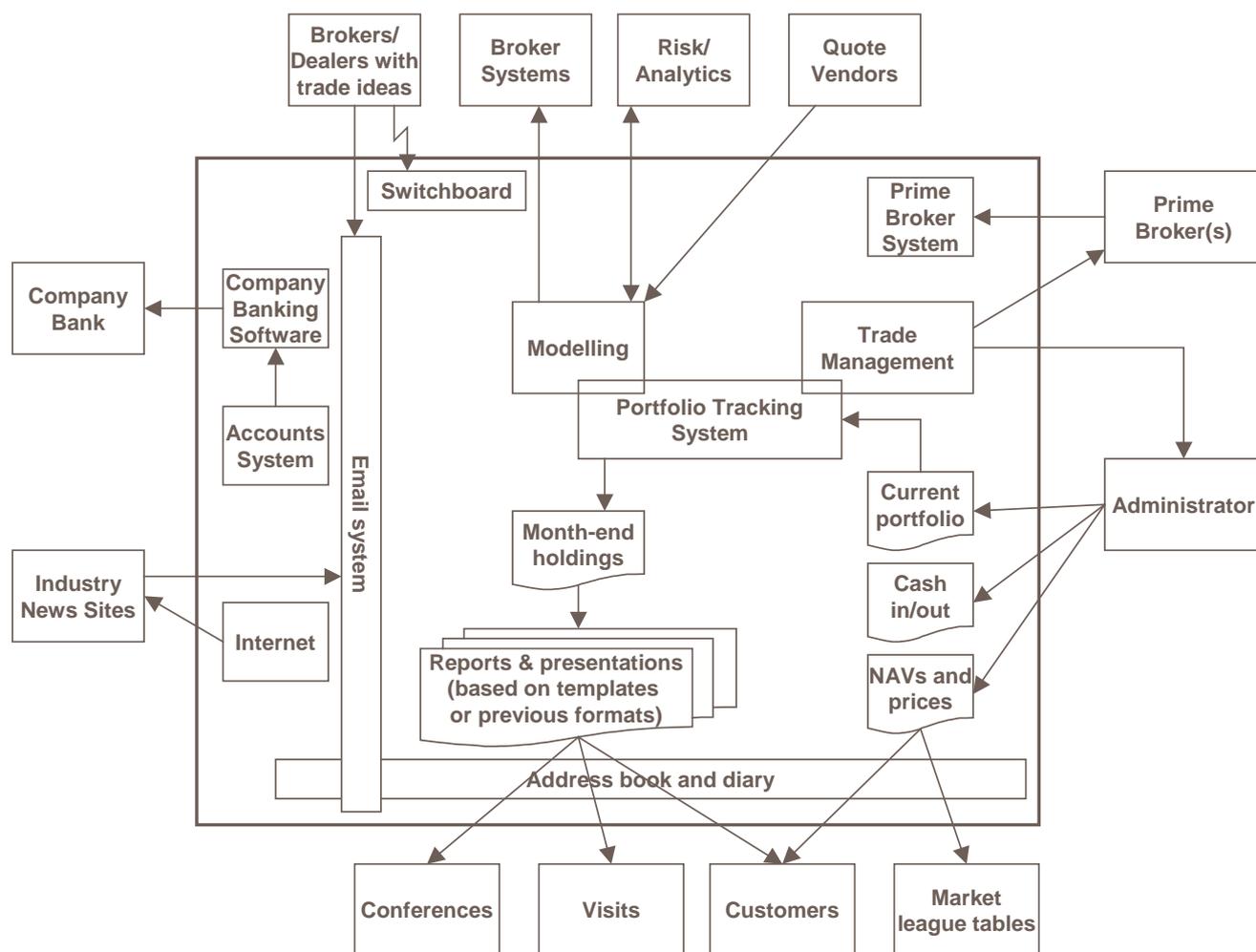
- Information may be stored and used in insecure locations.
- Unauthorised people may have access to buildings and systems without warning.
- A crisis can be created artificially in order to compromise security.

#### 4. PLANNING: INFORMATION TECHNOLOGY

This section of the Guide can be considered relevant to **Disaster Recovery Planning (DRP)**. A detailed analysis of DRP principles is beyond the scope of this document. If applicable, the IT Infrastructure Service Provider should build disaster resilience into their systems with well-worked fail-over and backup plans.

However, as a starting point it is usually 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:



Some of the questions worth considering would include:

- For each item entering or leaving the organisation, 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?
- How many simultaneous users on the VPN will be required in an emergency?
- 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, for example, statutory books and records?

This should give an overall understanding of the scale and quantity of systems and interfaces which need to be rebuilt in order for the company to function fully.

Resilience to technology problems is surprisingly easy, even for smaller managers, with laptops containing an integral UPS, wide availability of mobile broadband access, and broadband routers that fail-over seamlessly to high speed mobile internet.

Real-time backup of multiple servers to a single fail-over remote server is also increasingly cost-effective. Without such precautions, backup media needs to be transported physically at the time.

For telecoms fail-over, a full list of landline phone numbers should be maintained with the mobile numbers they should fail-over to. Conference call providers can be found on the Internet, which can host conference calls between large numbers of staff if it is not possible for them to physically gather together.

## 5. EXTERNAL DEPENDENCIES AND CONTACTS

### 5.1 Service Providers (SPs) and Other External Entities

A hedge fund or fund of funds does not operate in a stand-alone environment but is dependent on external service providers for many functions. Therefore the organisation is vulnerable to these service providers and need to understand the provider's contingency plans - and tailor its own accordingly.

On the positive side, service providers may be able to provide support and assistance to the hedge fund organisation (for example recovery of data, temporary office space, or outsourcing of functions).

A table should be maintained of service providers and should contain the following information:

- Name
- Contact Details
- Contact/Owner within Organisation
- Service
- Service Importance/Time Criticality
- Service Provider Contingency Plans
- Hedge Fund Contingency Plan to Cover
- Possible Assistance Available from SP in Event of Hedge Fund Crisis

For these purposes, service providers also include, for example, the organisation's regulator(s), the media and any other external organisation that may need to be contacted whether or not they are in a contractual relationship with the organisation.

### 5.2 Clients/Investors/Investees

A contact database of the organisation's clients, etc should also be available. However, due to reasons of commercial sensitivity it may be better that this is maintained separately rather than in the BCP. For example, if the Customer Relationship Management (CRM) database is regularly backed up remotely - and can be accessed remotely (for example, by the organisation's Head of Investor Relations) then this should suffice.

## 6. CRISIS SCENARIOS: RISKS, MITIGANTS AND OUTCOMES

Before focusing on how an organisation's BCP should be pulled together, it is useful to consider some of the generic threats that a business may encounter. These are discussed in the context of how these scenarios translate into a specific risk and how that risk can be mitigated. The following section applies these fairly abstract threats into practical impacts which can then be anticipated and planned for.

### 6.1 Scenarios, Risks and Mitigants

This section outlines a number of the most predictable business continuity scenarios resulting in business disruption. Inevitably, the list cannot be complete but any incident not covered is likely to be similar to one (or more) of those listed below and decisions can be taken accordingly.

We recommend that you use web searches for official guidance in drawing up your plans for different scenarios. For example, "What should I do in the event of a dirty bomb?" And your plan should include details of where to get up to date information at the time in the event of disaster.

#### 6.1.1 Large Area Explosion

A large area explosion is one that would destroy/seriously damage the office premises and other significant structures, for example, transport infrastructure and/or staff residential buildings. This could arise through, for example, a nuclear explosion (possibly as a terrorist attack) or a major bombing raid in the event of war (see below). While this scenario is, one hopes, unlikely, it is nevertheless possible. Risk mitigation really comes down to pre-emptively vacating the premises should a government agency so advise/instruct in the event of a warning.

#### 6.1.2 Localised Explosion

A localised explosion is one that seriously damages or destroys the office building and its immediate vicinity. Risk mitigation would include pre-emptive evacuation, as above, together with measures to reduce the effects of an explosion on the building (for example, applying adhesive film to the windows to hinder glass fragmentation).

#### 6.1.3 Explosion in Vicinity

An explosion in the vicinity is one that damages nearby infrastructure (for example, transport or utilities) and/or staff residential buildings - but not the office itself. However, a local police cordon could include the office building thus preventing staff from attending the office, or forcing an evacuation.

Mitigation would include invoking some of the general BCP provisions (for example, operate remotely).

#### 6.1.4 Radiological Bomb

A radiological bomb (often known as a "Dirty" bomb) involves a small-scale explosion but the release of a large amount of radioactive fall-out, forcing the evacuation of large areas. While there is some risk to human health, dependent on the prevailing wind, the epicentre of the explosion and the extent of the radioactivity, the largest impact would be economic - for example, large parts of central London could become uninhabitable so critically damaging the financial services industry and the broader economy.

While this threat may seem unlikely, it is one taken very seriously by security services.

### **6.1.5 War, Civil Unrest**

War or civil unrest covers a very broad range of scenarios and would almost certainly require a high degree of flexibility in response as the outcomes could cover one or several of the BCP outcomes listed.

### **6.1.6 Security Alert**

This would arise due to a bomb threat or similar. The likely impact would be the evacuation of the building and/or non-admittance for a period likely to be less than one day.

### **6.1.7 Gas Leak**

This may have a similar impact to a Security Alert (see 6.1.6)

### **6.1.8 Earthquake**

The likelihood of a significant earthquake is highly correlated to the geological conditions of the office location. Therefore the attention paid to this risk in planning would vary from extensive to none. For these purposes, an earthquake impact could be similar to a wide-area explosion.

### **6.1.9 Fire**

A relevant statistic is that a fire permanently closes 44% of the businesses affected. This is an area where effective business continuity arrangements will make a critical difference. The impact of a fire could involve damage, to a greater or lesser extent, to the office - at the minimum forcing an evacuation and likely seriously damaging the IT and telecoms infrastructure. It is also possible that the building could be left structurally unsound so preventing both the reoccupation of the premises and the retrieval of key documents etc. In most countries, mitigation of fire risk is embedded in relevant legislation.

### **6.1.10 Flooding**

As for an earthquake, risks vary considerably dependent on the office location - and also the floor of the building in which an office is located.

Floods can range from a tsunami, to the sea or a river bursting its banks, to a burst water pipe and therefore the commensurate damage can range from total destruction to a minor inconvenience.

Water damage can also occur through, for example, plumbing issues on higher floors and as a secondary consequence of a significant fire where water is used as an extinguishant by the fire service. This would be likely to exacerbate damage to the organisation's office and infrastructure.

### **6.1.11 Pandemic**

A pandemic is an epidemic of infectious disease that spreads through human populations across a large region, for example, a continent, or even worldwide. This is a serious risk, partly because the consequences are so unpredictable. Firstly, there is the possibility of staff becoming sick. Then there is the possibility of such a high proportion of the general population becoming sick that essential services start to break down (for example, transportation, power generation, food supplies etc.). It should also be noted that staff who are otherwise healthy may have to care for sick relatives and/or focus on securing essential food supplies and would therefore be unable to work. It is also likely that some, or all, service providers would be similarly impacted.

In this environment it is likely that staff would wish to (or even be forced to) work from home - however their effectiveness is likely to be limited due to the reasons noted above.

Mitigation would include acquiring a stockpile of surgical masks - and trying to secure supplies of any vaccine and/or drugs (assuming availability).

#### **6.1.12 Extreme Weather**

Very extreme weather could include a hurricane (for example, 1987 in London), very low temperatures, very high temperatures and torrential rain. This would be unlikely to impact the operation of the office directly - but would be very likely to disrupt staff transportation.

#### **6.1.13 Transport Disruption**

Commuter transport (and business trips) could be disrupted by adverse weather (see above), a strike, an explosion (see above) or technical failure. This could hinder a varying subset of staff's ability to get to (and from) the office. Mitigants could include booking hotel rooms near the office in the run up to, or during, a disruption.

#### **6.1.14 Accident**

An accident, whether in or outside the office, could result in the death or serious injury of one or more staff. Partial mitigants include life insurance policies for all staff, and key man insurance for senior executives. Nevertheless, if a scarce skill set becomes unavailable at short notice, this may cause disruption. This risk can be partially mitigated through cross-training (as for other Loss of Staff issues - see below). However the emotional impact on the colleagues of casualties is hard to mitigate for in the short-term.

#### **6.1.15 Electrocutation**

This is really a subset of "Accident" above - but may also have the side-effect of damaging the IT Infrastructure and so is included for completeness.

#### **6.1.16 General Power Outage**

A general power outage would be the failure of the national or local grid resulting in a power cut across a broad area, impacting both the office and local transportation - and conceivably the organisation's backup data centre, if any. Mitigation includes Uninterrupted Power Supply (UPS) - both desk and server-based. This will allow for an orderly shut-down of work and a head-start for the fail-over process, including backup generators (see below). The biggest issue here is likely to be when to commence fail-over given that it is likely to be hard to get information on the expected duration of the outage. Diesel generators may provide a medium-term solution.

#### **6.1.17 Localised Power Outage**

A local power outage is one that just impacts the building or, at worse, the local area. Therefore the impact is similar to the above other than it is unlikely to impact a backup data centre or transportation. Mitigation steps are therefore also similar to above.

#### **6.1.18 Circuit/Terminal Failure**

In the event of an individual PC failing, the damage should be confined to the loss of part of a day's work only, assuming that all files have been regularly backed up. Most firms should have a spare PC, already built to a basic configuration, which can be quickly substituted.

#### **6.1.19 Hardware Failure**

Computer hardware support arrangements should be in place, and a certain degree of resilience should be built into most systems.

#### **6.1.20 Virus/Hackers**

IT security should be treated as a significant priority and sensible precautions taken in conjunction with the IT Infrastructure Service Provider (ISP). Professional security firms can also attempt to penetrate IT security measures as part of a broader security audit.

#### **6.1.21 Theft/Sabotage**

This issue is also tied in with security - and ensuring that intruders cannot easily obtain access to office premises.

#### **6.1.22 Telecom Utility Exchange/Line Failure**

This includes lines that permit data feeds and internet access. Mitigation would include separate circuits and/or fail-over to mobile network(s).

#### **6.1.23 Telecoms Hardware Failure**

This should be covered by the telecoms service provider. Mitigation options include failing over to a mobile network(s).

#### **6.1.24 Local Mobile Network Failure**

Finally, there is the possibility of one or more mobile networks failing. There is a fair likelihood that this could happen at the same time as a major incident (for example, the London tube bombings). Mitigating options include using more than one provider.

### **6.2 Outcomes**

While it is very unlikely that any given crisis event can be accurately predicted beforehand, most events will feature a combination of one or more outcomes:

- timing;
- loss of building access;
- loss of staff;
- loss of IT; and
- loss of telecoms.

While not explicitly listed, attention should also be paid to the duration of transient events since brief events may require little action (although it is not always clear at the time of the event how long a transient event may last at the time - for example, a security alert). Previous experience has shown that organisations which pro-actively address disruptions - at the very least actively investigating and monitoring their status - have superior outcomes to those that adopt a more reactive posture. Therefore the chairman of the crisis management team should be advised as soon as any incident occurs where the duration is uncertain.

The final scenario to be considered is the failure of a key supplier - this is addressed separately.

### 6.2.1 Timing

This is a reflection of whether the event arises during or outside office hours (office hours defined for these purposes as when the building contains staff - which may be significantly beyond core hours).

### 6.2.2 Loss of Building Access

Loss of building access means that all staff within the building at the time of the incident must evacuate and all staff not within the premises will be refused entrance (this would include IT or telecoms contractors attempting to fix problems). In the event of a catastrophic failure (for example, an explosion) there is also likely to be a loss of staff (see below).

### 6.2.3 Loss of Staff

This covers all of injury, illness, death and inability to get to the office (or potentially get home) for staff and key contractors. More specifically, awareness of key man dependency is important. The other key factor to be aware of is that if the loss of staff includes fatalities or serious injury it is likely to have a very adverse impact on morale amongst the remaining staff - people who have lost a close colleague and/or are concerned about the safety of their families are unlikely to be in the right frame of mind to commence recovery and their duties will need to be re-assigned to less impacted colleagues. Longer-term, the provision of counselling and support for affected staff (perhaps all) should be offered.

### 6.2.4 Loss of IT Infrastructure

This includes partial or complete failure of the IT network, including hardware and operating software. The key factor here is to involve service providers at an as early stage as possible to instigate the IT fail-over to backup systems.

### 6.2.5 Loss of Telecoms Infrastructure

This includes partial or complete failure of the telecoms network (including equipment, land lines, mobile networks and the internet). In general, the contingency would be to use mobile networks if the land lines fail and vice-versa. If both fail then it is likely that the organisation's e-mail/internet would also fail.

## 6.3 Scenario/Outcome Mappings

The following table (on page 20) works through all combinations of the five variables listed above (variables which are extremely unlikely to arise or which are not feasible have been deleted). Examples of the types of scenario (6.1 above) that may result in these outcomes are also listed. Details of actions to take in the event of these outcome combinations are detailed under Crisis Management in section 7.

## BUSINESS DISRUPTION COMBINATIONS

During Office Hours?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N
Access to Office Lost?	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N
Loss of Staff?	Y	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N	Y	N	N	N
On-Site IT Servers Fail?	Y	N	Y	N	Y	Y	N	Y	Y	N	Y	N	Y	N	N	Y	Y	N
Telecoms Fail?	Y	N	Y	N	Y	N	N	Y	N	Y	Y	N	Y	N	N	Y	N	Y
Examples of Incident	Large Area Explosion	Explosion	General Power Outage	Security Alert	Electro-cution	Electro-cution	Transport Disruption	Localised Power Outage	Circuit/Terminal Failure	Telecoms Exchange/Line Failure	Large Area Explosion	Explosion In Vicinity	General Power Outage	Security Alert	Transport Disruption	Localised Power Outage	Circuit/Terminal Failure	Telecoms Exchange Failure
	Fire		Fire	Gas Leak			War, Civil unrest	Virus/Hackers	Hardware Failure	Telecom Hardware Failure		Radio-Logical* Dirty Bomb	Fire	Gas Leak	War, Civil Unrest	Technical Failure	Hardware Failure	Telecoms Hardware Failure
	Flooding		Flooding				Accident	Theft/Sabotage	Virus/Hackers	Local Network Failure			Flooding		Accident	Virus/Hackers	Virus/Hackers	Local Network Failure
	Extreme weather						Pandemic		Theft/Sabotage	Theft/Sabotage			Extreme Weather		Pandemic	Theft/Sabotage	Theft/Sabotage	Theft/Sabotage

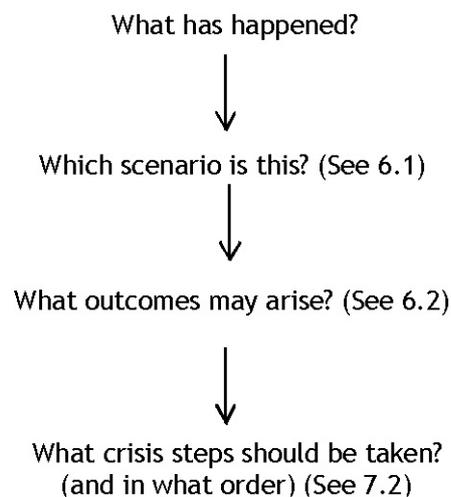
## 7. CRISIS MANAGEMENT

The previous sections have set out guidelines to plan for an incident requiring the BCP, and have described potential threats to the organisation and how these map to specific types of failure.

The following sections set out the processes for responding to incidents.

### 7.1 Decision Tree

The process flow for discussion at the initial Crisis Meeting (see below) is most easily set out as follows. If the event is a combination of scenarios then it should be adapted accordingly.



### 7.2 Initial Actions

The following steps (page 22) should be taken immediately following a business disruption event. Dependent on the event, it may be that the first actions will have to be: evacuation, the administration of first aid, notification of the emergency services and a roll call (see steps below). The Recovery phase is addressed in Section 8 below and Resumption in Section 9.

	Building Access Lost?	Loss of Staff?	Loss of IT Infrastructure	Loss of Telecoms Infrastructure?
Crisis Event	Y	Y	Y	Y
Initial Communication	Y	Y	Y	Y
Evaluation of Impact	Y	Y	Y	Y
Crisis Decision	Y	Y	Y	Y
Decision Communication	Y	Y	Y	Y
Evacuation	Y (if in office hours)			
Medical Assistance		Y		
Notification of Emergency Services	?	Y		
Roll Call	Y (if in office hours)	Y (in or out of office hours)		
Resumption of Initial BCP Meeting	Y	Y		
Redeployment of Staff	Y	Y		
Notification of Key External Parties	Y	Y	Y	Y
Commencement of IT Fail-over			Y	
Re-routing of Telecoms				Y

These action steps, in more detail, are:

### 7.2.1 Crisis Event

The event may be an immediate shock (for example, an explosion) or there may be some warning (for example, a transport strike). If it occurs during office hours the response will be different to that of out of office hours.

### 7.2.2 Initial Communication

The first actions to be taken by the staff member discovering the event are to arrange for the movement of staff in imminent danger to safety, and to notify the chairman of the Crisis Team.

### 7.2.3 Evaluation of Impact (Review of Scenarios)

If time allows, the CRISIS Team Leader will convene an immediate Crisis team meeting (dial-in arrangements if out of hours) to agree an immediate course of action. If there is no time, then one should move immediately to evacuation, including first aid, notification of emergency services and a roll call, before resuming the meeting.

If there is serious time pressure or a rapidly unfolding and/or potentially disastrous situation, this meeting should only take minutes. If the time pressure is extreme, the chairman of the Crisis Committee should have the authority to make decisions without consultation.

The crisis team's meeting agenda should focus on:

- What has happened?
- What are the immediate consequences/severity?
- How do we keep staff safe?
- What must we do NOW? Should we formally invoke a crisis?

During the meeting (and subsequent meetings) the questions "What if?" and "So, what?" should be asked.

### 7.2.4 Crisis Decision

While consultation is to be encouraged, at least to solicit information, the final decision as to whether to formally invoke a crisis should be the responsibility of the chairman alone. Decision making has to be swift, final and effective and it is for this reason that the chairman should have full delegated authority in the event of a crisis scenario.

The decision should take the form of a brief, simple scripted message. Staff must be instructed to leave their mobile phones switched on as a matter of course, and on their person, at all times until advised to the contrary.

### 7.2.5 Decision Communication

The immediate decisions taken should be communicated to the staff verbally in the office, outside the office or cascaded via the call tree verbally to any staff not in the office (or out of hours). The priority should be given to staff who will be most actively involved in the recovery scenario.

Every effort must be made to physically speak to the staff member concerned. If this is impossible, appropriate voicemails should be left and an SMS sent (including the instruction to call back on receipt) and assume that the recipient staff member will not be cascading the message and the originator will need to complete that part of the call tree on behalf of the (non-responding) recipient.

### 7.2.6 Evacuation

The evacuation should be organised by the nominated emergency wardens who will also liaise with the organisation's building management. When evacuating the building, consideration should be given to staff members or visitors who have disabilities.

If the event occurs during office hours, all staff should meet at the designated meeting point. In the event of a major problem or the cordoning off of a broader area, a secondary meeting point should be specified.

If possible, injured staff members should be moved to a location away from immediate danger. However, this must not compromise the safety of the staff member assisting.

If possible, staff (particularly the crisis team) should endeavour to take a hard copy of the organisation's BCP with them.

### 7.2.7 Immediate Medical Assistance

Once in a place of safety, appropriate first aid should be administered to any staff member (or visitor) requiring it. In the event of a large number of casualties, first aid priority should be given to the most seriously injured with the preservation of life the overriding goal.

### 7.2.8 Notification of Emergency Services

Appropriate emergency services must be summoned if required (Fire/Police/Ambulance etc.).

There is a growing international consensus towards using 112 as the emergency phone number - which should always work in the EU (incl. UK), Switzerland and on all GSM mobile networks. Otherwise, use 999 in the UK and 911 in North America. Other emergency numbers may apply in other locations.

Once paramedics have arrived (see below), a crisis team representative should liaise with them to, for example, to discover which hospitals the staff members are being taken to and ensure that all staff members who need treatment receive it. Similarly, a crisis team member should liaise with the other emergency services. Instructions received from fire department officers, police or ambulance services must be followed.

### 7.2.9 Roll Call

The emergency wardens will take a roll call of all staff and visitors believed to be on site from records as far as they can be recovered and advise the emergency services of anyone who is missing.

### 7.2.10 Recommencement of Initial Crisis Team Meeting

Once all staff are safe (or receiving medical treatment) and accounted for, the crisis team should reconvene their initial meeting, if required, to agree next steps. All other staff should remain on standby at the location.

### 7.2.11 Re-Deployment of Staff

The crisis team should then communicate next steps. These are likely to include:

- Staff to return home. They will be advised when the backup servers are likely to be available (if applicable). Some staff may be relocated to overseas offices or to other locations in the UK. This will need to be with their agreement.
- A reminder to keep their mobile phones switched on, charged if possible, and on their person.
- Advice of the next communication (likely to be the conference call the following morning, if not sooner).
- Selected staff, required to commence the recovery, should then be kept behind for more detailed discussion and advice.

### 7.2.12 Notification of Key External Parties

Dependent on the precise circumstances, initial notification should probably be made to the organisation's IT and Telecoms service providers (if not already done so), building management, regulator(s) and other key service providers (for example, the prime broker and administrator). Care should be taken to agree on a measured and consistent message that is to be delivered to all parties, as any external message may, inadvertently, end up in the media or otherwise in the public domain.

### 7.2.13 Commencement of IT Fail-over

If applicable, and in conjunction with the organisation's IT service providers.

### 7.2.14 Re-routing of Telecoms

If applicable, and in conjunction with the telecoms service provider, the organisation's crisis team should request the forwarding of all incoming calls to the individual staff members' mobiles, including the forwarding of calls from the organisation's main telephone line.

## 7.3 Crisis Management

After following the decision tree above, the outline of immediate steps to be taken should be reasonably clear. However, the magnitude of the event (and whether or not it is transient) also needs to be considered at this stage.

In essence, the first key point to address is whether the crisis team should meet first, or whether the building should be evacuated (with associated actions) first. This decision will almost certainly be governed by circumstances.

Once the crisis team does meet (with backup attendees if appropriate) it should move rapidly to a decision. The first meeting should focus on the first few hours only:

- Staff safety
- Instigation of recovery
- Urgent external communications.

As soon as the initial steps have been executed the meeting should reconvene to start to focus on the recovery in more detail (see Section 9 below).

## 7.4 IT Disaster Recovery/Fail-over

After determining the need for IT fail-over, the crisis team should work with the organisation's infrastructure provider to ensure that any mission critical applications and hardware continue to operate via backup/secondary means. These include:

- organisation's e-mail server;
- organisation's main servers;
- organisation's remote access to systems.

Hard copies of all portfolio holdings, major financial statements, external parties and all other documents deemed essential to normal business operations should be securely maintained by appointed staff. (See Section 3).

## 7.5 Telecoms

In the event of a telecoms fail-over being required, the provider should be instructed to begin diverting e-mail and data/communications lines.

## 7.6 External Communications

Managing external relationships during a business disruption is critical for the short and long-term prospects of the organisation. In the short-term, critical suppliers must be advised so they can adapt their processes to take account of the new circumstances. It may also be necessary to retrieve certain data from them which may have been lost during the disruption. For the longer-term, providing clear, honest, timely and consistent communications to clients and the media should go a long way to sustaining confidence in the organisation as a going concern.

As part of the output from the organisation's crisis team meetings, a script should be agreed for both internal and external communications. It is very important that external communications are consistent since confusion will result in confidence being lost rapidly by the outside world.

Finally, staff members who are not part of the communication process must refrain from external communication - and refer any query to the designated spokespeople.

### 7.6.1 Service Providers

The focus of the messages to critical service providers should be practical. The staff member owning each of these relationships must also have account numbers, security certificates, passwords etc. to hand.

### 7.6.2 Clients and Other External Parties

Communications to clients and the media are not particularly significant in the context of crisis management, recovery and resumption, but are critical in terms of protecting the organisation's franchise - assuming that the business disruption is of any significance. The focus of the message should be 'CARE' - Concern, Action and Reassurance - and should be carefully scripted and consistent across recipients.

In the event of a major incident, a press release should be considered.

A log of communications is also extremely useful, to ensure that efforts are not duplicated or inconsistent.

Finally, if applicable, the organisation's website should be updated with a message on the home page and, again if applicable, appropriate social media broadcasts made.

## 8. RECOVERY

The recovery phase commences once the initial crisis has been addressed - i.e. staff has been relocated, IT fail-over has been completed, key external parties have been notified, etc.

### 8.1 Internal Communication

In the aftermath of a crisis, communication requirements may be very fluid, so there will be many ad hoc communications and decisions, but it is important to ensure that formal collaboration is maintained, to help ensure that nothing is overlooked.

#### 8.1.1 Crisis Team Daily Calls

The crisis team should have at least one daily call. This would typically take place at 9am local time, with others scheduled as required. In the early days following an incident a 4pm call may also be advisable.

A dedicated conference number for these calls should be established ahead of time with the telecoms provider.

The baseline agenda will likely comprise the following, although this will evolve over time:

- Roll Call
- Status Check (including actions to move to necessary backup environments)
  - Staff wellbeing
  - Physical premises
  - IT Infrastructure
  - Telecoms
  - Other issues
- Business Continuity
  - Ability of departments/functions to continue key activities (for the staff calls below, each area should be prepared to make a brief update)
  - Upcoming business issues that require attention
  - Risks
- Communications
  - Internal
  - External, including public reaction to situation
- Recovery/Resumption Planning: Tasks required (including owners, timelines)
  - Staff wellbeing
  - Physical premises
  - IT Infrastructure
  - Telecoms
  - Other issues.

Minutes and an action log (task/owner/deadline) should be maintained and circulated following the meeting and prior to the next meeting.

#### 8.1.2 Staff Daily Calls

Daily, typically at 10am local time, all staff will be expected to dial in to a call hosted by the BCP chairman to run through a condensed agenda based on the BCP call at 9am (i.e. outcomes only, not discussion) and to solicit any questions, feedback or problems from staff members.

Once again, the dedicated number should be used.

Minutes/Actions should also be maintained by the BCP Administrator/BCP Owner.

## **8.2 Initial Recovery Actions**

Following the crisis event and movement to a fall-back infrastructure (details dependent on the circumstances of the event), the following additional tasks should be undertaken:

### **8.2.1 Risk Committee**

The risk committee should also meet as early as possible to consider the impact of the incident on the firm's portfolio of risks (market, operational, credit etc.) and where necessary, take appropriate action.

### **8.2.2 Investment Committee**

The organisation's chief investment officer and risk manager should jointly convene an early investment committee meeting to determine whether all necessary portfolio information has been secured. Missing or corrupted data should be reposted to the crisis team. The investment managers and risk manager should also decide whether investment actions are required although discretionary trading should be minimised to the extent supported by the organisation's operations.

### **8.2.3 Operations**

The organisation's operations department should continue to keep the fund administrator, prime brokers and other key operational service providers apprised of the situation.

### **8.2.4 Internal IT Systems**

The organisation's Head of IT should report to the crisis team the current status as needed and at least daily prior to the crisis team's morning meeting.

### **8.2.5 Other Infrastructure Functions**

Representatives from these teams will already be directly involved in the recovery process - and need to ensure that their colleagues have access to necessary information.

### **8.2.6 Business Functions**

Team leaders of the organisation's respective team lines need to focus on ensuring that their staff has access to information prioritised in the impact assessments.

## **8.3 Coverage of Critical Functions**

All functional areas should have previously identified their critical activities and their key staff required. These critical functions should then be carried out with any issues escalated to the crisis team as they arise. Additionally, a brief report from each area should be made at the daily staff meeting outlining progress and issues.

Staff not involved in critical functions should remain on standby and, if IT capacity allows, continue with their normal work.

Additionally, some staff may be required to work towards preparing for a resumption of normal business activities. These will be assigned by the crisis team in consultation with line management.

## 8.4 Data Management

### 8.4.1 Migration of work carried out during the crisis to core systems (or backup)

Some urgent work may have been carried out by the organisation's staff from home prior to the establishment of the backup infrastructure. In this case, files should be transferred to the backup network servers as soon as practicable.

### 8.4.2 Data Backup in Recovery Environment

In order to ensure that the organisation does not remain vulnerable to further disruption affecting the backup servers, some staff may be authorised to backup key files so secure drives of their laptops or home desktops - and periodically to encrypted flash drives.

## 8.5 External Communication

Key external stakeholders should continue to be kept updated regularly - in particular, the appointed communications representatives should ensure that external parties' expectations are managed (for example, if the organisation promises "to call back in two days", that happens) and their concerns addressed.

## 8.6 Rectification/Contingency Scenarios

### 8.6.1 Access to Building

It is highly likely that if the building is evacuated, or access is denied, that certain key documents or hardware will be inside and non-retrievable. In these instances, it may be possible to gain entry through negotiation with building management and the emergency services for that specific purpose, dependent on the circumstances and ensuring staff safety remains paramount. However, NO staff member should attempt to gain access without the prior agreement of the authorities and in conjunction with the Crisis team.

### 8.6.2 Alternative Accommodation

If the building is very seriously damaged or destroyed and it is clear that re-occupation will not be possible in the near future (or even at all) then an urgent priority is for alternative accommodation to be sought. Staff members who are not otherwise engaged in critical activities could be seconded to this activity.

The most likely option is serviced space which could be available within two to three weeks (but would also need installation of IT equipment).

Another shorter-term partial solution would be for two or more employees to work from a single location (for example, a staff member's home, given space and technology access).

Finally, it may be possible to get desk space at a service provider on a short-to-medium term basis.

### 8.6.3 Redemptions/Returning Funds

In very adverse situations, some investors may request early redemptions. This should be at the absolute discretion of the Fund Directors working with the investment manager and will clearly also depend on the organisation's ability to liquidate its underlying holdings.

In an extreme adverse situation (for example, the death or long-term incapacity of several key people), the best solution may be to wind down the firm in an orderly fashion and ultimately return funds to investors. Again, this would be at the absolute discretion of the Fund Directors working with the investment manager.

## 9. RESUMPTION

Resumption is the third key phase of a business continuity event. It is the transition from working in 'Recovery Mode' to 'business as usual' - therefore this is effectively a project.

Since time pressures should be easier at this stage, the BCP can be far less prescriptive. Therefore, this guide will be restricted to a series of check points within which the crisis team and management can determine the optimal course of action. However, it is recommended that a specific project team, probably comprising many of the same members as the crisis team, be tasked with managing the change.

As a project, tools should include a "ganttt" chart, defined tasks/checklists, assigned roles and a clear timeline. If the office is being re-occupied or the organisation is moving to a new office then the closest analogy would be to an office move project.

- Matters to be aware of include:
  - 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 does the organisation become compliant again?
  - Have clients been updated for transactions or conversations that may not have been captured via the normal methods?
  - Have investment decisions been correctly documented and passed by the appropriate investment committees?
  - Have clients and other external parties (including the regulator(s)) been informed that the organisation is changing its mode of operation, ensuring they have full contact details and are ready to resume full business?
  - 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 stored locally during the crisis or recovery phases into business as usual systems?
  - Is there a data synchronising test to ensure there is a clear and agreed starting point for business resumption?
- Will the organisation be moving to a new office?
  - Which contracts, stationery or other documents need to be updated?
  - Have staff been fully briefed on any new office specific issues?
- As with many projects, a fall-back position in the event of difficulties should be considered ahead of the transition.
- Finally, the BCP will need to be updated to cover the new building (lightning may strike twice...).

## 10. MAINTENANCE

The BCP needs to be updated at least annually, and more frequently if there have been any significant changes in the business, notably:

- Organisational changes
- Personnel changes
- New or changed business processes
- Office moves
- Changes to personal details (for example, phone numbers)
- Upgrades or changes to IT Infrastructure or systems

Furthermore, the BCP should be tested at least annually. These testing episodes should incorporate training opportunities. Further details of this are included in the next session.

## 11. TESTING AND TRAINING

Testing the BCP is essential to ensure that it works reasonably well, should it ever be needed. Due to the varying scenarios, different types of tests need to be designed. All of these should be carried out at least annually.

Therefore, testing should consist of the following scenarios which need to be carried out in sequence over a period, since it is virtually certain that issues will arise at each stage that need to be addressed, possibly necessitating a re-testing of that phase, before it is safe to move on to the latter stages.

Staff training is embedded within the testing. The only additional training required would be a classroom session for all staff to run through the BCP at the time of publication. To aid recall, key parts of the BCP can be printed on a laminated credit-sized card for all staff.

It is not necessary for all staff to know the full BCP Plan. Providing the decision and communication trees are well organised, a good test of preparedness for many staff is often limited to questions like: "Who would you call if you were prevented from entering the office area?" and "What would you do if there was a fire, or other evacuation?" However, senior managers need to be conversant with the plan, to have tested it, and for the most part, to direct operations without reference to the plan.

### 11.1 Telephone Call tree

The organisation's crisis team leader would commence the test (without advance notice) out of hours, imparting a code word to the recipients of the call. The next working day all staff would be asked to report back the code word. This tests the viability of the call tree and also that phone numbers have been accurately recorded.

### 11.2 Remote Connectivity

All staff should log in to the network from home and check that all key systems are functioning and available remotely, including vendor software. This also tests that all staff actually have functioning VPN remote access.

### 11.3 IT Fail-Over

Over a weekend, the IT service provider would switch over to the backup system and all staff would attempt to log in to that, testing key applications etc. as above. Later in the weekend they would switch back to the primary system (so also testing a key part of the resumption process).

### 11.4 Telecoms Fail-Over

Over a weekend, all landlines would be diverted to staff mobile phones and then these would be tested via a call-tree to landlines. Then switch back (testing another resumption process).

The diversion needs to be directed from a location outside the office, and effective at the exchange.

### 11.5 Full Test

On a given work day (flagged in advance so as to avoid key meetings, possibly on a day when a key market is not open), the IT Infrastructure would be powered down in the early morning then flipped to the backup system; phones would be diverted to mobiles and no staff (including IT Infrastructure and other suppliers) would be permitted on site. All staff would work from home (or a hot site, if applicable) - prioritising identified key tasks from the Business Impact Analysis. The crisis team would actively manage the test, organising conference calls as planned, etc. At the end of the day, the IT and Telecoms primary systems would be restored. On T+1 all staff would need to check that all files etc. have been appropriately saved back on to the primary servers. This will also test

whether hard copy documents etc. were available, contact numbers were accurate (in part), key tasks had been correctly identified etc.

### **11.6 Advanced Testing Options**

The first option would be to carry out a full test, as above, but not announce it in advance. Rather, the test would be instigated by the BCP chairman early in the morning.

The second option would be to carry out a full test, as above, but taking out various key members of staff to check cross-training and resilience of procedures etc.

Scenario testing can be a valuable way of observing how individuals perform under the simulated pressure of an event and how the team operates as a group under pressure.

### **11.7 Other Testing**

Other more IT specific testing should also take place periodically (for example, switching off the power to test the UPS).

## 12. STAFF OBLIGATIONS

Staff obligations in respect of business continuity should be set out clearly - either in contracts of employment or the HR handbook. Obligations should include:

- Keep an up-to-date hard-copy version of the BCP or relevant instructions both at home and in the office.
- Have the mobile phone numbers of the BCP chairman, their immediate colleagues and line manager programmed into their own phone.
- Have the conference meeting phone number (with passcode noted somewhere easily accessible) programmed into their own phone.
- In general, have computer and internet facilities at home(s) enabling them to access VPN at short notice (i.e. leaving their laptop in the office overnight is not an acceptable policy).
- Test periodically their ability to access both the main and backup servers via VPN.
- Maintain a clear desk policy - stored paper files are generally much safer than those left in the open in the event of a fire or theft for example.

Staff who manage the firm's relationships with service providers should also have their relevant phone numbers programmed into their phones.

### 13. APPENDIX - OTHER RESOURCES

Inclusion of an organisation or web site in this document does not imply an endorsement. AIMA takes no responsibility for the content of these sites.

[www.sans.org](http://www.sans.org)

The SANS Institute provides a vast selection of white papers relating to technology security, including guides to business continuity planning.

[www.drj.com](http://www.drj.com)

Disaster Recovery Journal is a commercial publisher of a disaster recovery magazine, but provides free resources such as sample plans and white papers.

[www.thebci.org](http://www.thebci.org)

The Business Continuity Institute is a forum for business continuity networking and thought leadership. It publishes a lengthy set of Good Practice Guidelines for a fee.

[www.drii.org](http://www.drii.org)

DRI International is a non-profit organisation promoting business continuity and disaster planning through education, assistance and publication of a range of resources.