Business Continuity Management Policy and Framework

Version:	13
Produced by:	University Business Continuity Team
Approved by (every 3 years):	Business Continuity Steering Group
Last approved:	27 February 2025
Original document produced 11th March 2010, and Updates:	5 July 2010, 14 December 2010, 19 May 2011, 5 April 2012, 21 September 2012, 3 January 2013, 30 January 2014, 17 March 2015, 29 January 2017, 15 September 2017, 22 October 2019, 3 July 2020, 28 February 2024,

This document consists of

- Policy Statement: Outlining the approach of the University to Business Continuity Management (BCM)
- Operational Framework: explaining the management of the University's BCM System (BCMS) and the roles and responsibilities of those involved in the delivery of the programme

The Business Continuity Team will review the Policy and Framework on an annual basis; it will also be reviewed when significant changes occur within the University. The Business Continuity Steering Group is responsible for formally approving this document on a three-year basis, and it will be reissued when revisions are made. This document is intended for all staff at the University.

Table of contents

Introduction

Business Continuity Management (BCM) is a process that enables the University of Sheffield to proactively identify and plan to minimise the impact of risks that could affect its objectives, operations and infrastructure. BCM supports the University's capability to continue priority activities, including teaching and research, following a disruptive event. Whilst the University does not have a specific statutory duty to undertake BCM, it is a business imperative. Also, the University has legal and moral responsibilities for staff, students and visitors and recognises the importance of this process in building trust and confidence in the response as a leading university in the UK.

The business continuity (BC) process starts with "Incident Management"- as illustrated below[1]:
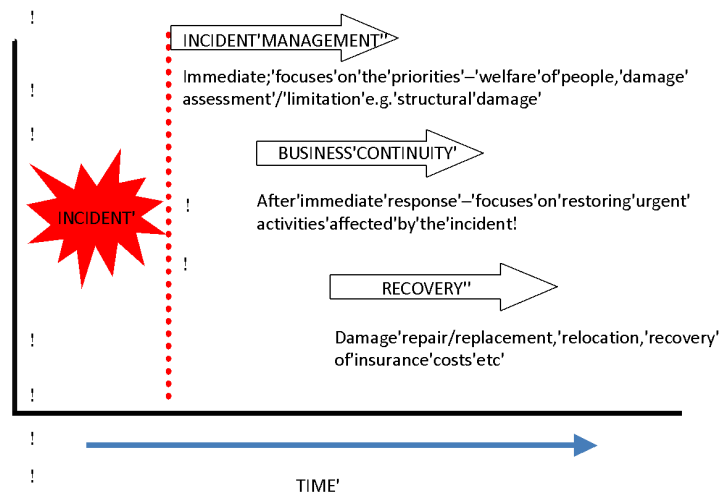
The University of Sheffield has defined two types of incidents based on their scale, duration and impact:

1. Minor incidents are interruptions/disruptions that are sufficiently disruptive to require the implementation of business continuity arrangements. They can be addressed by a departmental/school response using business continuity plans. They are smaller-scale events affecting one or a small number of departments/schools, e.g. a localised computer virus, a minor power cut for a short period, etc. However, sometimes minor incidents can become major incidents.

2. Major incidents require the implementation of the University's Major Incident Plan when they meet the plan's criteria of causing serious harm to staff, students, the University community, property or trust and confidence in the University. The Major Incident Plan is focused on the incident management phase, which is about containing the impacts and covers larger-scale events, e.g. a power cut affecting the campus or a national emergency. The Major Incident Team (MIT) will focus on the immediate priorities, i.e. the welfare of people, safety/security of buildings, communications, etc. In addition, a business continuity response would be required in terms of

---

[1] This diagram is intended to show the considerations after an incident - the timescales may change and in reality there may be overlap between phases e.g. the business continuity stage could start earlier.

how the University would continue its priority activities – those that are urgent and need to be recovered first.

Policy Statement

<u>Aim and Objectives</u>

Business Continuity Management is concerned with improving the resilience of the University of Sheffield. This means developing its ability to detect, prevent, minimise and, where necessary, deal with the impact of disruptive events or incidents. In the aftermath of an incident, business continuity enables the priority activities of the University to continue; in the longer term, it will help the University to recover as soon as possible. The University of Sheffield aims to develop, implement and resource a BCM System that will enable it to respond to and manage disruptions that occur.

The Business Continuity Management System has the following key objectives:

- To raise the profile of BCM within the University of Sheffield. This will include arrangements to make staff aware of plans, their roles in them, and are train them appropriately.
- To identify priority (time-critical) activities across the University and develop up-to-date, effective and fit-for-purpose business continuity plans for them
- To establish defined structures to plan for and respond to incidents
- To have ongoing arrangements that are subject to regular reviews, audits and exercises
- To develop and review the Programme for continuous improvement, with reference to best practice as appropriate, such as the Business Continuity Institute's Good Practice Guidelines and ISO22301[2]
- To embed business continuity into the culture of the University so that it becomes an integral part of decision-making

<u>Scope</u>

It has been agreed that the scope will operate across the institution, covering the five Faculties, all schools/departments within them and Professional Services based in Sheffield. Disaster Recovery arrangements (recovery of IT systems) will be the responsibility of IT Services for centrally managed IT and the responsibility of faculties and Professional Services departments for locally managed IT.

The University of Sheffield works with a number of partner institutions to deliver its services, and a risk-based approach will be adopted in terms of the University's expectations on these organisations, focusing on those for which the University has primary responsibility for the building and would be considered the greatest risk.

---

[2] ISO 22301:2012: Societal Security, Business continuity management systems - Requirements

The BCM System is focused on protecting and recovering the priority activities of the University and links to the aim of the University outlined in its vision to deliver world-class research, innovation and education by working as One University. A priority activity is identified based on how quickly it needs to be resumed and the impact if it is not available – on the safety of people, on trust and confidence in the University, its finances and customers. The focus of planning is on the first one to two weeks after an incident.

Operational Framework

Management of the Business Continuity Management System (BCMS)

- The System will follow the Business Continuity Lifecycle set out in ISO 22301 and will align[3] itself as considered appropriate with the requirements of the Standard
- Whilst Faculties oversee planning, it is expected that all University departments and schools will go through the business continuity process. This will involve identifying their priority activities, the resources required and appropriate arrangements in the event of a disruption
- The BCMS will be coordinated by the University Business Continuity Manager, however, individual departments and schools will be expected to nominate appropriate people to coordinate the development of their business continuity arrangements
- All documentation will be reviewed as a minimum on an annual basis, and will also be updated when there are significant changes to personnel, premises, suppliers, etc
- Documentation should be stored in the incident contacts system to ensure it remains accessible in the event of an IT-related disruption.

Validation

Validation confirms that the BCMS meets the objectives set in this policy and is achieved through a combination of review of the BCMS, maintenance of bc arrangements and exercising. These activities help to ensure that business continuity plans (BCPs) are kept up to date, effective and fit for purpose.

It is important for BCPs to be exercised on a regular basis, and any actions identified to be implemented. If there is a genuine incident, this may be used instead of an incident to assess their plan, but schools and departments should review and update their arrangements to reflect any lessons identified during the incident.

Existing BCPs will be exercised on an ongoing and risk-assessed basis. Faculty and Professional Services exercises (recognising key dependencies) may be undertaken to capture a number of departments and schools at the same time, given the size of the institution. Departments and

---

[3] "Alignment" to the standard has not been officially defined, but the University of Sheffield has interpreted it as following the principles of the standard and adopting practices that fit with the approach of the institution

schools are also encouraged to carry out their own exercises to validate their BC arrangements, using the exercise pack.

Roles and Responsibilities

University Business Continuity Team

The University Business Continuity Team (comprising the Head of Business Continuity and the Business Continuity Manager) are responsible for the development and coordination of the business continuity management system on behalf of the University. This involves:

- Raising the profile of BC across the University as an ongoing responsibility and ensuring that information is available to staff (with the aim of embedding BCM into the activities of the University)
- Providing advice and assistance throughout the BCM process
- Developing appropriate templates for the University to detail its arrangements, ensuring consistency in the System with flexibility to recognise the differences across faculties, departments and schools.
- Supporting departments and schools in completing the documentation from a business impact analysis (BIA) to developing a business continuity plan (BCP).
- Assisting in the development of overarching arrangements to support plans.
- Ensuring that the University's arrangements are regularly reviewed and exercised.
- Monitoring the level of business continuity planning in the institution and reporting to the Business Continuity Steering Group on this.
- Reviewing the System to ensure it remains fit for purpose and to continuously improve the arrangements in place.

Business Continuity Lead

The Director of HR is the lead across the University. This involves:

- Being the "champion" at strategic level by endorsing and supporting the Business Continuity Management System and ensuring it remains aligned with the University's strategy.
- Raising the profile of business continuity at a strategic level and supporting continual improvement.
- Chairing the Business Continuity Steering Group.

Business Continuity Steering Group (BCSG)

As the senior decision-making group, the Business Continuity Steering Group is responsible for:

- Reviewing the status/progress of departments, schools and faculties in developing and exercising business continuity plans and incident management arrangements.
- Discussing cross-cutting issues/concerns and identifying actions/solutions for which the Group will be accountable.

- Sharing lessons from incidents to improve resilience across the University.
- Supporting the Business Continuity Team in meeting the objectives of the BCMS and embedding business continuity by:
  - Promoting the inclusion of business continuity in agendas for local meetings.
  - Ensuring business continuity is considered at the design stage of projects in their department(s)/school/faculty, including IT and building projects.
- Ensuring a consistent approach to BC across the University, in accordance with the System, and supporting continuous improvement.
- Reporting on the Business Continuity Management System and the state of readiness to the UEB Risk Review Sub Group.

Business Continuity Coordinators (Department/School level)

Business Continuity Coordinators are the people nominated to coordinate the business continuity arrangements for the department/school and require a deputy. Their responsibilities are:

- Collating the required documentation, with assistance/involvement from other members of the department/school.
- Reviewing business continuity documentation to ensure it remains fit for purpose, up to date and stored appropriately, considering accessibility in the event of an IT outage.
- Reporting to the Business Continuity Plan Owner on progress, issues and when the plan needs approving.
- Supporting the Plan Owner in the running of events/exercises, including participating as appropriate.
- Attending relevant training and awareness sessions to develop knowledge of BCM.
- Liaise with the University's Business Continuity Team.

Business Continuity Plan Owners

The Plan Owner is accountable for the plan and will approve the documentation. It is expected that this will be the Head of Department/School (or appropriate deputy). Responsibilities will include:

- Approving business continuity documentation, ensuring it remains fit for purpose, up to date and stored appropriately, considering accessibility in the event of an IT outage.
- Attending and potentially leading on exercises, debriefs, and other events as appropriate.
- Attending relevant training and awareness sessions to develop knowledge of BCM.

Staff

It is important that everyone at the University is aware of what business continuity is, so this document will be shared on the website. Staff should be aware of the arrangements in their department or school's business continuity plan, especially how it may affect them. It is important that there is communication with them about business continuity, e.g. how they will be contacted /

notified of an incident, where they should report to if they are not able to access their usual place of work, etc.

Links to Other Areas

Incident Management

Incident Management is part of Business Continuity, focused on the containment of the incident. This is addressed in business continuity plans as part of their initial considerations and is covered in the checklist. This is also the focus of the University's Major Incident Plan, which addresses incident management arrangements for major incidents.

Risk Management

Business continuity management (BCM) and risk management are similar in that both enable us to think about uncertain events that could occur, with the aim of improving resilience and protecting our organisation.

Risk management is focused on the identification, analysis and mitigation of possible events or taking opportunities, whereas BCM focuses more on how we can limit the impact and disruption should an event occur. BCM is particularly focused on our most time-critical activities and the loss of resources (such as loss of staffing or system access), which will impact the delivery of our operations.

Business continuity management may be used as a treatment of some risks identified in risk registers and noted on the University's Corporate Risk Register, where this is the case. When developing business continuity arrangements, priority should be given to treating threats or vulnerabilities identified as being most likely and having the greatest impact.

Internal Audit

As part of the review and monitoring of the System, in addition to any reviews undertaken by the University Business Continuity Team, Internal Audit has an important role in ensuring that the Business Continuity Management System achieves its objectives as set out in this document.

Information Security

Information security covers the protection of all forms of information and is concerned with ensuring its confidentiality, availability and integrity. A key part of the BC process focuses on protecting against a potential loss of resources, including essential information, thereby ensuring it is stored appropriately and remains available after a disruption. Information Security should be considered when developing alternative arrangements to store/access key information. The loss of University information – either by a loss of access to it or by someone else being able to access it - could have serious implications, and, dependent on the severity, would be classed as an incident at department level and also potentially for the University.

IT Disaster Recovery

Disaster Recovery (DR) is a subset of BC and is about restoring data access and IT infrastructure after an incident. Disaster Recovery plans reduce the impact of disruption of critical services, applications or platforms by documenting the dependencies, resources and steps for recovery of a system.

IT Services has established an IT Services Disaster Recovery Policy that has a framework for setting DR objectives for centrally managed IT systems. Faculties and Professional Services departments will need to ensure appropriate Disaster Recovery arrangements are in place for locally managed IT systems.