Business Continuity Management Policy and Framework

Version:	11
Produced by:	University Business Continuity Managers
Date Produced:	11th March 2010
Approved by:	Business Continuity Steering Group (14 December 2010)
Updated:	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

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 Programme and the roles and responsibilities of those involved in the delivery of the programme

The Business Continuity Managers 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 and it will be re-issued when revisions are made. This document is intended for all staff at the University.

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 provides the capability for the University to ensure continuity of teaching and research, together with support for its students, staff, departments and faculties following any 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 ensuring it can continue its urgent activities after a disruption and to protect its reputation as a leading university in the UK.

The Business Continuity process starts with "Incident Management"- as illustrated below[1]:
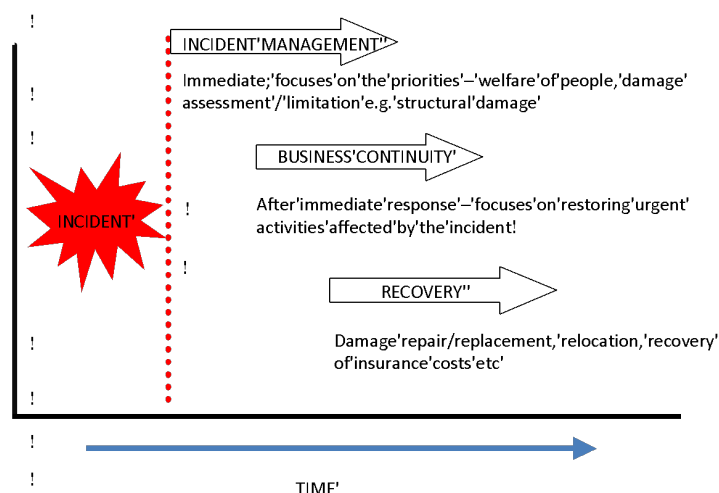
The University of Sheffield has defined two types of incident:

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 response - using business continuity plans. They are smaller scale events, affecting one or a small number of departments 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 its reputation. The Major Incident Plan plan is focused on the incident management phase and covers larger scale events e.g. a national emergency, a power cut affecting the campus etc. Using the power cut example, the Major Incident Team (MIT) would focus on the immediate priorities i.e. the welfare of people and the safety / security of buildings. In addition, a business continuity response would be required in terms of how the University would continue its urgent activities – those that need to be recovered first.

---

[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.

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 urgent or priority activities of the University to continue; in the longer term it will help the University to recover and return to "business as usual" as soon as possible. The University of Sheffield aims to develop, implement and resource a BCM Programme that will enable it to respond to and manage any disruptions that occur.

The Business Continuity Management Programme 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 trained appropriately
- To identify urgent or priority (time critical) activities across the University and develop suitable business continuity arrangements for them
- To establish defined structures to plan for and respond to incidents
- To have on-going BCM arrangements that are subject to regular reviews, audits and exercises
- To develop and review the Programme for continuous improvement, with reference to best practice, such as the Business Continuity Institute's Good Practice Guidelines and ISO22301[2]
- To embed Business Continuity into the culture of the University so it becomes an integral part of decision making

<u>Scope</u>

It has been agreed that the scope of the Business Continuity Management Programme will operate across the Institution, covering the five Faculties, all departments within them and Professional Services based in Sheffield. IT Services will remain responsible for specific Disaster Recovery arrangements relating to the recovery of IT servers/applications that they operate.

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.

The BCM Programme is focused on protecting and recovering the priority activities of the University and links to the aim of the University outlined in its vision and guiding principles of being one of the best universities in the world. This means being able to deliver its teaching, research and supporting the student experience. 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 the reputation of the University, its finances and customers. Initially the focus of the programme is on the first week after an incident.

---

[2] ISO22301:2012: Societal Security, Business continuity management systems - Requirements

Operational Framework

<u>Management of the Business Continuity Management Programme</u>

- The Programme will follow the Business Continuity Lifecycle set out in ISO22301 and will align[3] itself as considered appropriate with the requirements of the Standard
- Whilst Faculties may oversee planning, it is expected that all University departments 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 Programme will be co-ordinated by the University Business Continuity Manager, however individual departments will be expected to nominate appropriate people to co-ordinate the development of their department's 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, which would be available if the incident was affecting the provision of IT.

Validation

Validation confirms that the Business Continuity programme meets the objectives set in this policy and is achieved through a combination of review, maintenance and exercising. These activities ensure that Business Continuity plans (BCP) are kept up to date, effective and fit for purpose.

Newly developed BCPs would normally be exercised after completion. However, contingencies may be 'tested' during real life incidents. In this case, an exercise is not required but departments should review and update their BC arrangements to reflect any lessons identified during the incident. Existing BCPs will be exercised on an ongoing and risk assessed basis.

To increase the frequency of exercises and therefore reinforce key people's awareness of BC, Faculty and Professional Services exercises (recognising key dependencies) will be undertaken to capture a number of departments at the same time. Departments will also be encouraged to carry out their own exercises to validate their BC arrangements. A guide will be available to enable them to do this.

---

[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

Roles and Responsibilities

<u>University Business Continuity Manager</u>

The University Business Continuity Manager is responsible for co-ordinating the Business Continuity Programme on behalf of the University. This involves:

- Raising the profile of Business Continuity across the University as an on-going 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 Programme with flexibility to recognise the differences across faculties and departments
- Supporting departments 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 departmental 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 Programme to ensure it remains fit for purpose and to continuously improve the arrangements in place

<u>Business Continuity Lead</u>

The Executive Director of Corporate Services is the lead for Business Continuity across the University. This involves:

- Being the "champion" in terms of business continuity at strategic level by endorsing and supporting the Business Continuity Management Programme
- Assisting with raising the profile of business continuity at a strategic level
- Chairing the Business Continuity Steering Group
- Reporting on the Business Continuity Management Programme and the state of readiness to University Executive Board

<u>Business Continuity Steering Group (BCSG)</u>

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

- Reviewing the status/progress of departments 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 learning from incidents and responses to improve resilience across the University
- Supporting the Business Continuity Managers in raising and sharing of learning across the University. This includes members:

- o Promoting the inclusion of business continuity matters in agendas for departmental/faculty meetings on a regular basis
- o Ensuring business continuity is considered at the design stage of projects in their department(s)/faculty including IT and building projects
- Ensuring a consistent approach to Business Continuity across the University, in accordance with the Programme, and supporting the continuous improvement of the Programme

Business Continuity Co-ordinators (Department level)

The Business Continuity Co-ordinators are the people nominated to lead on business continuity for a specific department. They also require a deputy. It is expected that this will be the Head of Department (or appropriate deputy.) Responsibilities will include:

- Attending relevant training and awareness sessions to develop knowledge and understanding of Business Continuity Management
- Completing the required documentation, with assistance/involvement from other members of the department
- Ensuring business continuity documentation remains fit for purpose and up to date
- Attending corporately run exercises and participate/lead in the running of exercises for the individual department as appropriate
- Attending, participating and sometimes leading debriefs and other events as required to review and exercise the plan

Staff

It is important that everyone at the University is aware of the Business Continuity Management Programme. Staff should be aware of any arrangements in their department's business continuity plan that may affect them 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

Risk Management

Business Continuity Management and Risk Management work closely together, as both are concerned with good governance and raising awareness about risks. However, the focus of the two areas is different; Business Continuity Management is only concerned with managing those risks or what might be termed as threats or vulnerabilities that could cause a disruption to the University's operations, whereas Risk Management has a wider remit. A threat register is produced for Risk Review Group twice annually to identify the current vulnerabilities affecting the University. A meeting is held every few months between the Secretary to the Risk Review Group and the University Business Continuity Managers to share information between the two groups.

Business Continuity Management may be used as a treatment of some risks identified in risk registers and is noted on the University's Corporate Risk Register. 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 Programme, in addition to the reviews undertaken by the University Business Continuity Manager, Internal Audit has an important role in ensuring that the Business Continuity Management Programme 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 Business Continuity 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.

Disaster Recovery

Disaster Recovery (DR) is a subset of Business Continuity Management and is the 'ability of the ICT elements of an organization to support its critical business functions* to an acceptable level within a predetermined period of time following a disruption' [4]. The University's IT Services department has established an IT Service Continuity Management policy that provides a framework for setting DR objectives. The IT-Disaster Recovery (IT-DR) plan identifies key IT services / systems that would be recovered when a disruption occurs and the operational procedures to enable this recovery.

---

[4] ISO/IEC 27031:2011: Information Technology - Security Techniques - Guidelines for Information and Technology Readiness for Business Continuity.
* The University BCM Policy refers to these as services or activities.