APPROACHES TO BUSINESS CONTINUITY

IN UNIVERSITIES

Foreword

Universities are large complex organisations that can face many challenges throughout their day-to-day operation. Ideally incidents are prevented and avoided. But if they do happen this guide can help senior teams minimise disruption and protect their institution and its community of students and staff.

Christopher Hale, Director of Policy, Universities UK

Contributing organisations

AHUA

AMOSSHE
The Student Services Organisation

ARC
ACADEMIC
REGISTRARS
COUNCIL

AUDE
ASSOCIATION OF UNIVERSITY
DIRECTORS OF ESTATES

bufdg
british universities
finance directors group

Jisc

SCONUL
Society of College, National & University Libraries

ucisa

Contents

1. Executive summary

back to contents

1. Executive summary

ASK YOURSELF...
What will a major incident do to your reputation?

1.1 Why should we be interested?

Running a university or college is becoming more complex and will only continue to do so in future.

Not only is the range of operations expanding, but the number of underlying services and facilities that those operations depend on increases almost daily. The growth of outsourcing and the migration to cloud services as a standard business practice for providing critical services simplifies some aspects of operations but can complicate others particularly when things go wrong.

This increasing complexity can lead to fragility – relatively small failures in one area can have unexpectedly severe impacts on the ability of the organisation to deliver essential services.

All the above is exacerbated by a heightening threat environment, particularly where cyber security is concerned. Universities and their suppliers are at increasing risk of disruption through cyber-attacks for attempted financial gain (ransomware[1], for example), as a demonstration of the hacker's capability or as a political protest.

At the same time, stakeholders – from students, to research clients to collaborating institutions – have increasing levels of expectation about an institution's ability to 'deliver the goods' no matter what. After all, this guaranteed level of service is part of what they are paying for.

There are several approaches to providing this guarantee:

- recognising and minimising threats in advance through *risk management*;
- responding promptly to events through *emergency management*;
- restoring normality as quickly as possible through *business recovery*; and
- being able to carry on essential functions during the disruption through *business continuity*.

> "Universities live in a billion-dollar world, but with 'small organisation' resources. Students expect us to be Amazon-like in service levels and robustness.[2]"

While risk management, emergency management and business recovery are relatively well-understood and implemented, business continuity tends to be less mature throughout the sector. In simpler times, it was usually possible for key staff to improvise their way round most problems. Today and in the future, a great deal more understanding and forward planning is likely to be needed.

Effective business continuity planning also has benefits for the institution even before it needs to be invoked. The process of putting the plan together will lead to a better shared understanding of the key business processes, activities, dependencies and supply chains. This in turn can highlight opportunities for improvements, resulting in a better student experience, growing stakeholder confidence, operating efficiencies and healthier working relationships with partners and suppliers.

[1] Malicious software designed to deny access to computer systems or data until a ransom is paid.

[2] All boxed quotes in this document are from one of the contributors listed in Section 1.4, Contributors to this guidance, unless otherwise stated.

back to contents

1. Executive summary continued

> "In our experience, the business continuity plan development activity itself leads to a better understanding of business processes and their changing priorities throughout the year."

1.2 Where does this guidance come from?

This guidance has been created with extensive input from representatives from universities and higher education organisations but will be equally applicable to further education. The publication is based on interviews with people who either have experience of business continuity planning or with dealing with a business continuity situation, or both. They come from a wide variety of professional disciplines.

The full list of contributing organisations is given in Section 1.4, Contributors to this guidance.

The guidance also takes into account the relevant ISO standard, *ISO / EN / BS 22301*[3] and a number of other relevant standards and guides.

1.3 Who needs to read this?

This document is of value to:

- Senior managers within higher education institutions, particularly those with accountability for business-critical processes. This might include Finance Directors, Chief Operating Officers, Registrars, Chief Information Officers, Directors of HR, Estates, Libraries and IT, Deans, Deputy Vice Chancellors and Pro Vice-Chancellors;
- Managers and others who will be involved in putting the business continuity plan together; and
- Those with oversight responsibilities, such as Vice-Chancellors, members of the Board of Governors, the audit sub-committee and auditors.

1.4 Contributors to this guidance

The lead author was Jerry Niman, of Jerry Niman IT Services, who also conducted interviews with the contributors listed below.

Chris Cobb, Pro Vice-Chancellor (Operations) and Chief Operating Officer, London University (On behalf of AHUA, the Association of Heads of University Administration)

Matt Cook, Assistant Director (Infrastructure and Operations), Loughborough University (former UCISA Networking Group Chair and UCISA Executive Committee Member)

Brian Hipkin, Chief Executive Officer and Founder, ReFRAME Higher Education Consultancy Limited and formerly Dean of Students, Regent's College (On behalf of AMOSSHE, The Student Services Organisation)

Sue Holmes, Director of Estates and Facilities, Oxford Brookes University (On behalf of AUDE, the Association of Directors of Estates)

[3] Continuity Management Systems – Requirements
https://www.bsigroup.com/en-GB/iso-22301-business-continuity/

back to contents

1. Executive summary continued

John Maher, Director of Learning and Information Services, University of the Highlands and Islands (former UCISA Corporate Information Systems Group Chair)

Kate McLaughlin-Flynn, Director of Finance and Resources, University of Cumbria (On behalf of BUFDG, the British University Finance Directors Group)

Maxine Melling, Pro-Vice Chancellor (Operations), University of Gloucestershire

Peter O'Rourke, Director of IT, University of Suffolk (UCISA Executive Committee Elected Member)

Russell Roberts, Head of Academic Services, University of Derby (On behalf of ARC, the Academic Registrars Council)

Mike Stephens, former Head of Safety, Security and Resilience, Medical Research Council (On behalf of HEBCoN, the HE Business Continuity Network)

Steve Terrill, IT Security and Business Continuity Manager, University of London

Dave Thornley, Head of Networks and Infrastructure, Sheffield Hallam University

Mark Toole, Head of Libraries and Learning Resources, Nottingham Trent University (On behalf of SCONUL, the Society of College, National and University Libraries)

Steve Watt, Chief Information Officer, University of Saint Andrews

Janet Whitworth, Chief Operating Officer, University of Cumbria

Shirley Wood, Head of Customer, Engagement and Support, Jisc Technologies

back to contents

1. Executive summary continued

Anna Mathews, Head of Policy and Projects at UCISA, was the project manager for this resource. The HEBCoN Executive Committee and the Chair (Mark Webster, Head of Business Resilience, University of the West of England) provided advice during the creation of this publication.

The following individuals from across the sector acted as critical friends during the drafting process:

Jennie Christmas, Business Continuity Manager, CiCS, University of Sheffield

Andrew Dixon, Head of Service Management Office, IT Services, University of Oxford

Sue Dummett, Business Continuity Advisor, University of Exeter

Heidi Fraser-Krauss, Director of Information Services, University of York

Paula Harrison-Woods, Director of Student Administration and Support, University of Liverpool

Shona Nairn-Smith, Business Support Manager, Bournemouth University

Chris Newby, Systems Infrastructure Manager, University of Bedfordshire

Caroline Pepper, Learning Environments Manager, Facilities Management, Loughborough University

Chris Reeves, Web and Identity Systems Team Leader, University of York

Bruce Rodger, Head of Infrastructure Services, Information Services, University of Strathclyde

Sarah Rowe, Business Continuity Improvement Project Manager, Kings College London

Caroline Rushmer, Major Incident and Business Continuity Manager, Oxford Brookes University

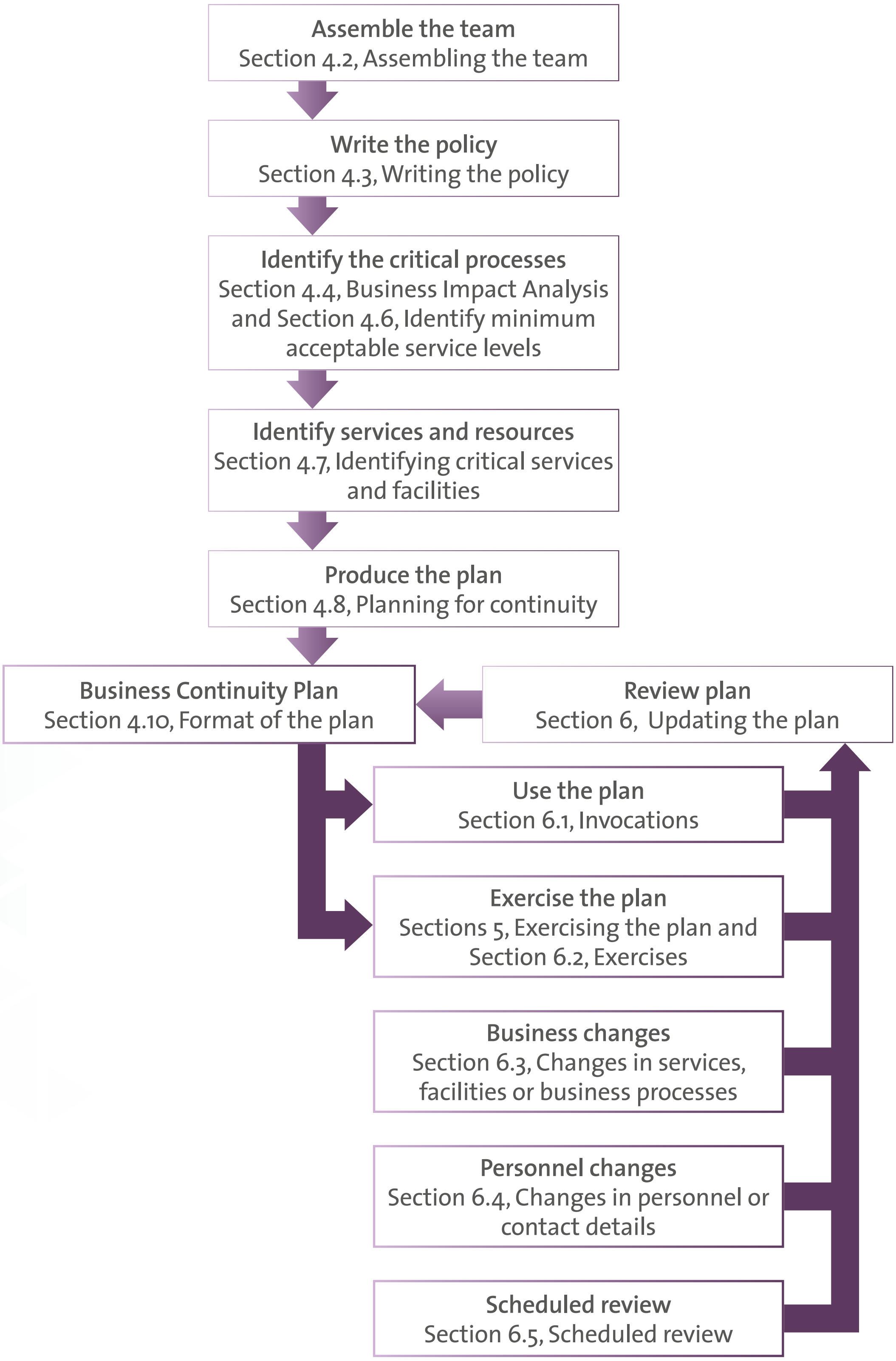
back to contents

2. Background

back to contents

2. Background

2.1 Route map for using this document



Assemble the team
Section 4.2, Assembling the team

Write the policy
Section 4.3, Writing the policy

Identify the critical processes
Section 4.4, Business Impact Analysis and Section 4.6, Identify minimum acceptable service levels

Identify services and resources
Section 4.7, Identifying critical services and facilities

Produce the plan
Section 4.8, Planning for continuity

Business Continuity Plan
Section 4.10, Format of the plan

Review plan
Section 6, Updating the plan

Use the plan
Section 6.1, Invocations

Exercise the plan
Sections 5, Exercising the plan and Section 6.2, Exercises

Business changes
Section 6.3, Changes in services, facilities or business processes

Personnel changes
Section 6.4, Changes in personnel or contact details

Scheduled review
Section 6.5, Scheduled review

back to contents

2. Background continued

2.2 Why now?

There have been several incidents recently that have had major impacts on higher education institutions or interrupted the services that they depend on. Other sectors have been equally affected, with hospitals, banks, air traffic control and global corporations all having major service outages.

The details of the incidents are many and varied, but they all had one thing in common – major disruption for the organisations and their customers. This has been an urgent topic of discussion in the higher education sector. A recurring theme is that although the service providers usually have well thought out plans for keeping customers informed and restoring services to normal as quickly as possible, sometimes the institutions themselves, as customers, are ill equipped to cope with the interruption. In some scenarios, an institution might struggle to carry out one or more essential business functions and would simply have to hope that normal service would be restored as soon as possible.

Recognising this, the community has increasingly focussed on the topic of business continuity and has voiced a need for sector specific best practice guidance.

ASK YOURSELF...
Three quarters of the staff of one of your departments have contracted food poisoning after a leaving party for the retiring head, and exams start in two days' time. Would you be able to cope?

2.3 Business continuity is a business issue

Disruptions can originate from many sources, not necessarily within the organisation. See Table 1, Possible sources of disruptions.

The expertise to produce the plans for keeping the business running lies in the areas owning the business processes affected, rather than in the areas owning the source of the disruption. Furthermore, business continuity planning cannot be allocated to a single area; it needs to take place in a coordinated manner within units across the whole organisation.   This publication has therefore been produced as a cross-professional collaboration between the organisations listed in Section 1.4, Contributors to this guidance.

Possible sources of disruptions

- Building fire
- Flooding
- Power outage
- Water supply failure
- Transport disruption
- Severe weather
- Medical epidemic, e.g. 'flu
- Industrial action
- Terrorism alert
- Exclusion from buildings because they are a crime scene
- Denial of service attack on the network
- Unexpected network outage
- Ransomware infection
- Vermin infestation
- Legionella infection
- Adverse social media storm
- Loss of mass personal data
- Damage caused by building and maintenance activities
- Discovery of asbestos
- HSE notifiable event
- Chemical incident
- Failure to renew contract with major monopoly supplier

Table 1 Possible sources of disruptions

2. Background continued

2.4 The need for a business continuity planning introduction for higher education

There is a wealth of material available about business continuity planning[4].

However, much of the guidance material assumes either a 'typical' commercial organisation or a government body. There is little material that addresses the unique challenges of a higher education institute.

The relevant ISO standard – *ISO / EN / BS 22301*[5], specifies requirements for setting up and managing an effective Business Continuity Management System. It does not give practical guidance on how to go about business continuity planning.

The Higher Education Business Continuity Network (HEBCoN[6]) is a network of higher education institutions in the UK and Ireland who are committed to sharing and promoting good practice in business continuity management, risk management and emergency planning. They offer expertise and support in these areas, including training courses, but not a general introduction to the topic for those unfamiliar with it. (See Section 9 Further information on HEBCoN and the BCI).

There is also a great deal of information dealing with the closely related areas of emergency management planning and business recovery planning. For example, the Association of University Chief Security Officers (AUCSO[7]) has produced a guide, *Resilience in Higher Education*[8], containing information and advice on good practice in emergency management with specific reference to higher education institutions in the UK.

2.5 How this document will help

This document will:

- explain how business continuity, emergency management and business recovery relate to each other and to risk management;
- give advice and guidance to senior managers who wish to set up arrangements to produce and maintain their business continuity plans;
- provide examples and case studies that will help with the process;
- give governors and others with oversight responsibilities an insight into what business continuity arrangements they should expect to find in place; and
- provide pointers to other relevant resources and organisations.

2.6 What this document does not do

Each institution faces different challenges and will need to decide for itself what business continuity arrangements meet its particular needs. This document is not intended as a set of step by step instructions for producing a

[4] 4·3 million hits on Google as of February 2018
[5] https://www.iso.org/standard/50038.html
[6] www.hebcon.org/
[7] www.aucso.org/
[8] http://eprints.lincoln.ac.uk/26747/1/26747%20resilience-in-higher-education-institutions_compressed_2__3480-4%20%281%29.pdf

back to contents

business continuity plan, nor does it specify what should be in those plans.

This introduction is not intended to be your institution's passport to gaining accreditation to ISO/EN/BS 22301 (although following it will certainly be a step in the right direction).

This document does not give guidance on emergency management or business recovery, except where the topics overlap with business continuity. (See Section 3.5, How risk management, emergency management, business continuity and business recovery relate to each other).

back to contents

3. What is business continuity?

back to contents

3. What is business continuity?

> "Good business continuity planning might be as much about the questions to ask as the answers."

In their shoes...

You are the Vice-Chancellor of a university. You have been concerned about the devastation to local economies caused by recent severe weather and wonder how well your institution would cope in similar circumstances. Would staff be able to get in, might there be power cuts, would the supply chain hold up? There is a disaster recovery plan, but fortunately, the university has not had to deal with any major incidents for quite a while. How would you go about establishing how resilient the institution really is?

One of the difficulties for anyone working in this area is that a variety of terms are used almost interchangeably. This can give the impression that *incident management, emergency planning, business continuity* and *business recovery* all mean roughly the same thing, so one approach, one plan, and one team can handle everything. After all, it is about sorting things out when something goes wrong. In fact, there are four distinct aspects of "sorting things out" that need to be considered.

They are each known by a variety of names, but this document will refer to them as:

- risk management;
- emergency management;
- business recovery; and
- business continuity.

3.1 Risk management

Risk management refers to the overall approach for handling risk in an organisation.

It involves the systematic identification of threats, their assessment and prioritisation, and the implementation of responses to reduce the likelihood of the threats being realised and/or reduce their impact should they occur.

Typically, risk management will take place at several levels within the organisation, with mechanisms to promote the most significant risks from the departmental or project level towards an overall organisation risk register.

3.2 Emergency management

Emergency management refers to the immediate actions an organisation needs to take when an incident occurs that impacts the normal operations and requires a different response. The concept involves a focus on an initial response to the situation and responding to the short-term requirements of those affected by the emergency. Emergency management is likely to involve liaison with multiple agencies, and establishing an effective communications chain is a key consideration.

back to contents

3. What is business continuity? continued

> "Business continuity is what the business experts do while the technical experts try to glue stuff back together."

ASK YOURSELF...

When you talk with your colleagues about emergency management, business recovery and business continuity, are you sure you are talking about the same things?

3.3 Business continuity

Business continuity is defined as the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business continuity will involve making whatever temporary arrangements are necessary for the organisation to continue with its essential functions. Depending on how long business recovery takes, the business continuity arrangements may need to be in place for considerable time.

3.4 Business recovery

Business recovery is the process of restoring the full functionality of the processes, services and/or facilities affected by the incident. It could involve repairing or replacing a lost building, restoring multiple computer systems or replacing study spaces and re-stocking a library after a flood. This is also referred to as disaster recovery. It will involve re-introducing normal day-to-day operations, often alongside the business continuity arrangements.

Business recovery can, depending on the nature of the service affected, be a complex and time-consuming activity. It does not necessarily involve restoring things exactly as they were before – sometimes the opportunity should be taken to do things differently.

3.5 How risk management, emergency management, business continuity and business recovery relate to each other

If planning and management for incidents is to be effective, it is important to understand how these approaches relate to each other.

Emergency management, business continuity and business recovery are planning and incident response processes that are intended to reduce the impacts of threats as part of an overall risk management approach.

While the process of planning how to deal with threats may well highlight opportunities to reduce the likelihood of them occurring, this is a welcome by-product and is not their primary focus.

While all three are approaches could be applied *on the hoof*, they are far more effective if there has been some degree of planning. Indeed, ad hoc emergency management could make a serious incident a whole lot worse.

Table 2, Risk management and the three incident response processes, summarises some of the key relationships between them.

3. What is business continuity? continued

"Make sure there is an external communications plan, especially for incidents affecting information security."

Approach	Description	Drivers
Risk management	How do we prevent fires? How can we limit fire damage?	Concern for the short, medium and long-term viability of the organisation
Emergency management	Get everyone out and call the fire and rescue service. Talk to media and students' parents.	Concern for the immediate welfare of those affected by the incident.
Business continuity	Find everyone places to eat, sleep and work.	Concern for the medium-term welfare of those affected by the incident, and the short-term viability of the organisation
Business recovery	Repair the building or relocate and replace the lost possessions.	Concern for the medium-term viability of the organisation.

Table 2 Risk management and the three incident response processes

Another way to picture the relationships is illustrated in Figure 1, Incident Timeline.

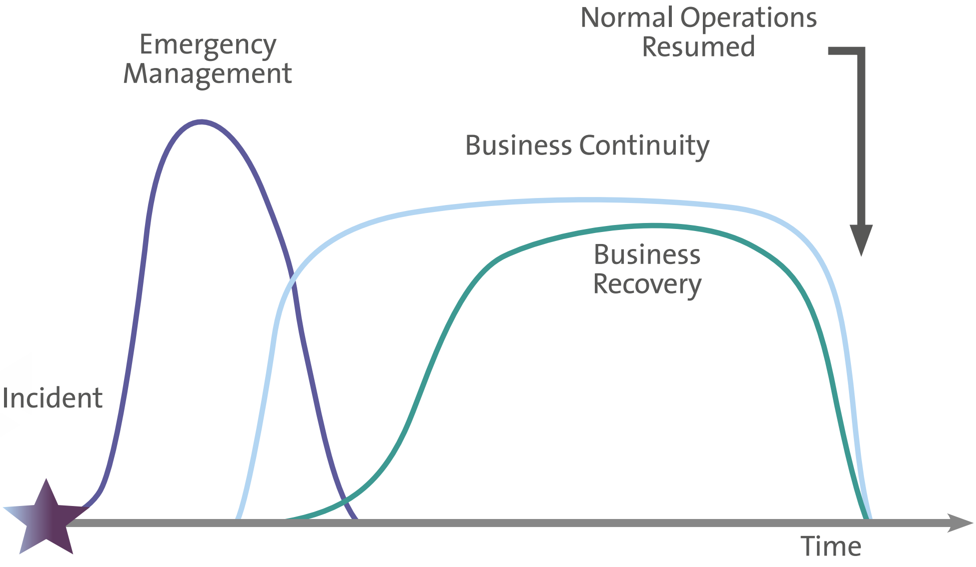


Figure 1 Incident timeline

Of course, in the real word, it is impossible to draw absolute distinctions between the emergency management, business continuity and business recovery processes. All three are bound to overlap considerably, in terms of the timing (business recovery and business continuity may both start while emergency management is active), the people involved, and the communications channels used. The plans for these incident response processes need to refer to each other where appropriate.

For example, organisations are likely to have Gold, Silver and Bronze team arrangements[9] for emergency management. The organisation for business continuity is likely to involve a slightly different set of people, and business

[9] A command structure used to establish a hierarchical framework for the command and control of responses to incidents. It is sometimes called strategic, tactical and operational command structure.

3. What is business continuity? continued

recovery possibly another set, but many key individuals will be involved in all three, and there needs to be an overall structure that manages the transition and overlaps between the phases of incident response. Furthermore, communication within the teams and with stakeholders needs to be well coordinated at all stages.

Nevertheless, the three processes have different characteristics (see Table 3, Comparison between the three incident response processes) and will benefit from being treated as distinct but related exercises.

	Emergency Management	Business Continuity	Business recovery
Emphasis	• Establishing what has happened. • Safety concerns. • Establishing communications channels. • Stakeholder communications.	• Continuation of essential business functions.	• Re-establishing stable operations. • Look for opportunities for improvement.
Knowledge	• Often imperfect initial information about the incident. • Important to build understanding of the implications of the incident and initial impacts.	• Continuity actions taken based on available information.	• Incident well understood.
Control	• Emergency services may be in control initially.	• Organisation in control.	• Organisation in control.
Starts	• As soon as possible.	• As soon as the situation is stable and the extent of disruption determined.	• As soon as business continuity arrangements are activated.
Continues until	• The situation is stable and business continuity arrangements are activated.	• Normal operations are resumed.	• Normal operations are resumed, and the backlog dealt with.
Planning	• Often restricted to establishing communication channels, informing stakeholders and response team. • Plan needs to be short and portable.	• Depth of planning varies by facilities and processes affected. • Plans can be as detailed as required.	• Depth of planning varies by facilities affected. • Plans can be as detailed as required.
Led by	• The Gold, Silver and Bronze teams.	• People responsible for the critical business processes.	• People responsible for the facilities affected by the incident.

Table 3 Comparison between the three incident response processes

back to contents

3. What is business continuity? continued

It is also worth remembering that not all business continuity situations start with an incident that is obviously an emergency. Examples might include a postal strike or a hacking attempt on the institution's network. It should not, therefore, be presumed that the emergency management plan has been invoked in all situations where business continuity and/or business recovery are needed.

3.6 Other names

Unfortunately, while there is general recognition of the three phases of incident response, there is no widespread agreement on the use of the terms emergency management, business continuity and business recovery.

Emergency management might be referred to as crisis management, incident management, major incident management or disaster management.

Business recovery is sometimes confusingly referred to as disaster recovery, particularly in the sense of a standby facility that can provide a temporary service until normal operations can be restored. This could be some transportable buildings equipped as offices to provide temporary working space, a standby generator or a truck full of computer hardware to provide a temporary student records or finance system service. These should really be thought of as *business continuity facilities*. The term disaster recovery is often used in the context of information and communications technology, where it refers to the process of resuming the provision of services (particularly the critical services) as soon as possible.

In some contexts, business continuity is used as an umbrella term covering both the temporary arrangements necessary to support critical business functions and the process of restoring the disrupted facilities to normal. HEBCoN uses the term business continuity in this overarching sense.

The term business recovery is sometimes known as recovery and resumption, or simply as recovery. In IT, the term disaster recovery is frequently used in this context.

For the moment, there is no set of terms that everyone can agree on, and the labels adopted in this document are the ones that seem to cover the most common ground.

back to contents

4. Producing the plan

4. Producing the plan

> "Get something written down. Start with a basic plan and an effective team and build from there. Using an audit-based tool, while useful in some instances, can make things too complex to get started. Instead use the right team and a few scenarios."

> "Don't try to capture every possible eventuality. Approach, communication and flexibility are key. Get the right people together with the right list of questions. What is the impact of this situation on our major customers? What about our more indirect customers? (This varies at different time of the year)."

> "The challenge in producing a plan is prioritising and getting people to engage with the organisation. Very visible senior management buy in is critical of course, but as important is making the case to everyone at the coal face."

This section sets out one approach to producing a business continuity plan. The approach presented is highly systematic, and should produce a comprehensive and detailed set of plans.

However, depending on how much is already known about business processes, following this approach to its conclusion could be a lengthy exercise. As any plan is better than none at all, it may well be worth producing a 'quick and dirty' version based on the existing knowledge and experience of the business continuity team members, and the communications protocols established in the organisation's emergency management plan. The business continuity plan can then be refined as soon as possible in the light of a more thorough analysis.

4.1 Responsibilities for business continuity planning

In their shoes...

As a member of the Risk and Audit Committee, you are reviewing the draft Business Continuity Policy. The policy suggests that the Director of Estates should have overall responsibility for business continuity exercises, as she is most likely to have the best understanding of what to do in the event of fires, floods, electricity, gas or water supply failures. Does this sound like a good idea?

Leadership and overall responsibility for producing the business continuity plans should be given to an appropriate role, such as the Secretary, Registrar or the Chief Operating Officer.

The person in this role should have:

- sufficient authority to release any resources necessary;
- the interpersonal skills necessary to foster effective team working across functional boundaries;
- a sound understanding of the business-critical processes;
- sufficient time to oversee the planning process; and
- excellent organisational skills and a systematic approach.

Producing, exercising and maintaining a business continuity plan is unlikely to be a short process, and the person in the responsible role will also need some degree of staying power.

back to contents

4. Producing the plan continued

"Thinking about possible challenges to running the business is key and capturing something - even if fairly basic - will mean that if disaster strikes you have a head start."

"The terms of reference are to create a modular business continuity plan that meets need of the institution as well as each individual department. There should be an overarching plan supported by departmental plans beneath. These should be modular, but not isolationist."

ASK YOURSELF...
Who are the best people to lead on business continuity – the people responsible for business processes, or the people responsible for the services and facilities they usually depend on?

4.2 Assembling the team

"It's important to maintain motivation beyond the initial enthusiasm once people understand the level of effort required."

Management of the planning process should be vested in a team of people representing a good cross section of the functional areas of the organisation. A balance should be found between ensuring that all critical business processes are covered and keeping the team to a manageable size.

The members of the team should be selected for:

- their collectively broad and deep understanding of the business processes;
- their capacity to devote the time necessary to the process; and
- their ability to engage others in the detailed planning.

"It is taken as read that the organisation must have business continuity plans. The problems may occur at lower levels with middle managers actually finding the time to undertake the discovery, analysis and planning."

It might be tempting to select these people from the 'Head of...' level. While there is nothing wrong with this, it should be remembered that sometimes the detail of many business processes is known best by those with day to day, front line operational experience.

"Service heads aren't necessarily the best people to know what goes on at the coal face. They may be unaware of the everyday work-rounds that their staff can use."

Example of Business Continuity Planning Team

Business Continuity Manager (Chair)
Two representatives (typically a deputy/associate director and a senior manager) from each of:

- Finance and Planning;
- Human Resources;
- IT;
- Property and Facilities Management;
- Student Services;
- Library;
- the Vice-Chancellor's department; and
- academic department/schools.

It would be unworkable for everyone to be on the planning team, so the team members should seek out and engage with those who understand how things really work.

4. Producing the plan continued

ASK YOURSELF...
How will your institution recognise that it needs to invoke the business continuity plan?

> "Don't set the bar too high! Likewise, don't involve the Vice-Chancellor in every network failure."

4.3 Writing the policy

One of the first tasks for the planning team is to produce a business continuity policy. This should follow the standard policy format of the institution, and should cover at least the issues set out in Table 4, Points to be addressed by the business continuity policy:

Policy item	Description
Aims	• What is the policy trying to do? Something along the lines of "This policy sets out the measures taken by the institution to minimise the impact of adverse incidents by planning how essential business functions would be carried out at acceptable levels despite the services and facilities they normally rely on being disrupted".
Scope	• This should set out how widely the policy applies, for example is it specific to one location? Does it cover spin-out companies, overseas campuses, student union operations? Bear in mind that some activities will inevitably be linked to the institution in the public perception, even if another legal entity is, strictly speaking, responsible. • It may be useful for the scope to be specific about what is not covered, for example emergency management and business recovery processes. • You might also consider putting an upper limit on the scale of disruption that business continuity arrangements are expected to handle, i.e. circumstances under which no-one would expect a University to continue to function.
Responsibilities	• The general responsibilities of different roles with respect to business continuity planning should be set out. These roles might include the Vice- Chancellor, governing body, executive team, the individual leading business continuity planning, the planning team, functional and academic heads, project management and change management boards, staff. • Specific responsibilities with respect to individual business processes and supporting services are more likely to be set out in the plan than in the policy.
Invocation	• How will the business continuity plan be invoked? There should be some linkage to the emergency management plan, but remember that not all business continuity situations follow emergencies.
Exercising	• This policy statement on exercising should give some sense of the balance to be struck between realism and pragmatism. The more realistic the exercise, the more disruptive it is likely to be, and so the less frequently the institution might be inclined to undertake it. • The general approach set out in the policy should in turn guide decisions on questions such as: How will the plan be exercised, (for example a table top activity or something more realistic)? How often will the plan be exercised? Will there be any prior notice?
Continuous improvement	• The policy should set out how the business continuity plan will be improved in response to: invocations, exercises, changes to processes, changes to the organisation, and on a regular review cycle.

Table 4 Points to be addressed by the business continuity policy

back to contents

4. Producing the plan continued

It may turn out that some of the points covered in the policy will need to be refined in the light of detailed planning. For example, unexpected dependencies might turn out that require the scope of business continuity to be expanded.

For this reason, it may be expedient to seek approval in principle for the draft policy, with formal approval for the finalised policy following the first iteration of planning.

4.4 Business impact analysis

ASK YOURSELF...
Does your institution have comprehensive descriptions of all its critical business processes?

The first stage of the planning process is to identify the business-critical activities, that is which functions the institution **must** continue to provide. This is done through business impact analysis - the process of analysing activities and the effect that a business disruption might have upon them.

These activities might include:

- accommodating students;
- feeding students and staff;
- paying staff wages;
- making offers of places to candidates;
- delivering lectures and providing access to learning and research resources;
- assessment, marking and examination boards;
- ensuring the welfare of overseas students or staff who are doing research or are on a placement or field trip; and
- conducting research.

This stage will be much easier if the institution has already documented all its business processes, however in most cases the planning team will have to identify them based on their own knowledge. The team should be conscious of the limits of their collective experience and consider ways to flush out any critical business processes they may have missed, for example by asking functional heads to review their draft list of essential business processes.

Be particularly alert for *submarine* business processes that might be operated locally to bypass central approaches. For example, one department might hold its exam boards later than others and in the event of a disruption to the student records system, the business continuity team might not know that this department's board are affected.

When drawing up this list, remember that the two criteria for a critical business process are that:

1. it must be a business process; and
2. it must be critical.

Many things are likely to be identified that are not really business processes, for example the student records system or a centrally located building housing several lecture rooms. While these are no doubt very important services or

back to contents

“Beware of over-egging the importance of ‘your’ systems and processes – are things really that critical?”

facilities, the business processes that they support (i.e. being able to identify and contact students and being able to deliver lectures respectively) could be carried out in different ways, at least on a temporary basis. Remember to keep a distinction between what needs to be done, and what is normally needed to do it.

How critical a business process is perceived to be will depend on several factors, including:

- what the business process actually does;
- when the disruption occurs relative to the business process cycle;
- how long the disruption is likely to last; and
- who is doing the assessment.

Business processes should be ranked by how critical they are from an institutional perspective. While, for example, paying suppliers may be seen a very important by the finance department, from an institutional perspective, suppliers might reasonably be expected to wait for payment until the disruption is over.

ASK YOURSELF...
Is there an institutional calendar or other source of information of what needs to happen when throughout the academic year?

The criticality of a business process often varies from month to month, or even day to day. For example, the business processes for clearing, HESA returns or exam boards can be crucial to an institution for a few days per year, but irrelevant most of the time. At this stage, it is probably most productive to consider the ‘peak’ importance of a business process.

Remember that the aim is to produce a list of all the business processes that need to be addressed in the business continuity plan, starting with those that are the most important.

Exactly how the business processes are identified and ranked will be for the planning team to decide. Guidance is available from many sources, including ISO/TS 22317:2015[10].

It would be valuable to add to the list any information readily available about variations in the importance of each business process at different times. This can be updated as more detailed analysis of each business process takes place.

The following steps, covering:

- Identify Maximum Tolerable Periods of Disruption (Section 4.5);
- Identify minimum acceptable service levels (Section 4.6);
- Identifying critical services and facilities (Section 4.7); and
- Planning for continuity (Section 4.8)

should be repeated for each of the critical business processes.

4.5 Identify Maximum Tolerable Periods of Disruption

The Maximum Tolerable Period of Disruption (MTPoD) is defined in BS25999 as “duration after which an organization’s viability will be irrevocably threatened if product and service delivery cannot be resumed”. In other words: how long can

back to contents

[10] https://www.iso.org/standard/50054.html

the organisation tolerate a business-critical process not being performed? This will vary with the business process, and in many cases with the time of year. It is important to know the MTPoD when considering continuity planning.

4.6 Identify minimum acceptable service levels

Following a serious incident, it is likely that service levels for some business processes will have to be reduced.

It will be essential for the business continuity planning to consider how much of a reduction would be acceptable.

For example, during normal operations it may be normal to offer a choice of three hot main courses at lunchtime in the student refectory. In a business continuity situation, it is still essential to ensure that students are fed, but it may be that a reduced level of choice is offered, or an alternative food outlet is used.

In some cases, the reduction in service level will also be varied depending on the length of the disruption. For example, Table 5, Example of service levels varying by length of disruption, shows how different service levels might be specified for supplier payments.

Length of disruption	Continuity Service Level
Up to 1 week	All supplier payment suspended
Up to 2 weeks	All supplier payments over £10k paid by manual processes
Over 2 weeks	All suppliers paid by manual processes

Table 5 Example of service levels varying by length of disruption

These variations may also be determined by when the disruption occurs. For example, the maximum acceptable delay in processing requests for prospectuses might be different at different times of the year.

In some cases, no reduction is service would be acceptable. In some instances, service levels would need to be higher than normal (for example handling media enquiries).

These minimum acceptable service levels must be driven by the business, health and safety and/or regulatory requirements, and not by considerations of what is likely to be straightforward to provide. At the same time, they should not be set any higher than the minimum levels necessary, and the owner of the business process should be prepared to justify the levels specified.

It will also be important to identify how quickly the 'continuity' service needs to be put in place.

On completion of this step, there will be a clear statement of the minimum acceptable levels of service for the business process and how quickly it needs to be provided, together with any variations due to the duration and/or timing of the disruption or any other factors.

4. Producing the plan continued

ASK YOURSELF...
What services and facilities need to be in place for freshers' week?
What about open days?

4.7 Identifying critical services and facilities

For each critical business process, it is helpful to identify the services and facilities that the process depends on. This will help to focus attention on the various ways in which the business process could be compromised when it comes to producing a continuity plan for the process.

These supporting services and facilities could be:

- Utilities such as electricity, gas, water;
- IT services such as email, network connectivity, virtual learning environment, student records system, telephones;
- Buildings or plant (e.g. student halls, library or a central boiler);
- Physical access (to a campus or part of a campus);
- People (groups of people or specific individuals); or
- External supplies or services such as food deliveries, scholarly publishers, postal services, BACS, public transport or local car parks.

> "We were quite shocked to learn about some of the things our critical processes depended on."

The most straightforward way to identify these services and facilities is by inspection of a business process diagram for the process, if one exists. If there is no existing process diagram, it will almost certainly be necessary to produce one for the next step, Section 4.8 Planning for continuity.

Take care to seek out hidden dependencies. For example, while a clearing call centre might be located in one building, the extra telephone handsets required might be stored in a different building for most of the year. Access to this store room therefore becomes critical for the clearing business process.

Consider how quickly these services could be restored after a disruption. This is often referred to as the Recovery Time Objective or RTO, and will be important when considering the next step.

Another important outcome of this step is to assemble a matrix showing which business processes are affected by disruptions to any given service or facility. Depending on how many services and facilities there are and the number of critical business services covered, some thought will have to be applied to how this matrix would be presented – it is unlikely to fit on one side of A4 paper!

Having such a matrix will allow faster impact analysis when an incident happens, as it is likely that in the early stages it will be easier to identify the services and facilities disrupted than the business processes affected.

ASK YOURSELF...
How would you respond to a Friday evening phone call to tell you there is gas leak, or that student data had been leaked?

4.8 Planning for continuity

At this point, there should be a statement of the Maximum Tolerable Period of Disruption (MTPoD) for each business-critical process under consideration, minimum acceptable service levels and a list of the services and facilities that it depends on, each with their Real Time Objectives (RTOs).

If the MTPoD is greater than the largest RTO (and you have complete confidence in both figures), then no specific action needs to be taken – the process should be up and running again within an acceptable window.

back to contents

However, in many cases, the RTO of at least some of the services will exceed the MTPoD of a business-critical process, so you will have to plan interim arrangements that will be in place within the MTPoD and that meet the minimum acceptable service levels.

The next step is therefore to plan how the minimum acceptable service levels can be met in the absence of some or all of the normal services and facilities.

For example, in the case of staff payroll, the minimum acceptable service might be that staff receive approximately the correct amount on the usual day of the month, but without a pay slip and without submitting the usual Real Time Information (RTI) to HMRC. This process would normally require the HR and/or Finance systems, plus the electronic link to the BACS service of the institution's bank and the electronic link to HMRC's RTI service.

A business continuity plan that caters for most eventualities is to lodge a 'standard' payroll BACS run with the bank, and to have an agreed protocol with the bank to authorise them to run this standard payroll in the event of a major incident. The RTI submission to HMRC may have to wait until normal operations are restored, and if this is not the first late submission, there might be a penalty imposed[11].

Note that there are:

- actions that need to happen in advance of any incident (and therefore as soon as practicable after the business continuity plan is agreed);
- actions that need to be invoked in the event of an incident; and
- actions that need to happen after an incident.

Table 6, Business continuity actions for payroll, gives an example of these actions for a payroll run. This is not meant to be exhaustive, your organisation will need to think this through in detail for itself. For example, are there times of year with a high number of new starters, and would you do anything differently in this case?

Phase	Description
Prior to incident	• Set up and maintain a standard payroll run lodged with the bank. • Agree protocols with the bank for invoking the standard payroll run, to be invoked by anyone from an agreed pool of staff.
During incident	• Use available communications channels to inform staff of payroll arrangements. • Use the agreed protocol to ask the bank to run the standard payroll. • Inform HMRC that PAYE RTI submission will be late, and why.
After incident	• Determine how pay adjustments will be made. • Consider additional payments for staff to recognise work during the disruption. • Inform staff of how payroll adjustments will be made. • Issue payslips for the emergency payroll run. • Update finance system with details of payments actually made. • Update HMRC on the situation, and pay penalty if imposed. • Submit missing PAYE RTI information to HMRC. • Run 'recovery' payroll handling adjustments and any additional payments.

Table 6 Business continuity actions for payroll

[11] Employers when submitting late have the option via the payroll software being used to indicate reasonable excuse before sending any late RTI submission, this ensures no late filing charge would be applied. If this is done consistently and filed late using the reasonable excuse option, it would eventually be challenged.

back to contents

4. Producing the plan continued

ASK YOURSELF…
What support can you expect from your key suppliers in an emergency? Can they provide extra services? How is this to be invoked? Is this written into the contracts? Who owns that information and who is responsible for that plan?

Note that if there are multiple minimum acceptable service levels, the plan will need to cater for them, either by having multiple variants or having multiple stages within the relevant sections.

The plan should be reviewed to ensure that:

- It is realistic;
- It is understood by the appropriate audience;
- It delivers the minimum acceptable service level;
- It can operate in the absence of the people, services and facilities the process would normally rely on;
- It identifies all the actions that need to be taken, particularly those that need to be taken in advance; and
- It is consistent with the known business continuity plans for other processes (e.g. the protocol agreed with the bank for invoking the standard payroll does not conflict with or duplicate the protocol agreed with the bank for emergency supplier payments).

One approach to undertaking this review might be to run a *table top* exercise to take the plan through a suitable scenario.

During the planning process, it may turn out to be impossible to meet the minimum acceptable service levels. Suitable adjustments to these levels should be agreed with the business process owner and the risk register updated accordingly to reflect the risk appetite agreed, if necessary.

Similarly, if the detailed planning shows that the normal operation depends on more services and facilities than originally listed, this should be noted.

The person responsible for taking forward the pre-incident actions should be identified, together with agreed timescales for implementation and a suitable mechanism to track progress.

Finally, the business continuity plans should be checked against any existing business recovery plans for the service and facilities involved. For example, in the payroll scenario above, the interim payments made will need to be taken into account when the finance system is brought back up.

ASK YOURSELF…
What support can you expect from outside agencies (emergency services, local government, other institutions, local businesses) in the event of an emergency? Do you know how to find/contact them quickly? How can you use multiple campuses, if you have them? Can the institution's insurers help (either in putting the plan together, or during a business continuity situation)?

4.9 Planning for communication

It is very important to make sure that the business continuity plan considers all aspects of communication.

Consider who you need to communicate with, when, how, about what, and who will be communicating with them. Check that this coordinates well with the communications aspects of the emergency management and business recovery plans.

Key stakeholders might include:

- Students;
- Parents or guardians;
- Student sponsor companies;

back to contents

4. Producing the plan continued

> "One of the most useful things we did was to issue corporate payment cards to key staff so we could buy things quickly when we needed to."

> "It's not meant to be *War and Peace*. You need no more five pages at top level. Means to communicate is absolutely key, including having a director available at all times."

- Staff;
- Key suppliers and commercial partners;
- Neighbours;
- Press;
- Governing body;
- Regulators, funders and accreditation bodies (if the disruption is likely to be lengthy);
- Conference, events and residential customers; and
- Research collaborators.

4.10 Format of the plan

The following sections are recommended for the business continuity plan:

- Introduction;
- Communication channels;
- Links to other information;
- List of critical business processes;
- Matrix of services and facilities; and
- Business continuity plans for each critical business process.

These are explained in more detail in Table 7, Suggested sections for the business continuity plan

Section	Description
Introduction	Explains the purpose of the document, the structure of the document and the relationship of business continuity to other process that are in place, in particular emergency management and business recovery.
Communication channels	Sets out in general terms how communications will work in the event of an incident, and who has authority for what aspects of managing the situation etc. Ensures that there is 24/7 cover where necessary and/or that key personnel have at least one trained deputy to cover absence. Sets out how to contact key stakeholders both inside and beyond the institution and highlights backup channels of communication. In most cases, this will have been worked through in considerable detail in the emergency management plan, and the business continuity plan should aim to build on that rather than try to start from scratch.
Links to other information	References to the business continuity policy, the emergency management plan, the business recovery plan and any other information that might prove useful, such as any information or services provided by the institution's insurers.
List of critical business processes	A listing of the business-critical processes, who the owners are, key activity points in the academic year, the minimum acceptable service levels, how these vary at different times and whether there is a business continuity plan for them.
Matrix of services and facilities	A matrix of the services and facilities likely to be affected by an incident, together with the critical business process affected by any disruption to them.
Business continuity plans for each critical business process	The detail of the business continuity arrangements for each business process. These could be in the main body of the document or in separate sub-documents. These need to set out the resources needed, the people and suppliers involved together with contact details and alternatives.

Table 7 Suggested sections for the business continuity plan

back to contents

4. Producing the plan continued

> “Make it a live conversation rather than dead documentation. The end result of effective business continuity planning needs to be captured in strengthened networks of contacts, improved business process, practice and staff capability rather than in a thick book.”

The physical format for the business continuity plan will be determined by balancing several requirements:

- It will be a substantial document, as it will contain a considerable amount of detailed content;
- Unlike the emergency management plan, it is not necessary for people to carry it with them at all times, as long as they can access it reasonably quickly and without relying on services that may have been disrupted by the incident;
- It needs to be in a format that allows for frequent updating; and
- It is likely to contain sensitive information.

Table 8, Advantages of physical and electronic formats, summarises the relative merits of each.

Issue	Hard copy	Electronic
Convenience	Easy to access, but vulnerable to being left in the wrong place.	Requires access to an electronic device with the latest version stored, or connectivity to the source of the document.
Ease of update	Presents issues ensuring that everyone has an up to date copy.	Copies always up to date unless stored locally on a device.
Confidentiality	Could be lost.	Vulnerable to accidental disclosure or deliberate hacking.
Tailoring	Holders can just keep the sections relevant to them.	Holders can just read the sections relevant to them.
Robustness of access	Not usually a problem, unless copy has been left somewhere.	Depends on having a robust location for central storage, or good mechanisms for distribution of local copies.
Environmental	Can use a lot of paper.	Should be more sustainable, unless everyone prints hard copies anyway.

Table 8 Advantages of physical and electronic formats

In the end, the format will be a decision for the institution to take, bearing in mind the maturity of its use of electronic information and the robustness of its IT infrastructure. Some institutions may wish to take a *belt-and-braces* approach and have both formats.

back to contents

5. Exercising the plan

back to contents

5. Exercising the plan

ASK YOURSELF...
How do you know your business continuity arrangements are fit for purpose?

IN THEIR SHOES...

You are a member of the Board of Governors, where there has been discussion about a draft business continuity policy, and in particular what the frequency of exercises ought to be. The Chief Operating Officer feels that frequent exercises would be too disruptive, could lead to complacency and would probably not generate much of real value. The University's legal advisor points out that the University has undertaken a number of research contracts which mandate regularly tested business continuity arrangements. The Chair has asked your opinion.

Writing a business continuity plan is one thing; knowing that it will work in practice is something else.

A genuine business continuity situation will throw up all kinds of complications that might not have been anticipated in the planning stage, for example:

- key staff may not be available;
- fall-back services that your business continuity arrangements are based on might not work as anticipated;
- small but important details of critical business processes might have changed since the plans were written; and
- staff on the ground might not be familiar with the business continuity arrangements.

Suitable exercises are an important way to flush out some of these issues, and is a key element in the continuous improvement of business continuity plans.

The aims of business continuity exercises are:

- to identify any areas for development in the existing plans so that they can be improved;
- to ensure that key staff, particularly those who may not have been closely involved in the planning process, are familiar with the business continuity arrangements;
- to build confidence in teams and in the organisation about its ability to respond to a disruption; and
- to raise the profile of business continuity planning so that the plans do not become *shelfware*, and staff are more likely to consider business continuity when planning changes.

To fully meet these aims, the exercise must:

- be as realistic as possible (this implies detailed simulations or exercises in the real world);
- avoid making the same assumptions as might have been inherent in the original planning (this implies involving different people in the exercises from those who wrote the plans);
- involve all the staff likely to be involved in a genuine business continuity situation; and

5. Exercising the plan continued

- be frequent enough to maintain familiarity with the arrangements and to keep business continuity recognised as a current topic (this implies at least annually).

In practice, conducting business continuity exercises along these lines could involve significant costs and risks to an institution.

Approaches to exercising the business continuity plans can cover a broad range including:

- 'Staged' disruptions;
- Detailed *table top* simulation of an actual scenario involving as many stakeholders as possible (including external stakeholders);
- *Table top* simulation of a scenario involving key staff;
- Desktop walk-through of the business continuity plan involving staff other than the planning team; and
- Desktop walk-through of the business continuity plan involving just the planning team.

In general, the more 'realistic' the exercise, the more costly and disruptive it will be, while the less realistic the exercise, the less information it will yield.

As an extreme example, the most thorough way to test the business continuity arrangements for the clearing process would be to arrange a disruption just before the clearing period. This would certainly show up any weaknesses in the business continuity arrangements but would be very high risk both for the institution and for the individual who suggested it!

Even detailed simulations can incur:

- significant costs in terms of the time taken to plan and undertake them;
- risk of disruption to normal operations while staff are engaged in the exercise; and
- diversion of staff from other activities which presumably also have some value to the institution.

Many institutions regard *table top* simulations of detailed scenarios as offering a good balance for business continuity exercises.

A further consideration is how business continuity exercises should relate to emergency management and business recovery exercises. In a genuine situation, all three processes could be involved and the relationships between them are important. There may well be advantages to exercising an incident response from beginning to end, but again this would introduce cost, risk and complexities.

It is therefore important to carefully balance the costs and benefits of the various exercise approaches in the context of your institution. Whatever conclusion is reached needs to be recorded in the business continuity policy and updated as exercise experience is built up. It may also be worth recording high profile scenarios that the institution decides are too risky to exercise, such as clearing.

back to contents

5. Exercising the plan continued

When planning specific exercises, the principles outlined in the following sections might be helpful.

> "It takes an outsider, or a new member of staff, to ask the obvious questions. It's then that you find out the IT department would not be able to get access to a building because the keys are with a caretaker."

5.1 Be humble

During the business continuity planning process, it is inevitable that some assumptions must be made about the detail of business processes, how people are likely to react in a business continuity situation, how technology will stand up, and what services and facilities are likely to be available in practice.

If the same assumptions are used during the exercise, it is possible that potential flaws in the planning could be missed.

One way to minimise this risk is to have different people involved in drawing up the exercise scenario from those who were involved in the original planning.

Consider the use of external people to lead or observe the exercise. These could be:

- colleagues from other institutions;
- staff from other local organisations willing to collaborate (remember, you may want to use each other's facilities at some point);
- advisors from your insurance company; or
- specialist consultants.

5.2 Be imaginative

Consider the business continuity situations that occur in practice. Some are the ones that would spring readily to mind such as fires, floods or power outages. However, others could be more surprising, such as:

- a demonstration outside adjacent premises which blocks access to your main administrative building;
- most of the staff from a department being wiped out for 48 hours by food poisoning from a leaving party;
- an air traffic controllers strike stranding your senior management team abroad after a foreign visit; or
- a credible message being received that malware has been planted somewhere in your IT systems and will be activated unless a ransom is paid.

The exercises should, over time, include a mix of the type of event you can easily foresee, some that have actually happened and some more unusual scenarios. Perhaps colleagues at other universities can suggest real or exercise scenarios you could adapt.

> "Test, test test, and make sure it is seen as important by senior managers. Test with key people missing."

5.3 Be awkward

It is highly unlikely that any business continuity event will take place without some complicating factors. Your building fire will inevitably happen when

back to contents

there is a newly appointed head of estates and the most experienced member of staff is on sick leave.

In planning your exercise, include some details to complicate matters somewhat, although you should also be wary of going too far and thereby undermining the credibility of the exercise.

5.4 Be secretive

It is very unlikely that the nature and timing of an incident will be known in advance, therefore it is well worth considering keeping the timing and other details of a business continuity exercise secret beforehand. This might mean that key staff would be missing for the exercise, but this is what would happen in practice, so it is not necessarily a reason for giving advance notice.

> "How 'deep' in faculties/directorates are key people identified? Would these staff feel supported in dealing with an incident when there are more senior people around?"

5.5 Be inclusive

Consider who will be involved in the exercise.

One common approach is the *table top* exercise where a few key members of staff sit in a room and work through a scenario. While this is a convenient approach in terms of being easily managed, it can exclude some of the people who would be involved in a genuine business continuity situation. This in turn means that the excluded people do not benefit from becoming more familiar with the arrangements, and the plan does not benefit from the detailed knowledge and suggestions they might bring.

There might also be value in involving key suppliers and partners so that they know what part they will be expected to play, you know your emergency contact arrangements are robust and you can gain some insight into how well prepared they are.

> "When you hold a BCP exercise, does it feel 'real'?"

5.6 Be reflective

As discussed earlier, the aims of business continuity exercises are:

- to improve the plans;
- To become familiar with the arrangements;
- To build confidence; and
- To keep business continuity on the agenda.

However, careful reflection on how an exercise went can also serve to improve the exercise process itself.

During the exercise, as in a real business continuity situation, it is good practice for those involved to keep detailed notes as they go along. It will also be helpful for one or more independent observers to keep notes of how the team works together, what is being reported back to the exercise leader, and any queries that arise. When the exercise has completed, extract maximum value from it by setting aside time for the whole team to reflect on what was learned.

Here are some sample questions for this "lessons identified" session:

- Did you consult your plan during the exercise?
- What parts of the plan worked well?
- What parts of the plan could be improved? Who will do this, and when?
- Was the format and presentation of the plan effective? Could people readily gain access to the business continuity plans, understand and implement them?
- Do the group have any questions about the exercise, were they confused at any point?
- Do the improvements identified point to any shortcomings in the way the business continuity plan has been written, exercised and updated in the past?
- How confident is the group that the exercise flushed out all the potential weaknesses in the plan?
- How confident is the group that following the exercise, implementation of the business continuity plan "in anger" would go smoother because everyone is more familiar with it?
- If the exercise were to be repeated, what would you change to make it more effective?
- Did the 'artificiality' of the exercise hinder the identification of lessons unduly? What could be done to improve this in future?
- Were the right people involved in the exercise?
- Was the balance about right between benefits gained from the exercise and the cost and disruption it caused?

See also Section 6.1, Invocations.

5.7 Be flexible

There is no particular reason why an institution should use just one approach to business continuity exercises.

There might be value in a combination of more frequent *table top* exercises and occasional, more in-depth simulations. Indeed, some variation in the types of exercise undertaken can keep the whole thing fresh.

6. Updating the plan

back to contents

6. Updating the plan

“It’s a rolling cycle – don’t stop when the first version is written. This also embeds BCP in the culture as a normal part of operations rather than as a ‘one off’ exercise.”

IN THEIR SHOES...

As chair of the Audit Committee you have asked whether the college has a business continuity plan. You are told that there is a plan, and that it was last reviewed five years ago. This seems quite a long time without a review, but the person responsible assures you that the plan is very high level, so does not need updating very frequently, and that the people on the ground are experts in their field and will know what to do in any foreseeable event. Do you accept this?

As discussed earlier, if there is currently no business continuity plan, rather than waiting many months for the 100% perfect version, there is value in producing something quickly, even if it is only 70% correct.

However, the institution should ensure that the business continuity arrangements are subject to continual improvement.

There are five triggers that should prompt the institution to update the plan:

- Invocations (or near invocations) of the business continuity arrangements;
- Business continuity exercises;
- Changes in the nature, scale or organisation of services, facilities or business processes;
- Changes in personnel or contact details; and
- Scheduled review.

These are each discussed in more detail in the following sections.

ASK YOURSELF...
When was your business continuity plan last internally audited?

Whenever the plan, or part of the plan is updated, the institution will need to ensure that all relevant staff are informed of the change, and that at any point people can always establish what the latest approved version of the plan is.

Similar considerations also apply to maintaining the emergency management and business recovery arrangements.

6.1 INVOCATIONS

Whenever the business continuity arrangements are invoked, people should be encouraged to keep notes of things that worked well and things that could be improved while they are still fresh in the mind. Once normal operations have been restored, there should be a formal ‘lessons identified’ session to pull all these ideas together and decide what changes need to be made to the business continuity plans.

A lessons identified workshop should consider the effectiveness of the plan both in terms of whether it worked, and in terms of whether people followed it (and if not, why not).

Remember that the lessons learned may also have applicability to business processes, services and facilities that were not directly affected by the incident.

back to contents

> "Disasters never go to plan. Experience is your most valuable asset; other people's experience is your next most valuable asset."

This session should also spend some time considering whether the improvements could have been identified before the incident. Could they have been picked up during the initial drafting and review of the plans? Could the exercise arrangements have brought them to light?

Some 'prompt' questions to spur discussion at a workshop are suggested:

- What went well with handling business continuity?
- What could be improved?
- Were people able to access the business continuity plan easily?
- Did people follow the business continuity plan?
- If people did not follow the business continuity plan, why was this?
- What departures from the plan worked well?
- Is there anything we could change about the way we write, exercise or update the plans that would help to make them more effective?

Are any of the lessons learned applicable to other parts of the business continuity plan?

Depending on the nature of the incident and the timescales involved, this review process may have considerable overlap with reviews of the emergency management and business recovery arrangements. If the sessions are combined, make sure that all the relevant people are involved and that the focus is not on one aspect of the incident response to the exclusion of the others.

It is important with any lessons identified exercise not to focus too much on the negative aspects of any experience. In most cases, a great deal will have gone well, and this should be recognised and built upon.

A review should also be prompted by any near miss (whether in the institution or elsewhere). For example, an item on the national news about a suspected leak of an infectious agent from a government laboratory should prompt members of the business continuity team to consider whether the local business continuity arrangements would deal effectively with the same situation. If nothing else, these near misses should be noted down as possible scenarios for future exercises.

> "Testing your BCP is one of those rare areas in life where 'failing' is to be positively encouraged."

6.2 Exercises

One of the key aims of business continuity exercises is to identify any areas for development in the existing plans so that they can be improved.

The process of identifying these lessons is essentially the same as for a real invocation, with the bonus that in the case of an exercise, there is often one or more people in observer roles, gathering information specifically for the purposes of improving performance.

The review should aim to follow a similar format to that discussed in Section 6.1, Invocations, but with consideration of the effectiveness of the exercise itself as well as the effectiveness of the response to the scenario.

See also Section 5.6, Be reflective.

back to contents

6. Updating the plan continued

6.3 Changes in services, facilities or business processes

The pace of change in an institution is such that there will be a near constant stream of changes to the critical business processes and the services and facilities that support them.

If the business continuity arrangements are to remain effective, an institution will need to have mechanisms to:

- Flag up when changes to the nature, scale or organisation of business processes, services and facilities take place;
- Decide whether there is any impact on the business continuity arrangements; and
- Update the plans accordingly.

These mechanisms depend on the whole topic of business continuity being embedded in the organisation rather than being the isolated responsibility of a small team of paranoid specialists. The idea of embedding business continuity planning is discussed further in Section 7, Embedding business continuity in the organisation.

> "Have an up to date list of internal and supplier contacts – invaluable in other circumstances."

6.4 Changes in personnel or contact details

It is important that the names of people and their contact details are accurate in the business continuity plans. This is not only to ensure efficient communication, but also because some of these details may be built into the protocols for some business continuity arrangements (see, for example Table 6, Business continuity actions for payroll, in Section 4.8, Planning for continuity).

As this is also likely to be an issue for the emergency management plans, it would be wise to see if there are existing arrangements that business continuity could hook into. If not, a joint approach to the HR department should be made to agree a process for flagging up significant changes.

In an ideal world, names and contact details should be kept out of the business continuity plans as much as possible to avoid frequent re-issue. A separate appendix would be one approach. If relying on purely electronic means of accessing contact details, it is important to ensure that the mechanism will be robust enough to survive a business continuity incident.

6.5 Scheduled review

In their shoes...

You are an internal auditor looking at the business continuity arrangements. The plan has been reviewed every year for the past four years, but no changes appear to have been incorporated as a result. Do you accept this without question?

back to contents

6. Updating the plan continued

ASK YOURSELF...
When did you last review your business continuity plan?

As a backup to all the mechanisms outlined above, there should be scheduled reviews of the business continuity plans.

Rather than trying to review the whole business continuity plan in one go, it is more manageable to break this up into staggered individual reviews of each of the business process arrangements plus the overall policy and framework.

These should consider:

- How recently the plan has been updated?;
- How recently was the plan exercised?;
- What, if anything, has changed in the organisation (services, facilities, business process or personnel) since the last update?; and
- Whether there have been any invocations or exercises since the last update?

Ideally, there should be no identified changes in the organisation after the last update to the plan. However, in practice the review team is likely to be aware of changes to staff, business processes, services, facilities or policies that would have some bearing on the plan.

The plan should, of course, be updated to reflect these changes.

An attempt should also be made to identify why the changes were not flagged up at the time, and whether there is any scope for improving the update mechanisms described earlier in this section.

Even if there have been no known changes within the organisation and no invocations or exercises, there should still be an active review of the plan rather than assuming that everything is still OK.

7. Embedding business continuity in the organisation

back to contents

7. Embedding business continuity in the organisation

In their shoes...

You are the project manager for the replacement of the University's sports facilities. This involves demolishing the old sports centre and building a new state-of-the-art facility. The project management methodology requires you to think about business continuity impacts, but as provision of sports facilities is not really a critical business process, this seems irrelevant to your project. Are you missing something?

Most Universities enjoy almost constant change at some level, for example:

- staff changes;
- departmental relocations;
- new buildings;
- new research contracts;
- new collaborations;
- new courses;
- changes in the arrangements for clearing;
- new IT systems; and
- new suppliers.

All these changes have the potential to affect the business continuity arrangements. They could simply require a change in the key contacts list, but they could equally remove the 'fall back' option that some plans depend on, or indeed increase levels of built-in resilience.

> "We need to ensure that business continuity is 'baked into' the process of introducing new services, especially those services that are technology based."

Business continuity plans should be reviewed regularly (see Section 6.5, Scheduled review) but the intervals between reviews is likely to be longer than the mean interval between changes that could affect the plan. This implies that if an organisation relies solely on periodic reviews to its business continuity plans, they will almost always be out of date.

To ensure that business continuity plans are always current, a more proactive approach to managing change is required, leaving the periodic review as a 'safety net'.

Whilst the management of change is a highly complex area, assessing some aspects of the impact of change have become reasonably well standardised across the sector, for example:

- equalities impact assessments;
- environmental (or sustainability) impact assessments; and (increasingly)
- Privacy Impact Assessments[12].

It is recommended that business continuity impact assessment is added to this list.

back to contents

[12] UCISA Privacy Impact Assessment Toolkit www.ucisa.ac.uk/PIAToolkit

7. Embedding business continuity in the organisation continued

For changes of personnel (probably the most frequent type of change), the process for reflecting the change, where necessary, in the business continuity arrangements should be as straightforward as possible. Institutions may wish to consider building this into the standard HR processes.

For other simple changes, a simple screening process should first establish whether or not the change has any business continuity implications. If it does, a member of the business continuity team should be contacted to discuss the proposed changes in more detail. The outcome could be adjustments to the proposed change and/or updates to the business continuity plans.

For more complex changes, assessment and management of business continuity implications should be built into the project management methodology. Depending on the nature of the project, there could be significant implications for the business continuity plans. Equally, business continuity considerations could have significant implications for the project. For this reason, business continuity should be taken into account early in the project and as work on the detail progresses.

> *The suppliers of the institution's HR system have introduced a facility for staff to download their payslips on a 'self-service' basis. (This standard approach will save considerable cost and logistical effort).*
>
> *A project was set up to roll out the change. As part of the project, business continuity impacts were assessed, and several alternative approaches considered. The project decided on a solution whereby in the event of a systems failure, the HR system supplier could produce paper copies of payslips corresponding to the standard business continuity payroll and distribute them to staff as required. This required changes to the corresponding business continuity plan so that changes to the standard payroll were sent to the HR system supplier as well as to the bank.*

The same considerations to maintaining business continuity arrangements in the context of organisational change also apply to emergency management and business recovery. Indeed, some changes may have implications for risk management by introducing new threats, removing existing threats, or by affecting the likelihood of threats being realised either positively or negatively.

Organisations may therefore wish to introduce a more general risk management assessment instead of a business continuity impact assessment. The process would follow the general approach outlined above, but would consider the impact of proposed changes on:

- risk management in general;
- emergency management plans;
- business continuity plans and;
- business recovery plans.

back to contents

8. Summary

back to contents

8. Summary

Universities are large organisations with considerable resources and significant responsibilities to a wide range of stakeholders. They are expected to be able to cope with most eventualities.

Risk management provides an overall approach within which threats can be identified and mitigated, but when an incident does occur the complementary processes of emergency management, business continuity and business recovery need to swing into action.

Prior planning is essential, particularly for business continuity where detailed arrangements may need to have been set up in advance and critical processes need to be up and running as soon as possible, albeit with reduced levels of service.

This document gives an overview of business continuity:

- Why it matters;
- How it relates to other risk management processes;
- How to produce plans;
- How to exercise them and;
- How to keep plans current in the face of constant change.

We hope you find the ideas and resources useful, and we wish you every success in your business continuity planning.

back to contents

9. Further information on HEBCoN and the BCI

back to contents

9. Further information on HEBCoN and the BCI

9.1 The Higher Education Business Continuity Network (HEBCoN)

HEBCoN is a network of Higher Education Institutions (HEIs) in the UK and Ireland who are committed to sharing and promoting good practice in Business Continuity Management (BCM), risk management and emergency planning.

HEBCoN became a professional body in 2007 and has since grown from strength to strength. Led by an Executive Committee and Regional Chairs, they offer expertise and support to their members in all aspects of business continuity.

Being a member of HEBCoN allows your institution to tap into a wealth of knowledge and expertise in Business Continuity Management. Members are able to access a wide range of benefits, from networking with professionals to attendance at training events and being able to access a library of resources. Their work is continually developing and their network continually expanding, changing the face of business continuity across Higher Education.

Website: *https://www.hebcon.org/*

Email: *info@hebcon.org*

9.2 Business Continuity Institute (BCI)

The Business Continuity Institute is the world's leading institute for business continuity. Established in 1994, the BCI has established itself as the leading membership and certifying organization for Business Continuity professionals worldwide.

The BCI offers a wide range of resources for business professionals concerned with raising levels of resilience within their organization or considering a career in business continuity.

With circa 8,000 members in more than 100 countries worldwide, working in an estimated 3,000 organizations in private, public and third sectors, the BCI truly is the world's leading institute for business continuity.

The BCI stands for excellence in the business continuity profession and its certified grades provide assurance of technical and professional competency in BC.

The BCI Partnership, through corporate membership, offers organizations the opportunity to work with the BCI to promote best practice in business continuity and to raise their corporate profile in the global BC arena. The BCI Corporate Partnership currently has approximately 120 Partners worldwide.

Website: *http://www.thebci.org/*

Email: *bci@thebci.org*

back to contents

10. Copyright, disclaimer and availability

back to contents

10. Copyright, disclaimer and availability

Copyright

The publication also contains resources from institutions; where this material is copied or otherwise reused, both UCISA and the institution concerned should be acknowledged. The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas, such as internet addressing, and consequently URLs and email addresses should be used with caution. UCISA cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Disclaimer

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas, such as internet addressing, and consequently URLs and email addresses should be used with caution. UCISA cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability

back to contents

AHUA

AMOSSHE
The Student Services Organisation

ARC
ACADEMIC
REGISTRARS
COUNCIL

AUDE
ASSOCIATION OF UNIVERSITY
DIRECTORS OF ESTATES

bufdg
british universities
finance directors group

Jisc

SCONUL
Society of College, National & University Libraries

ucisa

March 2019