RISCAuthority

Administered by

FPA Fire Protection Association

A Guide to Incident Management and Business Continuity for Small Businesses

Download from www.riscauthority.co.uk

Version 1 Published 2015

Who is this for?

This document is intended to provide businesses with the necessary tools to help them develop a basic incident management and business continuity plan (hereafter known as an '**incident management plan**'). Incident management generally refers to the immediate handling of a disruption; business continuity to maintaining an acceptable level of service to customers.

What is incident management?

Having an appropriately skilled and practised team in place to enable all incidents that might detrimentally affect the business be dealt with in a quick and efficient manner.

What is business continuity?

This is the process of giving some thought in advance to how you would maintain service to customers and recover from damage to, or loss of, a particular element of your business and developing those thoughts into positive plans of action.

How do I do incident management?

Create an incident management team which has the appropriate skill sets and experience to deal with unexpected incidents. Allocate duties to each of the team (either in advance or at the time of the incident). Practice disruptive scenarios.

How do I do business continuity?

Look at the six critical business elements detailed in this plan (people; premises; machinery/equipment/utilities; data; communications and suppliers) and ask yourself: *"How would I continue to carry out my business if any of these elements was interrupted for a period of time?"*

The effects will differ depending on the duration of the interruption so consider a range of time periods. Establish the time period in which you would need to recover the particular aspect before the business starts to suffer. Decide what measures you need to put in place to prevent the business being adversely affected. These measures could be in the form of 'recovery plans' (post-event) or additional protection/mitigation measures (pre-event).

In addition to the above you will need to consider:

- when to invoke the incident management team and how to contact the team members;
- where the incident management team might meet should the main premises become unavailable as a result of the incident;
- whom you might need to contact to inform them of the incident and/or to seek assistance; and
- what information and equipment you might need to assist recovery in the event of an incident.

Note

The information written in black typeface is provided as examples of what to include in your plan or guidance as to what should be considered in your planning. This can either be verified as appropriate or changed to suit your own requirements.

Incident management plan [example]

Company name

Plan owner			
Plan objectives	▪ *To assist the incident management team (IMT) in managing an incident* ▪ *To provide, via checklists, an orderly process for managing incidents* ▪ *To assist in prioritisation of the recovery of critical functions* ▪ *Provide a detailed, prioritised and timetabled response to an emergency situation* ▪ *To provide information on how to recover critical functions* ▪ *To provide contact details to assist in the management of an incident*		
Date issued			
Date of next review	*The plan must be regularly reviewed (six monthly) to ensure:* - *information contained within is up to date and correct;* - *that it reflects any changes in the business or the way in which it operates;* - *that the exercise programme is up to date; and* - *that it continues to be appropriate and sufficient.*		
Location of plan	- *saved file location* - *memory stick* - *printed copy*		

Plan contents

1. Invocation and mobilisation

Invocation
The incident management plan may be invoked by any member of the incident management team in response to an incident that they feel may have an adverse effect on the normal day-to-day operations of the company.

Definition of an incident
An event that has the capacity to lead to loss of or a disruption to an organisation's operations, services or functions – which, if not managed, can escalate into an emergency, crisis or disaster. An incident need not be physical it may be one that could lead to reputational damage without any associated material loss.

Escalation
The incident management team will be assembled by the person invoking the plan using the contact numbers in section 2. The person invoking will direct the team to one of the incident control rooms listed below.

Should any further staff be required to populate the Incident Management Team they will be contacted individually, by the IMT, via phone or email.

Initial contact with staff (to explain the situation) will be made by the communications role via the text messaging service (refer section 2).

A member of the IMT should be instructed to collect the ***grab bag**** *on their way to the crisis control room. The duplicate grab bag is located at the gatehouse of Site F.*

The IMT can only be stood down on the instruction of the incident commander.

*a grab bag contains items and information that may assist in the event of a crisis eg site plans showing utilities, fire protection and isolation points, staff contact lists, torches, camera, high visibility jackets etc.

Crisis control room locations

Location	Contact details	Resources available
Board Room Any Street AN1 1XX	name@address.com 0102 569443	two landlines Projector Television screen

2. Incident management team

Definition: The group of individuals responsible for implementing a plan in response to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.

Role	Responsibilities	Person responsible	Contact details
Incident commander	▪ *Take overall control of the incident* ▪ *Allocate roles and responsibilities* ▪ *Establish the strategic objectives of the response to the incident* ▪ *Determine recovery policy and long- term strategy* ▪ *Second other staff to the team as required* ▪ *Take strategic decisions and authorise expenditure* ▪ *Provide regular team briefings and updates*	It may be appropriate to also identify deputies in the event of unavailability	
Personnel	▪ *To account for the whereabouts and well-being of all staff* ▪ *Ensure safe evacuation and staff well-being* ▪ *Provision of welfare facilities and support* ▪ *Liaison with hospital* ▪ *Staff transportation*		
Record keeper	▪ *To record all actions taken and decisions made* ▪ *To record all expenditure* ▪ *To record all other relevant information* ▪ *To present the information in the post-exercise debrief*		
Communications	▪ *Deliver initial text message to staff* ▪ *Update staff at regular intervals* ▪ *Set up staff helpline* ▪ *Liaise with personnel to ensure clear and consistent communications*		

	▪ *Control text communication channel* ▪ *Update the website at regular intervals* ▪ *Liaise with the media representative to ensure the correct message is delivered* ▪ *Co-ordinate the communication with all external parties, suppliers, customers and stakeholders*		
Media liaison	▪ *Agree and issue media statements* ▪ *Monitor the media channels for latest developments* ▪ *Liaise with external and internal communications to ensure clarity and consistency of message*		
Technology	▪ *Ensure that the IT disaster recovery plan is expedited effectively* ▪ *Comms reinstatement*		
Facilities	▪ *Damage assessment* ▪ *Securing of the site* ▪ *Utility isolation and/or provision* ▪ *Emergency services liaison* ▪ *Co-ordinate relocation to alternate premises*		

3. Incident management checklist

	Task	Owner	Completed
1	*Start action log*		
2	*Account for staff (whereabouts and well-being)*		
3	*Dispatch facilities team member to site*		
4	*Liaise with emergency services and identify salvage priorities*		
5	*Identify and assess damage*		
6	*Identify disrupted activities*		
7	*Secure damaged asset/building*		
8	*Review critical functions priority list*		
9	*Identify appropriate recovery strategy and strategic response*		
10	*Decide on a course of action and allocate duties*		
11	*Convene operational recovery teams*		
12	*Communicate details to staff and stakeholders*		
13	*Prepare media statement and communication strategy (copy held in grab bag)*		
14	*Inform Insurance company/broker/loss adjuster*		
15	*Set up helpline and update the website*		
16	*Ensure adequate resources to man phone lines and communicate with all stakeholders*		

17	*Contact customers and suppliers*		
18	*Update the board and other stakeholders*		
19	*Arrange a debrief*		
20	*Review incident management plan and reassess priorities*		

4. Recovery plans

People		
Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable	
Recovery plan(s)	**Person responsible**	**Status**
▪ Identifying and documenting details of which people have key skills and knowledge ▪ Training individuals to acquire additional skills and knowledge ▪ Documenting key processes to allow staff to undertake roles with which they are unfamiliar ▪ Keeping a list of retired or ex-employees with key skills and knowledge that can be called up when required ▪ Using people with the relevant skills and knowledge from a third party (either through a contractual arrangement or keeping a list of suitable third parties) ▪ Geographical separation of individuals or groups with key skills and knowledge ▪ Outsourcing a portion of the work requiring key skills and knowledge to a third party that has the capability of taking over more of the work at short notice		
Additional mitigation identified		**Date implemented**
Ensure all job descriptions are up-to-date		
Arrange a training session on key systems		

Premises		
Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable	
Recovery plan(s)	Person responsible	Status
▪ Using available space at another of the organisation's sites, where possible (this might include meeting rooms, training space, canteens, etc). ▪ Increasing staff density at another of the organisation's sites (sometimes referred to as 'budge-up'). ▪ Displacing staff undertaking less urgent activities from another of the organisation's sites and using the space made available (care must be taken when using this option that backlogs of the less urgent work suspended do not become unmanageable). ▪ Remote working includes the concept of 'working from home', and working from other non-corporate locations like hotels. Working from home can be a very effective solution but care must be taken to ensure health and safety issues are addressed, suitable IT equipment with properly licensed software is provided and sufficient networking capacity/technical support is available. ▪ Reciprocal agreements with other organisations to use their premises – care must be taken when establishing this type of agreement to ensure that testing is allowed and procedures are put in place to ensure that periodic checks are made to determine whether or not the required space is still available. ▪ Using a list of available premises or potential suppliers of premises to find alternative premises after the disruption (this option is suitable for activities with relatively long optimum timescale for recovery, and is often referred to as		

'Ad-hoc'). ▪ Contracting with a third party to provide a recovery site. ▪ Acquiring and fitting out additional premises ready to be used when required as a recovery site (this can range from keeping an empty facility that needs fitting out through to having a fully equipped replica site). ▪ Mobile accommodation – can be brought into use rapidly, but provides limited space and may require service and power connections. ▪ Moving the activity, but not the staff, to another site that has the capability to undertake the activity (known as 'Diverse Locations'). <u>And where possible</u> ▪ Temporary prefabricated accommodation (caravans, cabins, etc) – this requires available land that is suitable, can take a number of days to construct, and may require significant preparation of foundations and other site preparation including the supply of power, water, and telecommunications. ▪ Replica sites – the activity is transferred to one or more alternate locations, at which staff and facilities are already prepared to handle the workload.		
Additional mitigation identified		**Date implemented**
Install sprinklers		

Data (electronic and paper)			
Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable		
Recovery plan(s)		Person responsible	Status
▪ Backups – backing up the information held in the computer systems, and storing the backups in a safe and secure location that is geographically separated from the computer systems on which the original information is held. ▪ Ad-hoc – wait until the IT is lost and then obtain replacement equipment if required, and recover the systems and information from backups (this option is low cost, but high risk, and is suitable where the optimum timescale for recovery is in weeks rather than days, or where the replacement equipment is readily available and the configuration of the IT is relatively straightforward). ▪ Support agreement – enter into a support agreement with a third party to supply replacement equipment in a pre-defined time period to a pre-defined configuration, and recover the systems and information from backups. ▪ Standby equipment – spare equipment held as a standby (either pre-configured or not) that can be used if equipment is lost, with the systems and information recovered from backups (holding standby equipment at a geographically separate site will improve the chance that the standby equipment is available when required). ▪ Duplicate equipment – a complete duplicate of equipment pre-configured with the systems already loaded, that can be used if equipment is lost, with		

the information recovered from backups. ▪ Third party equipment – a contract with a third party to use their equipment located at a third party site, with the systems and information recovered on to their equipment from backups. ▪ Replica systems – replicas of the equipment, systems, and data, which can be held at one of the organisation's own sites or at a third party site (a geographically separate site will improve the chance that the replica can be used when required) and can take the form of: ▪ Continuous replication – where the data is being continually replicated from the original system to the replica (theoretically providing zero data loss) ▪ Mirroring and or shadowing – where changes to the data in the original system are mirrored or shadowed in the replica (providing minimal data loss) ▪ Logging – where changes to the data in the original system are logged and batched before being sent to the replica (depending on the timescale used, data loss could be measured in minutes or hours) ▪ Backup – where a backup is taken of the data in the original system, which is then copied to the replica (changes made to the original since the last backup would be lost) <u>Paper</u> ▪ Do nothing – accept the loss. ▪ Copy the paper records and store the copies at a site geographically separated from where the original records are held. ▪ Scan the paper records and store the images electronically (the electronic records can be held either at the same site, with backups held		

elsewhere, or at a geographically separated site). ▪ Recreate the paper records as best as possible from information supplied by staff, customers, suppliers, and other stakeholders.		

Additional mitigation identified	Date implemented
Purchase fire-proof safe	

Communications

Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable

Recovery plan(s)	Person responsible	Status
▪ Automatic call diversion ▪ Manual call diversion ▪ A recorded message asking callers to telephone another number ▪ Broadcast notification to staff and other stakeholders of alternative numbers to call ▪ Non-geographic numbers (0845) ▪ Managed network services ▪ Mobile switchboard ▪ Use of mobile telephones – although this cannot be relied upon as mobile telephone communications may be switched off, or become over-loaded, following a major incident		

Additional mitigation identified	Date implemented
Purchase additional mobile phone chargers	
Purchase spare pay as you go mobiles	

Machinery/equipment/utilities

Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable

Recovery plan(s)	Person responsible	Status
General equipment *(that used day to day in normal business process and readily available).* ▪ Ad-hoc – wait until the equipment is lost and then obtain replacement equipment if required (this option is low cost and may be suitable where the optimum timescale for recovery is in weeks rather than days, or where the replacement equipment is readily available). ▪ Support agreement – enter into a support agreement with a third party to supply replacement equipment in a pre-defined time period (sometimes referred to as a 'ship in' contract). ▪ Standby equipment – spare equipment held as a standby that can be used if equipment is lost (holding standby equipment at a geographically separate site will improve the chance that the standby equipment is available when required). ▪ Duplicate equipment – a complete duplicate of equipment that can be used if equipment is lost (again, holding such equipment at a geographically separate site will improve the chance that it is available when required). ▪ Third party equipment – a contract with a third party to use their equipment located at a third party site. ▪ Specialist equipment *(bespoke equipment for specific processes, not readily available).*		

▪ On-site maintenance or maintenance contracts with guaranteed service levels. ▪ Use of subcontractors or competitors with similar equipment configurations. ▪ Holding spares of important components (holding spares at a geographically separate site will improve the chance that they are available when required). ▪ Holding of older equipment as emergency replacement or for spares (again, holding such equipment at a geographically separate site will improve the chance that it is available when required). ▪ Changing the process to use more readily available equipment. <u>Utilities</u> ▪ Uninterruptible power supply (UPS) – to cover short power outages and enable the safe shut down of equipment (particularly computers). ▪ Standby back-up generators – that cut-in, either manually or automatically, when power fails to protect buildings or equipment from more prolonged power failures (however, these need to be maintained and tested regularly to ensure performance when required). ▪ Portable generators – shipped in when required either as a contracted service or on demand (this would be subject to availability, and in the event of a wide spread disruption of power may be difficult or impossible to obtain). ▪ For all manufacturing plants the availability of water supplies both for staff and process purposes will be essential. Other fuels (gas and oil) will also be essential and the suppliers.		

Additional mitigation identified	Date implemented
Purchase critical spares for the production line	
Ensure all maintenance contracts are current and valid	

Suppliers

Optimum timescale for recovery	eg 1 hour, 2 days, not quantifiable

Recovery plan(s)	Person responsible	Status
▪ Dual or multi-sourcing of supplies ▪ Identification and pre-acceptance of alternative suppliers ▪ Contractual obligations on the supplier to implement BCM ▪ Inspection of supplier's BCM capability for the products and services supplied, which should include evidence of successful exercises ▪ Holding spare or buffer inventories ▪ Significant penalty clauses on supply contracts (though this will not protect against supplier bankruptcy) ▪ Reciprocal Arrangements: Any mutual agreements with another company in a similar field that could be activated in an emergency, to supply the business with facility, equipment or product, to minimise the effect of the incident		

Additional mitigation identified	Date implemented
Research local companies for mutual aid agreements	

5. Exercise programme

Type	Process	Participants
Test options		
Desk check	▪ Check the structure and content of the plan	▪ Author of plan
Walk through	▪ Discuss the theory of the plan to check that it is usable	▪ Author of plan ▪ Users of the plan
Unit test	▪ Confirm that a recovery procedure or the recovery of a piece of technology works	▪ Users of the procedure or technology ▪ Others as required (eg technicians)
Rehearsal options		
Simulation	▪ Use the plan to undertake a theoretical response to an incident	▪ Facilitator ▪ Users of the plan ▪ Others as required (eg observers)
Full rehearsal	▪ Practice the recovery of a complete area of the organisation, a business process, product or service or interconnected technologies, following a script	▪ All those in the area of the organisation, or all those that are required for the business process, product or service or all the users of the interconnected technologies ▪ Others as required (eg technicians)

Sample exercise scenarios	
1	Fatality within the business
2	Hazardous chemical spill at the entrance to the site
3	Flu pandemic
4	Cyber attack resulting in release of data into the public domain
5	Denial of access due to flood

Exercise log			
Date	Type of exercise	Report completed Y/N	Plan revised (Date)

Appendices

Appendix A Activity log sheet

Date	Time	Information/decisions/actions/expenditure	Initials

Appendix B Resource needs planner

Resource needs planner – Pre-plan the resources needed for recovery, or use during an Incident to lay out the timeline of what is needed to recover							**Page:**	
What resources are needed? Staff, 3rd parties, equipment, premises, IT/comms, power, water, gas, catering. Quantify resources needed (eg 3 trained operators, 6 cutting machines, hot food catering capacity, 1000sqm of area, 500KVA of power etc.	**Timeline of obtaining Resources** - Estimate How much/how many by when? Set appropriate timeline eg <1 hour to 5 days, or <4 hours to 15 days, or <12 hours to 30 days							
	<4 hrs	4-12 hrs	12-24 hrs	1-3 days	3-5 days	5-10 days	10-30 days	>30 days
Operators (6 trained)				1	2	3	6	
OEM / Contractor – Italy – (3 engineers)					1	2	3	
Premises Area - 25,000 sq.m				10,000		15,000	25,000	
Production equipment – 2 x 6000 Units/wk					1		2	
Electricity – 500kVA				200KVA		300KVA	500KVA	

Appendix C Staff contacts

Name	Position	Phone number	Email address

Appendix D Emergency contact list

Date	Company	Contact name	Phone number	Email
Electricity				
Gas				
Telecoms				
Water				
Security				
Salvage				
Police				
Hospital				
Council				
Water board				
Environment				

Appendix E Critical suppliers contact list

Company	Nature of supply	Contact name	Phone number	Email

Appendix FKey customers contact list

Company	Contact name	Phone number	Email

Appendix G Other stakeholders

Stakeholder interest	Company	Contact name	Phone number	Email
Insurance co				
Insurance broker				
Bank				
Regulator				