Business Continuity Guide

# Introduction to Business Continuity

Business continuity is about having a plan to deal with situations, so that the University can continue to function with as little disruption as possible.

Business Continuity (BC) is defined as

“The capability of the organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.” (ISO 22301:2019).

In practise this means that we must be able to return to operating the critical activities of the University at acceptable levels within pre-agreed timescales during and after an event which causes disruption (e.g. staff will expect to be paid on time regardless of an issue with the HR system, students will expect a certain level of teaching and engagement with staff even during a pandemic).

Business Continuity is related to Risk Management but differs in that Risk Management is about identifying specific risks and minimising the disruption of these, whereas Business Continuity Management is about how functions can be operated regardless of the nature of the disruption.

In order to be able to meet this goal, we need to identify all of our critical activities (e.g. student teaching, staff salary payments) and plan for ways to continue or resume them regardless of the nature of the disruption.

# Business Continuity Process

In the development of a Business Continuity solution, the first step is to identify all of the activities that each Faculty or Service Area within the University are responsible for, identify which ones are time critical and carry out a Business Impact Analysis for each critical one. You can then develop a Business Continuity Plan (or plans) which covers the critical activities and documents the ways in which you can implement recovery of the activity to the minimum acceptable level.

The process is summarised in Appendix 1. Templates and further information can be found at <https://www.stir.ac.uk/about/professional-services/estates-and-campus-services/safety-environment-security-and-continuity/business-continuity/>.

## Business Impact Analysis (BIA)

Once the time critical activities that are performed have been identified, each one needs to be analysed to determine the features of the activity in terms of required resources, stakeholders (both internal and external), the impact of disruption and how this varies over time, and hence the necessary recovery timescales.

When carrying out a BIA, it is important to think in terms of effect rather than in terms of cause. The failure of an activity will have the same effects regardless of why the failure has occurred (e.g. it won’t matter to students whether their exam results are not published in time due to a staff strike or a significant power failure). It is also important to realise that the effects will change over time, and in most cases will become more significant the longer the failure lasts and / or the recovery takes (e.g. a failure to pay suppliers for a few days probably won’t matter too much, a failure to pay them for several weeks will be much worse).

The analysis of each critical activity should be carried out with the teams who understand the activity, it’s relationships to other activities and its interactions with stakeholders. This means that where multiple critical activities are identified by a Faculty or Service Area, the business impact analysis for each may need to be carried out by different groups of staff, but in each case they should be led by the same person to ensure continuity across all of the BIAs.

When considering the impacts which could be caused by the failure of an activity over time you should be thinking in terms of

* Stakeholder impact
* Loss of reputation
* Failure to meet statutory obligations
* Financial loss
* Data loss

You should also keep in mind that some impacts can vary depending on the time of year.

During this process it is possible that you will uncover new risks that have not been previously identified. In this case, these should be added to the relevant Risk Register(s).

## Business Continuity Plans

One the BIA’s have been completed, these should be used to form the basis of a Business Continuity Plan(s) (BCP(s)) for the area.

The BCP must be generic enough to cover any type of incident which may arise and should not focus on any specific types of incident, although if incident specific emergency plans already exist these should be referenced in the BCP.

When producing the BCP, specific consideration should be given to the following for each critical activity –

* Any actions which need to be completed before an incident (in preparation for one)
* The actions which will be required during the incident
* The actions which will be required after the incident to get everything back to normal

The major items which should be covered are –

* The membership of the Response Team who will lead on any local incident
* How you will communicate with all stakeholder groups (remembering that some, or all, of your normal communication methods may be unavailable)
* Your expectations of those who you rely on (you must ensure that this is communicated to and agreed with them)
* The impact of disruption on those who depend on the activity
* Actions required to minimise and recover from the disruption and the timescales within which these actions must be carried out

When considering the above, the following should also be considered –

* Can staff be contacted out of hours? Key staff should be aware of each other’s contact details.
* Could extra capacity be built into your staffing to assist you in coping during an incident?
* Are key staff aware of the business continuity arrangements for their area and what the critical activities are?
* Are key staff familiar with the possible resolution actions identified in the BCP(s) and are all involved staff trained to an appropriate level?
* In the absence of the key staff, deputies should always be identified. Are all deputies prepared for their roles?
* Could you operate from a different location? Could staff work from home?
* Is there an asset register or other central record of any specialist equipment required for the critical activity and will it be accessible in the event of an incident?
* Could alternative equipment/resources be acquired in the event of an incident or do they need to be acquired in advance of an incident?
* Is equipment “off the shelf” or specialised and if so what are the lead-times on critical equipment?
* Can you have agreements with other organisations regarding staffing, use of facilities, etc., in the event of an incident?
* Do you have alternative contractors/suppliers or are you reliant on a single contractor/supplier? Any alternative arrangements should be appropriately documented.
* Do your contractors/suppliers have contingency plans in place? If not, this should be discussed with the contractor/supplier and made compulsory when the contact is due for renewal.
* Could contractors/suppliers be contacted in the event of an incident? Ensure that the contact information for each is appropriately documented.
* Do you have alternative ways of working e.g. if systems go down what next – manual?

# Regular Review

All BIAs and BCPs should be reviewed regularly to check if all information is up to date and to make any necessary changes. Reviews should take place annually, or sooner if any significant changes take place which are likely to affect the accuracy or completeness of the BC documentation.

# Business Continuity Response Structure

The University currently has a two stage Response Structure with the following teams -

* MIRT (Strategic Team) – who will lead on incidents which are of more serious impact or where the impact affects multiple Faculties / Service Areas
* Operation Teams (One in each Faculty / Service Area) – who will lead on incidents where the impacts are only local

# Business Continuity Exercises

In order to ensure that Business Continuity Plans will be effective should they ever have to be activated, the plans should be exercised on a regular basis.

Normally this will be carried out as a desktop exercise, where the Response Team gathers together and talks through how they would handle a specific scenario with a view to identifying issues which have not previously been considered.

Once people are comfortable with desktop exercises, simulation exercises should be carried out where possible. During simulations, roleplay is used to carry out a simulated scenario in real time where the detail of the scenario develops during the exercise depending on how the Response Team reacts.

After any form of exercise, a debrief should be undertaken to see if anything could be improved and relevant BIAs and BCPs should be updated.

Stakeholders (upstream and downstream) should be included in the exercise process if appropriate to the chosen scenario and any relevant feedback from the outcome of the exercise should be communicated to them.

# Appendix 1 – Business Continuity Process Summary

