

EDINBURGH NAPIER UNIVERSITY

BUSINESS CONTINUITY MANAGEMENT POLICY AND FRAMEWORK

1. Purpose

This policy and framework sets out the University's approach to business continuity management and provides a structure for maintaining and developing business continuity plans across all Schools and Professional Services as part of the wider approach to managing Emergency Planning and Business Continuity.

The Risk & Resilience Committee (RRC) will review the Policy and Framework no less than once every three years; it will also be reviewed when significant changes occur within the University. The RRC, through its delegated authority from the University Leadership Team (ULT) is responsible for formally approving this document.

2. Business Continuity Management (BCM) - An Introduction

BCM is an essential element of risk management. It is the term used to describe the process of ensuring that organisations can continue to provide services in the event of a major incident which has the potential to cause severe disruption. It comprises two key aspects:

- i. Business Impact Analysis (BIA) - an approach to determine critical services and the resources that are required to maintain these services at acceptable levels: and
- ii. Business Continuity Plans (BCP) - contains the response and recovery information required to ensure that critical services, identified via BIA, are recovered in priority order following a disruptive incident to aid a return to business as usual as quickly as possible.

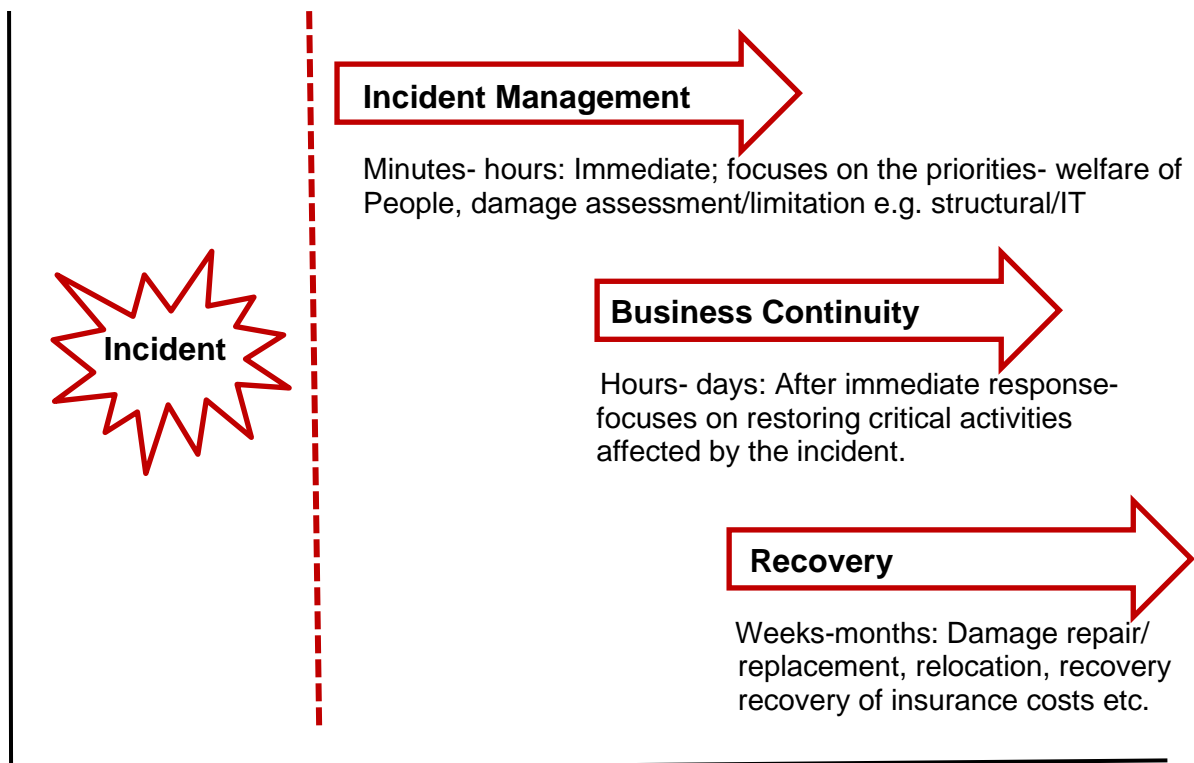
3. Why do we need Business Continuity Management?

BCM is a process that enables the University to proactively identify and 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, Schools and Service Areas following any disruptive incident. Whilst the University does not have a statutory duty to undertake BCM, it is nonetheless business imperative.

The Business Continuity process starts with "Incident Management" as illustrated in Figure 1:

Figure 1: Incident Management



4. Minor Incident

A minor incident is a serious situation or occurrence which happens unexpectedly and demands a business continuity response. These can be managed locally and are smaller scale events. This could range from damage to a (single) office caused by a major leakage, dealing with a medical emergency or the damage caused by a chemical spillage. The University's established Emergency Response Procedures have been prepared to deal with incidents of this nature.

5. Major Incident

A major incident is an event that prevents the University from continuing with normal business functions as a result of a real threat to the University's estates, facilities, utilities, IT infrastructure or human life and therefore requires a business continuity response. In the most serious situations the Crisis Response Plan (CRP) would be invoked.

In the event of a major incident, the Crisis Response team would focus initially on the immediate welfare of staff and students and the safety and security of our buildings and IT infrastructure. A business continuity response would, however, be required at the appropriate time following an incident. This would determine how key functions and services would be recovered with the aim of returning to business as usual as quickly as possible.

6. Aims and Objectives of Business Continuity Management at Edinburgh Napier University

BCM is concerned with improving and protecting the resilience of the University and its ability to detect, prevent, minimise and deal with the impact of a disruptive event. In the aftermath of an incident, it will enable the business-critical activities to continue; in the longer term it will help the University to recover and to return to “business as usual” as soon as possible.

The key aims of BCM within Edinburgh Napier University are as follows:

- (i) To raise the profile of BCM within the University. This includes making staff aware of plans, securing their involvement in the development of BCPs; raising their awareness of their specific roles within them and to ensure that all staff receive the appropriate training to carry out and duties required of them to fulfil the plan;
- (ii) To establish defined structures to plan for and respond to incidents;
- (iii) To establish ongoing BCM arrangements that are subject for regular reviews, audits and exercises;
- (iv) To develop Business Continuity Plans (BCPs) based on a Business Impact Analysis (BIA) in line with best practice;
- (v) To embed BCM into the culture of the University so that it becomes an integral part of decision making

BCM instils a level of confidence in corporate governance arrangements as well as providing key stakeholders such as insurers, internal and external audit providers and staff and students with the necessary reassurance that the University is suitably prepared in the event of a disruption.

7. Business Impact Analysis (BIA)

Business Continuity Management starts with Business Impact Analysis. BIA is a systematic process undertaken by Schools and Professional Services to identify key activities and resources to determine the critical services that must be given priority following an incident. It is the first activity that should be undertaken as it underpins the preparation of robust BCPs and provides assurance that all business-critical activities and supporting resources are identified and are subsequently developed with recovery measures. BIA will be developed by local stakeholders using a standard template.

Key steps involved in carrying out a BIA include:

- Identifying all key services and the activities on which these depend including supporting resources, critical suppliers etc;
- Mapping the workflow of the identified critical processes ensuring supporting resources are not overlooked;
- Assessing the impact in the event that a critical activity is disrupted; and

- Identifying recovery measures including Recovery Time Objectives (RTO) and Maximum Tolerable Downtime Period (MTDP) for services to identify recovery priorities so as to optimise recovery strategies.

8. Business Continuity Plans (BCPs)

Business continuity plans are developed from the BIA process and set out the priorities for the resumption of business-critical activities in the event of a major incident. Detailed recovery measures for each identified business critical activity should form the majority of the content of plans aided, where necessary, by relevant logistic information such as contact lists.

9. Business Continuity Planning Framework

There are three elements to the business continuity framework which includes plans for managing i. the digital estate and IS infrastructure managed by Information Services (IS) ii. the physical estate managed by Property and Facilities (P&F) and iii. plans developed by Schools and Professional Services areas overseen by the Governance Officer.

IS colleagues are putting in place a new approach to managing the University's digital software through 'Project RAID'. This project will deliver major benefits for the University and amongst the key deliverables from a business continuity perspective is a comprehensive software catalogue for all University systems held centrally together with information on their operation and change control processes. In addition, all University software applications will be assigned a priority recovery listing with those systems deemed to be most critical to University business being accorded a Priority 1 status. In the immediate aftermath of an incident these systems will be the first to be recovered using the documentation on system recovery that will be held in the central database. This approach will aid decision making at the time of an incident and ensure decisions are taken on an informed basis reducing prolonged downtime and extended recovery time.

In the event of an incident affecting a campus location, online working will be the default for many colleagues and this will be monitored and reviewed during the business recovery period. Property and Facilities colleagues may, however, be asked to assist in reviewing options for alternative working arrangements where a physical estate presence is required for business continuity reasons. Property and Facilities maintain a property database which contains information about the physical estate and purpose/functions of the spaces within each of the different campuses.

Separate School and Professional Services plans have been developed and these are accessible on the Business Continuity SharePoint Management site. The Governance Officer, in conjunction with the relevant BC Leads for each School/ Professional Service area will develop and manage these plans. It is recognised that these plans will require some adjustment to align with the IS plans that are being developed via Project RAID. These adjustments will be undertaken as the IS work begins to deliver outputs.

10. Operational Framework

In order to support the University achieve its strategic objectives and to support the continued development of BCM, an operational framework has been created. This framework recommends that:

- i. The University will ensure it aligns itself to best practice with regards to business continuity planning;
- ii. All Schools and Professional Services will follow the BIA/BCP process. This will involve working alongside the Governance Officer (Risk & Governance) to identify their priority activities in addition to the immediate resources required and appropriate arrangements to be followed in the event of a disruption;
- iii. The Business Continuity framework will be coordinated by the Governance Officer, however individual schools and service areas will be expected to nominate a Business Continuity Lead to liaise with the Governance Officer to coordinate the development of their department's BC arrangements;
- iv. The BCP will be reviewed as a minimum on an annual basis. Plans will also require to be updated when there are significant changes to staffing/structure and premises etc.; and
- v. The Governance Officer (Risk & Governance) will liaise with Business Continuity Leads to arrange for BCPs to be tested at least once over a three-year cycle.

11. Roles and Responsibilities

Business Continuity is the responsibility of everyone - all staff should be aware of it and the role they play within their own School or Professional Service area plan. However there are a number of individuals within the University who have a key role to play in the development, progression and coordination of Business Continuity Management and Planning.

Director of Strategy & Planning and Secretary to Court

The Director of Strategy & Planning and Secretary to Court, who delegates responsibilities in this area to the Head of Governance and Risk, has senior executive (ULT) level oversight of the maintenance and development of the University's BCP framework. This involves:

- i. Being the strategic lead for Business Continuity Planning in the University by fully endorsing and supporting the framework;
- ii. Raising the profile of Business Continuity at a strategic level;
- iii. Assuring University Leadership Team (ULT) and University Court that the University's business continuity plans are being appropriately and effectively managed and tested; and

Attending the Risk & Resilience Committee and convening its meetings if not delegated to the Head of Governance & Risk.

Director of IS

The Director of IS has senior executive level oversight for maintaining and developing the digital estate and IS infrastructure and recovering that in the event of an incident where IS resources are impacted.

Director of Property and Facilities

The Director of Property and Facilities has senior executive level oversight for the maintenance and development of the physical estate/infrastructure and recovering that in the event of an incident where the University's estate is impacted.

Governance Officer (Risk & Governance)

The Governance Officer is responsible for coordinating the Business Continuity Framework on behalf of the Director of Strategy & Planning and Secretary to Court and Head of Governance & Risk. Specifically, this involves:

- i. Raising the profile of Business Continuity across the University and ensuring that all relevant information is readily available to staff;
- ii. Working across all services to ensure interdependencies are recognised and that a consistent approach is applied across the University;
- iii. Providing guidance and assistance to Schools and Professional Service areas on business continuity planning;
- iv. Developing appropriate templates for the University to detail its arrangements, ensuring consistency across the Framework, with the flexibility to recognise the difference across Schools and Service areas;
- v. Ensuring that the University's BC arrangements are regularly reviewed and exercised;
- vi. Providing training and leading on the development of corporate exercises to review the arrangements that have been put in place;
- vii. Reviewing the Framework to ensure it remains fit for purpose, to improve the arrangements in place and to amend and update any plans when there are any major changes to staffing, premises or key business processes.

Business Continuity Leads (Schools/ Professional Services)

The Business Continuity Leads are individuals within each School/ Professional Service area who are nominated to lead on Business Continuity for their relevant area. It is expected that this will be the Dean of School/ Director of Service or their appropriate deputy/ nominee.

The role of the Business Continuity Lead is to assist the Governance Officer (Risk & Governance) in "championing" BCM by:

- i. Acting as a single point of contact within the School/ Professional Service area for BC issues;
- ii. Along with the Governance Officer, holding a master version of the department BCP;
- iii. Ensuring all BC documentation remains current and fit for purpose;
- iv. Advising the Governance Officer (Risk & Governance) of any changes that require to be made to their BCP;
- v. Attending relevant training and awareness sessions to develop their knowledge and understanding of BCM;
- vi. Being able to explain how BC works, the benefits of undertaking it and ensuring that the school/ department is engaged with the process;
- vii. Attending corporately run scenario based exercises and participating and leading these for the department as appropriate;
- viii. Acting as a conduit for any queries issues raised, but deferring to and seeking guidance from the Governance Officer should the need arise;

The Business Continuity Leads will ensure that all members of staff are made aware of the arrangements which are relevant to them and of the plans in which they have roles.

12. Business Continuity Network

A network of business continuity leads meets periodically as required at least once a year to discuss University approaches to business continuity and to assess whether the aims and objectives of BCM are being met. It will also provide a forum to discuss of wider sector-related developments and to share good practice.

13. Plan Testing and Timing

BIA should be conducted at least every 5 years or in the event of significant organisational change. This will ensure that there is formal validation of the content of plans and ensure they continue to reflect the University's requirements and support optimum recovery measures. Any changes to the BIA would lead to an update in the BCP.

BCPs should be reviewed annually and tested every three years. The Governance Officer will be responsible for assisting the Business Continuity Leads to develop and test their plans.

14. Links to Other Areas

Risk Management

Business Continuity Management and Risk Management are interlinked as both are concerned with good corporate governance and raising awareness about risks. BCM however is only concerned with managing those incident related risks that could cause a disruption to the University's operations, whereas Risk Management has a wider remit concerning the delivery of operational and strategic objectives

Internal Audit

Internal Audit has an important role to play in BCM in ensuring that the Business Continuity Framework achieves its objectives as set out at the start of this document.

For further information about the University's internal audit protocol please contact the Governance Officer

Information Security

Information Security is concerned with the protection and integrity of both manual and digital information. A key feature of the Business Continuity focuses on protecting against a potential loss of resources including important information thereby ensuring information is stored appropriately and remains available after disruption.

The loss of information- either by a loss of access to it or by someone else being able to access it - could have serious ramifications and dependent on the severity, would be classed as an incident at department level and also potentially for the University.

Document Control

Author	Governance & Compliance
Date first approved	November 2015, updated June 2018
Last review date	April 2023
Next review date	April 2026
Review Frequency	3 years

Glossary

BCM	Business Continuity Management
BCP	Business Continuity Plan (s)
BIA	Business Impact Analysis
CRP	Crisis Response Plan
CRT	Crisis Response Team
ERC	External Relations & Communication
HRD	Human Resources and Development
RRC	Risk and Resilience Committee
ULT	University Leadership Team