

Business continuity guide for small businesses





Contents

Introduction	4
Demystifying risk analysis	6
Frequently asked questions	7
Case study scenarios	8
A guide to successful business continuity planning	11
ROBUST New business continuity planning software tool launched	18
Sample business continuity plan	19

This information, including documents and any discussion surrounding them, is provided for illustrative purposes only. It is provided on an informal basis for the information of the named intended recipient only as an example of how AXA approaches its own contingency business planning. The information documents have been prepared following AXA's interpretation of contingency business planning practice for its own internal purposes. The information and documents are confidential and may not be passed by the intended recipient to anyone else.

The intended recipient must not rely on the information, but must consult a professional adviser about the suitability of this information. AXA cannot accept any responsibility for any loss incurred by the intended recipient or any other person arising out of the use of the information whether such loss arises by reason of the negligence of AXA Services UK plc or its servants or agents or otherwise howsoever. © Photos: Getty Images and Jacques Grison.

Introduction

The first decade of the 21st century has firmly established the importance of having a business continuity capability. Recent events, including the recession, severe snowfall and swine 'flu, have increased the challenges for maintaining business continuity capability. We continuously have to re-appraise our plans to cover new and unexpected disruptions.

But what does having a business continuity capability mean? Organisations need to understand which of their processes and resources are critical for their survival and put arrangements and plans in place to ensure that they are protected, whatever disruption occurs. The effort required to achieve this is likely to be commensurate with the size and nature of your organisation and doesn't need to be overly complex. You need to be confident that you can continue to service your customers, pay your suppliers and look after your stakeholders, from your staff to your shareholders. And of course there are tools to help you. An example is the new free to use BCP tool, Robust (launched via FPA and RISC Authority), which demonstrates the support insurers are giving to business continuity management.

So if you haven't already done so, now is the time to start – when an unexpected event occurs, make sure that you are not the organisation that doesn't survive.

Angela R. Robinson

Angela Robinson FBCI
Chair of the Business Continuity Institute
www.thebci.org





“ As one of the largest insurers of small businesses in the UK, AXA knows all too well the disasters that can affect SMEs – driven by issues ranging from crime, fire and flooding, to computer failure and legislation. We have seen first hand the long-term effect of business disaster – as a high proportion of businesses affected by a major incident either never re-open or close within 2 years.

It is essential that you have a Business Continuity Plan in place and your employees are aware of it. A continuity plan fits in with your business so it need not take a lot of time to complete. We have produced this guide to help you write your own continuity plan.”

Douglas Barnett
Head of Customer Risk Management, AXA

More information on
business continuity
is available on:

www.axa.co.uk/axa4business

Demystifying risk analysis

Businesses are operating in a world full of risk and uncertainty, yet the identification and management of risk is still often poorly understood. Most companies will survive if they ensure risk management is central to their business ethos and updated regularly, in line with their business plan and mission.

Any number of incidents can bring businesses grinding to a halt, and simply getting back up and running is not where it ends. For this reason, when planning for serious incidents like fire and flood it is critical to look beyond the basics. Effective business continuity planning should look at every possible impact on the business, from stock losses, impaired transport and communication links to damaged customer relationships. For small businesses, the impact of the potential risks mentioned is likely to be more destructive as the majority operate in specialised markets and any short interruption to normal business can have a disproportionate effect – totally halting output and letting customers down. In addition, it is more difficult to absorb the financial impact of business interruption, making it hard to recover even after returning to normal operations.

AXA understands that many small businesses don't have easy access to basic information about business continuity planning.

We've addressed the most frequently asked questions on the next page.



Frequently asked questions

What is business continuity planning?

Put simply, business continuity is about anticipating the crises that could affect a business, and planning for those crises, making sure that the business can continue to function in the event of an emergency.

What is a business continuity plan?

A Business Continuity Plan sets out clear roles and responsibilities, for example those assigned to manage all liaison with customers, employees and the emergency services. It lists a series of contingencies that enable key business activities to continue in the most difficult circumstances, for example when a vital computer system or other equipment is unavailable. Importantly, it also details clear emergency procedures to ensure that the safety of employees is a top priority.

Because it requires an assessment of all critical areas of a firm, business continuity planning is a valuable management tool.

Why should small firms care about business continuity planning?

Business success is as much about protection as growth. In an uncertain world, that means creating a business with the flexibility to prosper in changing conditions and strong enough to survive should a disaster strike. The ability to withstand serious incidents like flooding and fire, and quickly re-open for 'business as usual' is critical. There is also the commercial benefit to consider, as companies with business continuity plans are more attractive to do business with. For example, large businesses that rely on the outsourced services of third parties will prefer to work with suppliers who have a Business Continuity Plan in place.

How does business continuity planning differ from a disaster recovery plan?

Disaster recovery plans traditionally focus on the IT recovery of the business such as tape backup systems, storage systems, and hot sites. A Business Continuity Plan will address all the requirements essential to keeping the business running and includes processes to keep disruption to customers and employees to a minimum. In short, it is about ensuring that a crisis is managed effectively before it escalates to a disaster.

Case study scenarios

Putting business continuity planning into context

The first step in creating a sensible business continuity process is to consider the impact of any potential disaster and the effect of each on your business – this is critical if you are to plan properly. If you have little idea of the likely impact on your organisation then it is impossible to be prepared. Below are a series of scenarios and hypothetical situations to give you an idea of what can go wrong if you do not have a plan in place.

1. Sector: Retail Risk: Telecom/IT Failure

Company A is a busy independent travel agency relying on telephone and IT systems to provide its customers with the same service as the major travel groups. In January last year, a key trading period for travel agents, the telephone and IT systems failed due to a power cut. The council was resurfacing a road near the premises and cut through a power supply cable affecting one side of the high street for three days.

Company A relies on phone and IT systems to confirm prices, check availability of holidays and flights and complete currency exchange transactions for its customers. As a result, the travel agency lost considerable business to competitor agencies including one contract for a business account with a large manufacturing business in the town.

Customer loyalty and repeat business are very important in what is now an extremely competitive industry. Company A suffered from negative customer experiences and lost its most profitable customer.

Douglas Barnett

Head of Customer Risk Management, AXA

This is a classic example of not being prepared and thinking that ‘it won’t happen to me’. This scenario shows how planning before an event can allow a business to react quickly to interruption. Having the foresight to discuss reciprocal agreements with other independent travel agencies would have allowed for staff to utilise their mobile phones to check availability of flights/holidays and process bookings through the alternative agency in the short period.

Company A was lucky that this was not a long-term disaster, and that power was restored after a few days. Had it been a fire or flood the business could have lost considerably more customers. The travel company suffered a serious setback as a result of damage to its reputation which might never be restored. If Company A had the foresight to make reciprocal arrangements with other local travel agents its key customers could have continued to make bookings and passing trade would not have been lost to the national travel chains. A disaster can happen to any company, big or small, and it is important to be prepared for every eventuality.

2. Sector: Manufacturing Risk: Fire & key equipment failure

Fifteen years ago a food-processing company was ravaged by fire, but the owners were lucky enough to be able to rebuild and start again. The business went on to trade successfully for many years in a traditional brick building. Changes in environmental health regulations forced the company to improve its process and storage areas. The guidelines stated that the business needed to create a 'food safe' structure within the factory, by using insulated sandwich panels. The sandwich panels are comprised of two thin sheets of metal with a core consisting of a combustible insulation material – to form rooms within the original building. A few weeks later, a contractor was employed to fit a safety handrail to an elevated platform. While welding, sparks ignited in the combustible core of a sandwich panel adjacent to the work area. The fire spread rapidly through the combustible insulation within the panels, causing the internal structure to collapse and the building was completely destroyed. This time, the owners lost a major retail customer and the business never reopened.

Douglas Barnett

Head of Customer Risk Management

The alterations to meet revised environmental health requirements changed the physical structure of the factory considerably. The owners made one very large and fatal error – they forgot to align their risk assessment intelligence with the newly built factory. The risks faced by a business are transformed as the business changes. Every time you update your business or premises, make sure your plans and processes reflect these changes. For example, consult with insurers when undertaking structural changes to your business premises – they may be able to assist in the specification of appropriate materials that in the long term will protect the business and control premium levels. Understand and control the risks posed to your business by third party contractors – hot-work permits can be used to control contractors. Reevaluate your overall risks regularly to ensure you stay one step ahead at all times.

3. Sector: Service (Sales Industry) Problem: Unable to access business premises

Company X is a market research firm that relies on its telephone systems to conduct business and communicate with clients. On a day-to-day basis employees are constantly using the telephone conducting market research surveys to fulfil client requirements. In October 2008 a fire broke out in the building next door to Company X on the industrial estate where it is based. The fire caused considerable damage to the adjacent building and because of the Fire & Rescue Service's need to ensure the area was safe, all the company's employees were denied access to the building. As all the information and materials needed to run the business were held in the office, the company had to send all employees home. The company could not access their telephone systems, databases, key telephone numbers and had nowhere for a core team to work. It took them the better part of the day to alert their key clients and they failed to meet a large deadline with a very important client.

Douglas Barnett

Head of Customer Risk Management

Here is an example of the need to have a plan in place with preparations for all eventualities. Company X did not have the essential off-site Business Continuity Plan which would include the disaster recovery pack and access to an off-site location where important data was stored, including key contact details of all customers and suppliers. The plan would also include a designated recovery site with telephone and IT systems that could be up and running quickly so it could resume a 'business as usual' status to meet client demands and expectations. Company X needs a Business Continuity Plan to ensure this does not happen to them in the future. It is then essential for several key members of the senior team at the company to know about the plan and be clear of their individual responsibilities in terms of implementing it when needed.

4. Sector: Service Problem: Health issue

Company Y is a medium sized, regional, graphic design company based in Manchester with 50 employees. In March 2004, one of its managers unknowingly contracted Tuberculosis (TB) and came into work feeling unwell. After having the illness diagnosed by his doctor, the manager was advised to notify immediately anyone with whom he'd been in contact over the past three days. He was told that his team must be tested for the disease straight away as he had been working in very close proximity to them over the past week on a project that was due to launch that week. After taking medical advice that confirmed that TB is highly contagious and potentially very dangerous, the MD of the company was forced to quarantine and send home key team members who had been in contact with the manager with immediate effect. Temporary employees were bought in to cover essential work requirements on the project but they could not access the systems used at Company Y. There was no one to show them how to use the systems and as key members of the team were not in the office it soon became clear that there were certain aspects of the project that only they knew about. The client did not react positively to having to deal with new contacts unfamiliar with their needs and requirements. Consequently work was delayed and the company was unable to deliver the project on time, which seriously affected its relationship with the client and the prospect of future work for Company Y.

Douglas Barnett

Head of Customer Risk Management

This scenario shows the importance of having a plan in place for action when key employees are unavailable. The company needs a manual on how to operate all the systems so any temporary or new member can join the team and start work quickly. This would form part of any continuity plan. It is also important that all teams be updated on all the work in progress so they can join critical projects when needed and client deadlines are met on time. There will always be a varying degree of skills within any team. We advocate cross skilling teams to ensure the work continues to flow in the absence of one or more team members. These actions will serve to protect and preserve the company's reputation when it is most important.



A guide to successful business continuity planning

Spending time developing a Business Continuity Plan will not only increase the likelihood of your company's survival following a crisis or business interruption, but will also ensure the safety and protection of your biggest asset, your people.

The main objective of the plan is to recover all business critical processes and minimise the impact for your employees, customers and your reputation.

Implementing a plan is essential to every business, but many don't know where to start. It requires careful preparation and planning. Appointing a business continuity project manager, who will ensure that a Business Continuity Plan is created, developed and maintained is the best approach.

The business continuity project manager's role is to ensure all the steps outlined in this guide are followed and the plan is updated on a regular basis.

Step one: Basic emergency procedures

Before you begin work on a Business Continuity Plan check that you have in place the following emergency procedures. Please note: these are all part of essential Health and Safety Legislation and are a legal requirement for any UK business.

It is essential that all businesses have and follow basic emergency procedures to ensure safety at all times:

- Make certain your employees understand the evacuation procedures
- Make sure your employees really know what to do if a fire breaks out
- Ensure your employees know what to do if a colleague is injured
- The key to a sound emergency procedure is clear process, clear roles and responsibilities and employee awareness. A clear evacuation process should be in place, with team members from each department given responsibility for ensuring a smooth and orderly process.

All employees must receive training on your emergency procedures, with regular updates and refresher courses about this. It is also important that your workforce know where to access a 'guidelines and procedures' document to ensure that they are always fully aware of what is expected of them.

Step two: Define your disasters and assess your risks

It is vital to remember that a disaster could happen to any company – no matter the business size, be it a multinational company or a small business. Before looking at risks in individual areas of the business, it is important to determine what would constitute a disaster. In simple terms, a disaster is an incident that has serious consequences for the business.

Common small business disasters include:

- Fire/flooding
- Computer/telecoms failure
- Key equipment failure
- People issues such as illness/resignations/maternity leave
- Denial of access to the premises
- Product defects
- Bomb/terrorism threat
- Legal/regulatory action
- Utilities failure

It is critical that you understand the disruptions that would be disastrous for the running of your business when writing your plan. Take the time to identify all the risks your business faces and then rank them in order of likelihood and importance.

Step three: Secure your business, bit by bit:

Thoroughly assessing the disasters that could threaten your firm will give you a clear idea of the business areas that are most important to secure. Usually, these will be the areas on which your business relies the most, and which are exposed to the greatest degree of risk. This is the most important part of your plan.

The following check points are essential when writing this stage of your plan. You need to systematically go through each of the following areas and take a practical approach to tackle each of the threats that your business may face. Follow the same process for each:

1. Assign ownership
2. Identify threats and resources
3. Develop contingency plans and policies.

Premises and key equipment

Clearly, your premises are fundamental to your business. So much so that you probably take them for granted. But have you ever considered the long-term impact that damage to or destruction of your premises would have on your business?

The same applies to business critical machinery. If a vital piece of equipment is destroyed, damaged or stolen, what impact would it have on your business? Ask yourselves the following questions:

- Would you be able to inform your employees and customers of disruption to the business?
- What would happen to customer orders due during the time that your premises were closed?
- Would you be able to make alternative arrangements for regular orders, to keep loyal customers happy?

The Business Continuity Plan will ensure you are prepared for the worst situation that would keep your business from being operational.

Review the plan at least every six months. Check to see the plan includes all the correct contact details for employees, suppliers etc.

People

The loss of key people and injury to employees is a risk that many businesses overlook. In the end, the success of any company is determined by the skills of its people. Your people are your most valuable asset. Think about how your business would cope in these situations:

- If three members of your team went to work for your major competitor, how would your business survive?
- If several key female employees went on maternity leave around the same time – who would cover for them?
- Are there provisions in place for post incident counselling in your work place?
- When was the last time you reviewed health and safety procedures in your work place?

From product development to production, sales, marketing, finance and management, every company can identify a set of key people without whom its operations would be severely disrupted.

- **Key people** – Identify people that are critical to the immediate operation of the business and work hard to reward, challenge and protect them
- **Skill sharing** – Make sure that specialist skills are not held by just one person. Develop understudies and teams of specialists so people can step into specialist roles at least temporarily should the need arise
- **Keep an eye on local competitors** – If they are recruiting, make sure your people in relevant positions are happy
- **Assess workplace risks** – Identify employees that are exposed to particular risk of injury and ensure they are equipped with and use relevant safety equipment and procedures. Ensure that all employees are aware of workplace hazards and follow good safety practice.

Protect your employees and your business

Employers' Liability insurance is a legal requirement in the UK. It will enable you to pay for medical treatment and compensate your employees should the worst happen.



IT/Telecoms

These days, most businesses rely on computers to some extent. Some companies may only use them for accounting and email, but others base their entire business on them. Telephone systems are equally important.

The chances are that most companies would soon find themselves facing a disaster if a computer or telecom failure was not properly planned for and managed. For example, if your computer or telephone systems were unavailable for three days, would you be ready? Ask yourself the following:

- Would your business still function?
- Would you be able to contact your customers?
- Would it hold up production?
- What alternative arrangements would you be able to make and how long would it take?
- What could you do to make certain you have access to vital data, even if your computer system were destroyed?

If your computer systems are stolen:

- Could sensitive information fall into the wrong hands?
- What would happen if your competitor got hold of sensitive information?
- Are your computer security systems robust?

The environment

The experience of recent years has clearly illustrated the impact that natural disasters can have on business. Flooding in the south of England, the Midlands and Yorkshire has affected thousands of firms, putting many out of business.

Climate change is likely to have other impacts on business. Increased green taxes could have a significant impact on heavy manufacturers. For example water shortages and rising bills could put pressure on a wide range of firms.

- Would your business survive a serious flood?
- How would electrical circuits, computer systems, stock and machinery be affected?
- How long would it take to recover from a flood? How would you keep customers happy and pay your employees in the meantime?
- Some businesses were out of action for over twelve months following flooding in 2007. Would your creditors be patient for that long?
- Are you up to date with environmental legislation that could affect your business and increase costs over the next few years?
- How reliant is your business on a large and relatively inexpensive water supply?



Businesses should familiarise themselves with changing EU legislation which will affect employers now and in the future.

Here are a few examples of legislation that may be already having an impact on your business or will be something to consider soon:

- **Directive on the Physical Agents (noise):** this is an EU Directive which was enacted in the UK in February 2006 and has introduced new Noise at Work Regulations with lower noise exposure limits. The new regulations apply to businesses previously outside the scope of the existing legislation, eg the leisure industry including pubs and clubs. These businesses will have to conduct noise assessments and record the results – as well as issue hearing protection to all employees affected
- **Work at Height Regulations:** this legislation was introduced in April 2005 in order to stem the rising toll of deaths from work at height. Work from ladders has been identified as a serious risk and specific HSE guidance has been produced to show when it is appropriate to use ladders.
- **Energy Performance of Buildings Directive:** Buildings that are to be sold or re-let must now include an Energy Performance Certificate (EPC) or Display Energy Certificate (DEC) for public sector buildings. This could have implications for business continuity and awareness is important. Also to be considered are the ways of improving performance of this directive, such as more efficient windows, wall and roof insulation which should be selected with due consideration of fire spread implications.
- **EU regulatory framework for chemicals:** REACH (Registration, Evaluation and Authorisation of Chemicals) came into force on 1 June 2007. Companies that manufacture or import more than one tonne of a chemical substance per year are required to register it in a central database and to fully ascertain the risks posed by the use of the chemicals. This legislation therefore affects SME's who use chemicals (particularly in the manufacturing sector)
- **Disability Legislation:** The Disability Discrimination Act 2005 is in force in it's entirety with fines of up to £5,000 for non compliance. There are simple steps small firms can take to show they are complying with the legislation – changes required by the act include widening doors for wheelchairs, introducing ramps and hand-rails, and providing wheelchair-friendly lavatories.

Thoroughly assessing the disasters that could threaten your firm will give you a clear idea of the business areas that are most important to secure.

Step four: Writing your own Business Continuity Plan

A Business Continuity Plan will ensure you are prepared for the worst situation that would keep your business from being operational. The plan only needs to include the business processes that are most critical to keeping your company running. For this reason the plan has been presented in a generic form so it can be adapted as necessary.

To assist you to write your own plan we have included an example of a Business Continuity Plan, on pages 19-21 of this guide. As a plan of this kind should be tailored to suit your business please remove and add sections as needed. It is to be used as a reference point to help get you started.

Here is a checklist of items to include in any Business Continuity Plan. They are all included in the sample plan:

- Business continuity project manager's name and contact details
- Structured management team that will make the key decisions
- Contact details to enable the team to be brought together
- Nominated control centre as a meeting point
- Identification of business critical processes
- Details of how a recovery would be phased
- Telephone divert arrangements
- Emergency contact number for employees to obtain the latest information
- Resource requirements (people, work area, IT, telecommunications)
- Details of recovery resources
- Contacts for internal and external agencies committed to supporting the recovery efforts
- Address of the recovery site
- Contents and storage location of a disaster pack
- List of key customers, suppliers, third parties and their contact details
- Comprehensive team cascade list
- Details of the vital records' store containing backup computer data and any critical paper records held off-site
- Network diagrams and other technical information
- Precautions to be taken in the event of an incident.



Step five: Test the plan

Once the plan has been agreed it should be communicated to your team/teams. This will expose any flaws in the plan and will also ensure all the roles and responsibilities are understood. It is worth completing a test simulation of the plan to ensure its smooth running if the time comes to use it.

Step six: Regularly update the plan

Review the plan at least every six months. Check to see that the plan includes correct contact details for the recovery site, vital records, suppliers and the team.

Distribute the plan to all people assigned responsibility and advise them to keep copies off site. You can also use your team meetings to remind all employees of the process to follow.

Start now

The essential safety net for any organisation is a Business Continuity Plan. Investing the time and energy in the short-term will benefit your business in the long run.

The message is simple – it's never too early to take steps to assess your business risks and set the internal recovery procedure. Make your plan as detailed as your business needs it to be and take the time to communicate this with your team. Regularly review the plan in tune with the changing needs of your company. A well thought out Business Continuity Plan will adapt to any incident or crisis for your company. This guide is written to help you do exactly what your business needs, to be ready to recover at any time.

ROBUST New business continuity planning software tool launched



AXA can also now provide a free of charge software tool for a more detailed business continuity plan. This is available via <https://robust.riscauthority.co.uk>.

ROBUST is a software program that will help you create and manage an effective Business Continuity Plan for your business and provide essential on-the-spot advice immediately following an incident. ROBUST has been designed specifically to address the hurdles currently identified as discouraging companies from embracing business continuity planning and as such it:

- Is FREE
- Requires no other paid-for software elements aside from the computer's operating system
- Is designed with logical workflow, easily recognisable within normal company structures
- Provides feedback on quality and completeness
- Provides all output in a format suitable for insertion into other company documentation
- Is provided with all necessary training to develop the plan

ROBUST has been financed through RISC Authority, a scheme annually financed by a group of UK Insurers, including AXA, and administered by the Fire Protection Association. The aims of RISC Authority are to invest in research to support the development and promotion of best practice guides and tools for the mitigation of business and property loss. The Fire Protection Association is a not-for-profit organisation.



<< Insert Company Logo >>

Business Continuity Plan

Business Continuity Project Manager
<<insert name>>
Contact
1. Office:
2. Mobile:
3. Home:

The maintenance of this document is the responsibility of the Business Continuity Project Manager. This plan will be updated on a regular basis and includes the key details and actions needed to continue all business operations.

Business Continuity Team

This team will comprise the key decision makers in the company. Ideally they should congregate in a pre-designated location. They will be in close contact with the Business Continuity Manager and will authorise any variations to the recovery plan.

<<insert name>>	1. Home	4. Mobile
	2. Work	5. Pager
<i>Business Owner/Leader</i>	3. Internal	6. Other

<<insert name>>	1. Home	4. Mobile
	2. Work	5. Pager
<i>Deputy Business Continuity Project Manager</i>	3. Internal	6. Other

<<insert name>>	1. Home	4. Mobile
	2. Work	5. Pager
<i>Finance or HR Manager</i>	3. Internal	6. Other

Business critical processes (in order of priority)

Agree on the most important function to be restored first. This function is critical to keeping the business running. For example:

1. Sales
2. Order fulfilment
3. Banking

Initiate Recovery Log

In all instances it is the Business Continuity Project Manager's responsibility to ensure a recovery log is kept. This will track all decisions that are made and the actions taken. The log will include the following activity:

- Time and date
 - Description of the activity and the reason for it
 - Name of person initiating the action
 - Names of those instructed
 - Dependencies (e.g. people, resources)
 - Other persons who need to be kept informed
 - Expected time in which task will be complete
 - Time in which task is completed
- Activity checklist during the incident**

This checklist provides a number of actions for the Business Continuity Project Manager to complete.

<< Insert Company Logo >>

Note: This plan is based on the scenario having the biggest impact on the business, which is destruction of the premises. The plan can be adapted for less severe incidents - as all the tasks appropriate in the worst scenario might not always be needed.

1. Alert the Business Continuity Team
2. Agree with Business Continuity Team the recovery activities to be followed and implement Recovery Action Plan
3. Initiate recovery of disaster pack from the off site location
4. Advise relevant staff to report to the designated recovery at appointed time
5. Advise remaining staff who are not required immediately to remain at home until contacted
6. Obtain essential items/records from the off-site location
7. Notify critical contacts (e.g. customers & suppliers)
8. Establish immediate business needs and necessary actions
9. Establish operations at designated recovery site
10. Assess last known status of workload and the extent of work lost or outstanding
11. Maintain a log of actions taken
12. Refer to the telephone directory of all employees (includes work and home telephone), keep note of the team's whereabouts
13. Obtain authorisation from Finance Manager for business recovery expenditure
14. Consider shift patterns and overtime requirements

Designated Recovery Site

Some companies may make arrangements for an alternative site from which to continue their business. It is usual that a recovery site has access to telephone, internet and computers. Again, this will depend on the needs of your business.

Recovery Site Location	Contact Name	Contact Tel
<<insert address>>	<<insert name>>	Office Home Mobile

(attach map)

Vital Records

All your important records and materials to run the business will be stored at an off site location so they can be retrieved in times of an emergency.

Back-up Computer Records stored at:	<<insert name, address & contact number>>
-------------------------------------	---

Critical paper records stored at:	<<insert name, address & contact number>>
-----------------------------------	---

Disaster Pack stored at:	<<insert name, address & contact number>>
--------------------------	---

Critical Contacts

The following list contains names of important business contacts, where it is considered that personal contact is appropriate. This will include key customers and suppliers.

<< Insert Company Logo >>

Company	Contact Name/Department	Telephone
Client 1		
Client 2		
Supplier 1		
Supplier 2		

Recovery Action Plan

Here is an example of how the recovery action plan is structured. It should be easy to follow so that any member of the team can action – in the case that the Business Recovery Project Manager is absent.

- Contact BT to switch phone lines to <<designated recovery site>> telephone/s. Telephone BT on <<insert number>> account number <<insert company account number>>
- Contact IT Consultants <<insert number>>
- Load 6 PCs stored at <<designated recovery site>> with software and back-up data
- Purchase additional PCs from <<insert PC supplier and telephone/address>>
- Back up server stored <<designated recovery site>>
- Additional office equipment can be purchased from <<insert PC supplier and telephone/address>>
- Manual workaround process guides and order forms stored at current location and duplicates stored at <<designated recovery site>>

Team Cascade List

This list will ensure that every member of the team is contacted about the incident and instructed on what they need to do. If the cascade is activated, be sure to keep a record of those members of staff not contacted.

Mr. X will notify: Sales Team

Name	Home	Mobile

Mr Y will notify: Order Fulfilment Team

Name	Home	Mobile

Debrief

After the incident it is important to meet with the team and evaluate how the plan worked. All agreed improvements should be added to the Business Recovery Plan.

Appendices

May include, for example, plans for a specific, highly probable, incident or detailed IT recovery requirements and procedures.

AXA is a world leader in wealth management and financial protection, managing funds worth more than €981 billion (as at 31 December 2008). We operate in over 50 countries and serve 67 million customers worldwide. We cater to a wide range of needs, providing advice and guidance to our individual and corporate customers on a variety of financial products and services. These include investments, life assurance, retirement planning, long term care, asset management, medical insurance, dental and hospital care services as well as motor and home insurance.

ACLD0330

www.axa.co.uk

