The University Of Sheffield.

A Short Guide to Business Continuity.

Introduction

Business Continuity (BC) is focused on improving the resilience of the University. It means developing the University's ability to detect, prevent, minimise and where necessary manage the impacts of disruptive events.

This guide provides a summary of the stages of the University's process.

What is Business Continuity Management (BCM)?

Business Continuity Management is defined in the University's Policy and Framework as a "process that enables the University to proactively identify and plan to minimise the impact of risks that could affect its objectives, operations and infrastructure."

It enables the University to continue as normal - or at least its priorities at an agreed level - following an incident. The University does not have a specific legal duty to undertake Business Continuity (BC), but recognises its importance and has established a BC Programme. Its aim is to return to normal as soon as possible after a disruption; however what is classed as "normal" may change after an incident.

What is an incident?

An incident is *"a situation that might be, or could lead to, a business disruption, loss, emergency or crisis"* [1]. It is something out of the ordinary that may cause a disruption to the University; it can happen suddenly e.g. a fire or there may be advance notice, e.g. swine flu, where there is time before the event to prepare.

Building Collapse | Fire | Heavy Snowfall

How does BCM work?

There are four stages to the BCM process at the University:

1. Understanding the University

What you do, the priorities and why

Each department completes a Business Impact Analysis (BIA) to build a picture of what the University does. The BIA identifies the:

- Services a department provides and activities to deliver them
- Impacts if the activities can't be delivered
- Time they need to be available within

This confirms the priority activities to recover after a disruption.

2. Developing Strategies

The resources you need and your plan b if they are unavailable

The resource requirements are identified alongside the BIA, specifically what:

- Resources e.g. staff, are needed to keep the priorities going
- Current strategies/plan b to deal with their loss
- Alternative options to cope without a resource

A decision is then made on the appropriate strategy.

3. Developing Plans

The plan to help you manage an incident

A Business Continuity Plan (BCP) is produced using the data collected in stages 1. and 2. This is a practical document to help manage an incident i.e. who is involved and what the arrangements are to recover/continue the agreed priorities.

4. Reviewing and Exercising

Ensuring your plan is relevant so it will work when needed

A BCP needs to be updated to ensure it is effective when required. As a minimum, reviews should be on an annual basis. Exercises are held to assess how the plan works, without the pressure of dealing with a genuine incident.

The University's Business Continuity Manager will offer support during the process, but departments know their areas so are best placed to develop arrangements.

What does it link to?

BCM has links to other areas, referred to in the Policy and Framework:

Major Incident Plan (MIP): Sets out the response to major incidents (where there is a significant impact) including having a University Major Incident Team. Their focus is on the initial response, dealing with the safety of people, buildings etc.

An incident may be minor (with a limited impact) so the MIP would not be used; however some incidents can initially be minor, but become major.

Risk Management: Identifies all risks i.e. uncertain event(s), which if they occurred would impact on the achievement of objectives. BC focuses on issues relating to incidents so are likely to be considered "threats" which tend to have an adverse impact on objectives. Business Continuity can also be used as a risk treatment.

Information Security: Aims to protect all forms of information and ensure its confidentiality, availability and integrity. BC considers how to cope if key information is unavailable and could require a business continuity response.

We must ensure that relevant legal, regulatory and contractual requirements for protecting information are met. This includes, but is not limited to, Data Protection law, the rules relating to credit/debit card data and any contractual regulations stipulated by our research partners.

Responsibility and Ownership

Responsibility and ownership for plans rests with the Head of Department (for information on governance see Stage 4.)

[1] ISO 22301 Societal security – Business continuity management systems - Requirements

Stage 1

Understanding the University.

What you do, the priorities and why.

The University should identify its priorities, to keep going or recover and "return to normal" after an incident, by completing a Business Impact Analysis.

What is a Business Impact Analysis?

A Business Impact Analysis (BIA) is the process of identifying and assessing University activities and the impacts that a disruption will have on them over time[2].

Why complete a BIA?

It may not be possible to continue doing what you normally would after an incident; to manage the disruption you may need to stop certain activities and concentrate on others. The BIA identifies the most urgent to continue, called priority activities, and similar to managing your workload prioritises based on what is most time sensitive and what would have the greatest impact if not delivered.

In order for a Business Continuity Plan to be effective it requires the foundation and information provided by the BIA.

What is the University's approach?

There is a BIA template to complete; whilst the outputs from each department may differ, it is important that the process to identify the priorities is consistent. The BIA provides a list of priority activities and timescales they need to be recovered within. The BIA has the following sections to be completed:

Services
List the services performed by your department i.e. what you deliver to someone e.g. paying staff, delivering assessments, managing waste, inspecting buildings etc.

[2] ISO 22301 Societal security – Business continuity management systems - Requirements

Activities
For each service list the activities that are performed to deliver it (ideally no more than 7). Each activity may cover a process or a group of processes e.g. if your service is delivering assessments your activities would involve setting the assessment, marking, holding an exam board.

Owner/s
Identify who is responsible for each of the activities; it may be the same person, but sometimes there are a range of people - or departments - involved.

Impacts
Consider what would happen if the activity wasn't provided. Key areas to focus on are health and safety and legal issues, impacts on students and staff, reputation, finances and also stakeholders (anyone with an interest in what you do). The impacts considered should be based on the first seven days after an incident.

When is it Performed and the Peak Periods
Some University services are performed on a cyclical basis, e.g. registration. Assessment of activities to support them should be based on the time of the highest demand, because arrangements need to be able to cope with the worst-case scenario. The peak period/s should be noted.

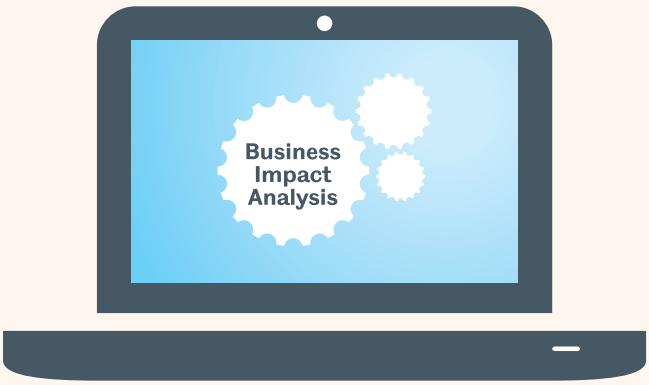
Recovery Times
The question is how quickly do you need this activity to be running if it completely stopped? The timeframe isn't based on when it would operate at normal levels, but the point in time that you would need a minimum level of service available. Assessing when the impacts or consequences of it not being available become unacceptable should help to identify a recovery time; this needs to be realistic – allow time to fix the problem. The template splits recovery times into three groups – you identify the recovery time, and should note it in the relevant column:

- Short term: 0 - 24 hours
- Medium term: 1 day - 6 days
- Long term: 1 week or greater

Priority/Urgent Activity?
A priority activity in the Policy document *"is identified based on how quickly it needs to be resumed and the impact if it is not available – on the safety of people, the reputation of the University, its finances and customers."* It is focused on how time sensitive it is. For each activity you need to determine whether it is a priority, based on the impacts if it wasn't available. If it has a recovery time within the short term it will be a priority, the medium term it is likely to be. If it falls into the long term, it is not a priority under the current programme.

This is not a question of importance; there is a reason for all the activities performed - but they are not all urgent to continue after an incident.

Completing the BIA
A co-ordinator is required to collate information for the BIA. They are not responsible for providing all the information for it - it requires involvement from across the department. The Head of Department should approve the BIA. It should be updated annually as a minimum - and reviewed if there is a change that could affect its content for example, a new service is being provided.



Stage 2

Strategies.

The resources you need and your plan b if they are unavailable.

Once the priorities are identified, the resources to support them need to be considered by completing the Resources Requirements. This also reviews what the strategies to manage any disruption to the resources.

Resource Requirements

There is Resource Requirements template, completed with the BIA.

What are the Resources?

- People - staff and skills
- Buildings - location, space, specialist facilities required
- Information, communications and technology (ICT) and data - computers, phones, printers. Also information stored both electronically or on paper
- Equipment and Finance e.g. machinery, research equipment, PPE, credit cards
- Stakeholders including suppliers - dependencies and people with an interest

Business Continuity is focused on the impact of the incident, not the event itself. So arrangements are focused on the loss of a resource, not how to deal with a specific incident. This enables the plan to be used for any incident, not just those that are likely to occur. For example, it doesn't matter if there is severe weather, flu or a problem with transport the impact will mainly be on staff.

The Resource Requirements has the following sections to be completed:

Activities
Only those activities identified as a priority in the BIA are considered in this process and should be transferred into the first column of the form.

Issues / Vulnerabilities?

You may already be aware of an issue relating to an activity. This could be related to the location of your building, due to a recent event or something on your risk register. Alternatively, there may be an issue that only a few people can perform certain tasks, or specialist equipment available from one supplier. This should be noted here.

Resources (minimum)

Considering the recovery time you have set, identify the minimum level of service you would aim to provide at this point, and what resources you would need to deliver it. There may be a backlog if the activity has not been performed for a while.

Your Strategy?

All activities depend on resources to continue, so BC is focused on having a plan b or strategy to manage a disruption to the resources. For each resource, consider:

- What arrangements are currently in place i.e. could be used if the incident occurred now?
- What else could be done – what are the other options?

The "Strategy Considerations" that follows, gives considerations to assist with this.

Once this information has been completed for all the priority activities, an assessment should be made about whether the current arrangements are sufficient. This should consider the information in the vulnerabilities column i.e. would the arrangements you have in place manage the issues noted?

If it is decided they are not or it would be beneficial to have alternatives, then work is required to implement the other option(s) identified, before moving on to the next stage. The Business Continuity Plan cannot be produced until the strategies are agreed.

Approval

It is important that the final document - the BIA and Resource Requirements - is approved by your Head of Department.

Incidents and Impacts

Despite their being many different incidents/ causes of disruption, the impacts can be summarised in the categories above i.e. on resources.

	Staffing / Skills	Buildings / Facilities	Equipment and Finance
Identify	What staff are required to carry out priority activities?	What building/s are needed to continue priority activities?	What equipment is needed to continue priorities?
	What skills are needed for priority activities?	What alternatives are in place?	What alternatives do you have in place?
	What alternatives are in place?	Dependency on a specific location/facilities?	What alternative suppliers are available?
Check	Can key staff be contacted out of hours?	Could you operate from more than one location?	Do your key suppliers have business continuity arrangements?
	Are they/could they be trained in other roles?	How would you cope without heat, water, power?	Can you contact your key suppliers at any time?
	What documentation is in place for key tasks?	Where should key staff go when an incident occurs?	How could they support you during an incident?
	Could more be developed?	Could priorities be delivered using technology?	
Review	How would they cope with demand in an incident?	How easily could you relocate your priority work?	Reliance on a single supplier?
	Could other staff perform their role or other departments assist?	Would other departments be able to assist?	Actions to mitigate this?
	Could you outsource?	Are staff set up now to work from home?	How does the tendering / procurement process support you in an incident?
	Reciprocal arrangements?		

ICT and Data	Stakeholder / Reputation / Profile
What IT is required to continue priorities?	Who are the key stakeholders?
What documents are essential to continue - how are they stored?	What communications are required?
Communications required? Is there a manual alternative?	What are the legal/regulatory requirements?
How is data backed up electronically?	How will disruption affect strategic objectives, KPIs?
How are paper records stored?	How could reputational damage be reduced?
Who knows how to access this information/data?	Would any groups be vulnerable if you didn't perform?
Information security?	
Could paper records be scanned in?	How can you provide information to staff in the event of an incident?
Stored in fire proof safe?	Do you have arrangements to log, decisions, actions and costs?
How flexible are your systems?	
Does someone else also store this information?	

Stage 3

Developing Plans.

The plan to help you manage an incident.

The key outcome of the process is a Business Continuity Plan that can be used to manage any disruption caused by an incident.

What is a Business Continuity Plan?

A Business Continuity Plan (BCP) is a document to assist in managing an incident, helping to continue or recover priority activities at a pre-defined level.

Why complete a BCP?

The Plan should be used when an incident/ disruptive event occurs (or is expected to), that may affect the department's ability to continue as normal. Departments can identify their own triggers for it should be used.

The Business Continuity Plan provides a structure to manage the response at a stressful time. Having a plan means the approach is agreed, so even if the person "who usually deals with it" isn't available, then the Plan should help others to manage the situation.

What is the University's approach?

It is essential that a Business Impact Analysis is completed before developing a Plan, so the information in it has been discussed and agreed (see Stage 1). The University has a Business Continuity Plan template; sections can be adapted to suit the needs of individual departments. The BCP has the following sections to be completed:

Priority Activities and Resources
You should include the priority (most time sensitive) activities in the plan, with the resources to continue delivering them, identified in the BIA. The Plan should also have the agreed strategy or arrangements to manage a loss of any resources, so it is adaptable to deal with any incident - even if it's not one experienced before.

Roles and Responsibilities

The department needs to agree the system to manage the response:

- A team, with roles assigned and where possible deputies to cover absences (it usually wont be possible for one person to manage)
- A location for them to meet - and an alternative
- A record of events/decisions - someone should be asked to take notes.

The Plan needs to be accessible to those who need it. It should be stored in the incident contacts system, because this is hosted both on and off site and information can easily be shared.

Communications

Communications is essential when responding to an incident. Considerations for your department are:

- Who in the department should be notified when an incident occurs - during and outside of working hours. The incident contacts system stores details for the contacts the Security Control Room should inform - all Heads of Department and their chosen nominees have access to this.
- Other staff who need to be informed by internal processes, after the initial notification from the Control Room. Departmental Lists can also be added to the incident contacts system.
- A procedure is required to inform staff when the Plan - or part of it - is used and also when it is stood down, as it may affect them e.g. staff may be working from home and now need to attend their normal workplace.
- Key stakeholders should be noted in the plan and informed as appropriate. Media enquiries should be referred to the Media Team in Corporate Affairs.
- If the incident has a wider impact, a University Major Incident Team may form and communicating with them will be important.

Logging/Recording Information

It is important that records are maintained during an incident (an incident log example is in the plan). This information may be required for insurance or legal purposes and should be kept safely after the event.

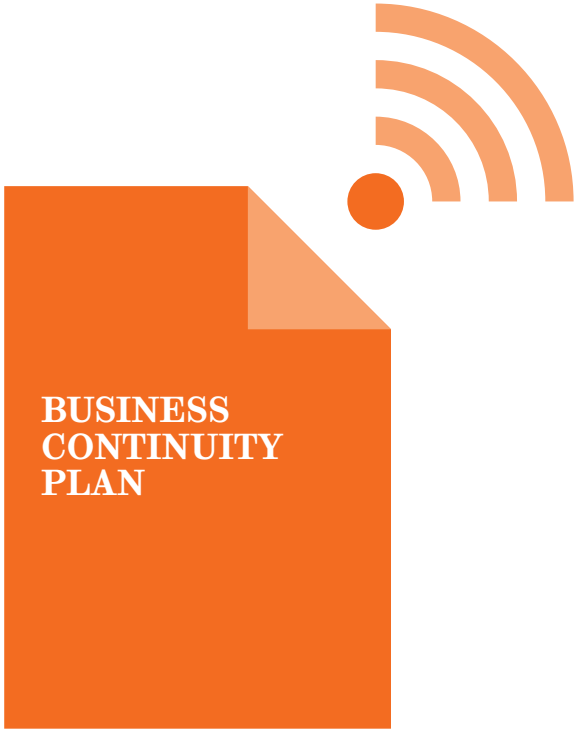
Checklist

The Checklist in the Plan notes considerations when managing an incident. They may not all be applicable, depending on the incident.

Completing the Plan

A plan co-ordinator is required to collate information and maintain the Plan. They are **not** responsible for providing all the information - it requires involvement from across the department. The Head of Department should approve the plan.

For the plan to be useful, people need to be familiar with it. The BCP needs to be circulated and a record kept of who has a copy in the Distribution section. The Plan should be updated annually as a minimum - and reviewed when there is a change that could affect it e.g. a restructure. The new version should be distributed so everyone has the latest version.



Stage 4

Reviewing and Exercising.

Ensuring your plan is relevant so it will work when needed.

In order to ensure arrangements in the plan can be used when an incident occurs, they need to be maintained and assessed (by exercising).

The Plan is complete?

It's easy to assume once a plan is in place that everything is complete - but the process is ongoing. Regular reviews are required to ensure arrangements are appropriate and realistic. This means checking the information in the Business Impact Analysis, Resource Requirements and BC Plan (Stages 1-3).

Reviews
The Business Impact Analysis and Business Continuity Plan have "owners" to maintain them. Owners are not responsible for providing all the information for these documents – they are co-ordinators to maintain them.

Reviews are required to ensure that when the plan is required, the information is up to date, so should take place:

- Annually for the BIA and BCP - dates/versions should be updated.
- When there is a significant change in the department that could impact on BC arrangements.

The Head of Department should approve changes. The update should be circulated so everyone has the latest version.

Exercises

After producing a Business Continuity Plan, the best way to assess how it will work during an incident is to hold an exercise. This enables a review of arrangements in a safe environment, without the pressure of a genuine incident.

Exercises can take a variety of formats, from a discussion about the plan to a live event with participants role-playing. A tabletop exercise is the most common, where participants are given a scenario and use the plan to respond. Plan co-ordinators should attend exercises, together with anyone who has an identified role in the Plan. Exercises can be run by the University's Business Continuity Manager or locally.

Incidents and Near Misses

Even once you have a Business Continuity Plan, incidents will happen. Or there may be occasions where an incident almost occurs but is prevented at the last minute, known as a near miss. These are useful opportunities to review the plan and identify lessons to help manage any disruptions in future.

Identifying Lessons

Exercises, incidents and near misses can be useful to identify areas for improvement, which helps to develop arrangements but also to continue good practice.

It is useful to hold a review to identify what worked well, what could be improved on and why. This review, known as a debrief, could range from a discussion, questionnaire or a formal meeting, or a combination of these, depending on what has happened. For major incidents and exercises, a formal report will usually be produced. In whatever format the debrief is held, it is essential to identify lessons – note they are not "learned" until action has been taken.

Audit

Business Continuity arrangements are subject to audit. This can be useful to review arrangements in place and identify areas for further work.

Governance

There is a Business Continuity Operational Group (BCOG) that meets regularly with representation from Professional Services and the Faculties. BCOG is chaired by the Director of CiCS and has developed a work programme. Part of its role is to review business continuity documentation; it also has a standing agenda item to discuss incidents and near misses to identify and share lessons.

The Business Continuity Steering Group (BCSG) has oversight of the Business Continuity Programme and approves the work of BCOG. Both groups are essential in the development of the University's Business Continuity arrangements, and lead in reviewing its implementation.

Useful Information.

There is more information about Business Continuity and Incident Management on the University's website at:

www.sheffield.ac.uk/incidents

Or by contacting the University's Business Continuity Manager: Jennie Christmas

Telephone: (0114) 222 3078
Email j.christmas@sheffield.ac.uk

Departmental/Faculty Business Continuity Representatives

For information about Business Continuity in your department, contact your faculty/ departmental representative:

www.shef.ac.uk/incidents/reps

Guidance on using the incident contacts system
www.shef.ac.uk/cics/incidentcontacts

Business Continuity Guidance for Learning and Teaching
www.sheffield.ac.uk/lets/pp/qa/bcp

Corporate
Information &
Computing
Services.

The
University
Of
Sheffield.