THE UNIVERSITY of EDINBURGH

Business Continuity Management Policy and Framework

This document is reviewed annually or following a significant change e.g. an organisational restructure.

Version	Date	Approved by	Reason
V0.1 DRAFT	n/a	n/a	n/a
V0.2 DRAFT	n/a	n/a	n/a
V0.3 DRAFT	07/02/19	n/a	Updated to include comments from Risk Management Committee (04/02/19)
V1.0	19/02/19	University Executive	n/a
V2.0	03/05/21	Risk Management Committee	Scheduled review
V3.0	02/05/22	Risk Management Committee	Scheduled review
V4.0	1/05/23	Risk Management Committee	Scheduled review
V5.0	1/05/25	Risk Management Committee	Scheduled review

CONTENTS

SECTION A: BUSINESS CONTINUITY MANAGEMENT (BCM) POLICY

1.0 Introduction

> "Business continuity is the capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption."
>
> (ISO22301:2019).

Business Continuity (BC) enhances an organisation's resilience by putting in place arrangements to help it respond to, and recover from, disruptive incidents effectively and efficiently. It provides reassurance which allows the organisation to focus on growth and development with confidence. This in turn strengthens its ability to achieve its strategic objectives and development themes.

2.0 Statement of Intent

This *BCM Policy and Framework* documents the University's approach to Business Continuity Management (BCM) and provides a consistent, overarching structure to support Schools and Departments in the development and implementation of their own BCM arrangements. It has been developed to reflect best practice and recognises the distinct challenges faced by the University's size and diverse range of activities and services.

This *BCM Policy and Framework*:

- Respects the University's devolved responsibility model and, where appropriate, values flexibility to ensure Schools and Departments can develop arrangements that meet their own specific needs and priorities
- Is informed by the International ISO22301:2019 Security and resilience – Business continuity management systems
- Is supported by senior management
- Requires all Schools and Departments to have effective BCM in place, to demonstrate continual improvement of their BCM arrangements and to embed BCM in decision-making processes.

This *BCM Policy and Framework* has been developed within a wider framework consisting of:

- The values, vision, culture, mission and goals of the University and its constituent organisations
- The University's governance and reporting structures
- Legal, regulatory and other requirements applicable to the University
- The University's risk management structure
- ISO22301:2019 Security and resilience – Business continuity management systems
- Business Continuity Lifecycle (BS25999-1:2006)
- The University Risk and Resilience Services' vision
- The University's Business Continuity Toolkit which contains guidance, templates and exemplars, etc.
- Associated policies including procurement, emergency management and risk management
- The internal audit process.

3.0 Aim and Objectives

3.1 Aim

To be a resilient organisation with robust BCM enabling the continued delivery of critical services that support the University's strategic objectives of *Leadership in Learning* and *Leadership in Research*.

3.2 Objectives

- Manage a comprehensive, risk-based BCM programme informed by the requirements set out in ISO22301:2019 (Security and resilience – Business continuity management)
- Identify and prioritise the University's critical services through the use of a robust and consistent Business Impact Analysis (BIA) process
- Using a risk based approach, develop effective contingency strategies for critical services (as determined by the BIA process) for inclusion in BC plans
- Establish effective incident management procedures for use during a BC disruption
- Develop BC plans that are fit for purpose, regularly reviewed, available and simple to follow and understand
- Deliver a programme of training and exercising, developed against required competencies and delivered to all staff with a direct BC responsibility
- Continually improve the University's BCM through regular evaluation of its efficacy and appropriateness taking into account any changes to legal and regulatory requirements
- Raise awareness of this BC Policy, promote BCM across the organisation and embed BCM into 'normal' business practices
- Implement a clear governance framework to monitor and report on the University's adherence to this *BCM Policy and Framework*.

4.0 Scope

- The University's BCM extends to all University sites
- The University's BCM extends to all staff and activities of the University, including its subsidiaries
- Where activities are delivered in partnership with external partners, BCM arrangements will be agreed and implemented with these partners.

5.0 Roles, Responsibilities and Authorities

5.1 The University Executive has overall accountability for the University's BCM.

5.2 The Risk Management Committee has responsibility for the annual review and approval of the *BCM Policy and Framework*, oversees the University's compliance to the *BCM Policy and Framework* and ensures the *BCM Policy and Framework* remains aligned to the University's strategic objectives. The Risk Management Committee also oversees the BCM Programme and approves key methodologies and templates.

5.3 The BCM Sponsor (Director of Corporate Services) provides senior level endorsement of the University's BCM and promotes the importance of BCM and its benefits.

5.4 Senior Management (Heads of College/Professional Services Groups, Heads of Schools/Departments) are responsible for:

- Providing sufficient resource (with appropriate authority and competence) to ensure effective implementation, maintenance and improvement of local BCM arrangements
- Integrating BCM into normal business processes within and across Schools and Departments
- Acting as advocates, communicating the importance of effective BCM
- Demonstrating their commitment to continual improvement
- Participating in training and exercising.

In addition, Heads of Schools and Heads of Departments are also responsible for:

- Ensuring a BC plan and other appropriate BCM arrangements are in place for their School / Department and that these are regularly reviewed and exercised.
  Note: Heads may wish to consider delegating the development and maintenance of BC plans and arrangements for their individual School / Department.
- Sign-off of their School / Department BC plan.
- Collaborating with colleagues in other Schools / Departments where co-located or where there are interdependencies in delivering critical services to ensure appropriate joint or location-based BC plans are in place.
- Invoking their BC plan, if required.

5.5 The Incident Management Team's (IMT) responsibilities (non-BC) and membership is detailed in the University's Emergency Incident Response Plan. In addition to these, the IMT has BC responsibilities including:

- Coordinating the response and recovery of critical services across the University
- Prioritising resources, as appropriate
- Participating in incident debriefs and, as part of robust planning,
- Participating in training and exercising.

Note: During a significant incident the IMT may establish a separate Business Continuity Response & Recovery Team (BC Response & Recovery Team). This BC Response & Recovery Team will lead on the responsibilities above in addition to providing update reports to the IMT on impacts and mitigating actions taking place.

5.6 The Business Continuity Manager is responsible for:

- Developing and maintaining the University's *BCM Policy and Framework* and BCM Programme
- Developing and implementing cross-University procedures, templates and methodologies with input from College and Professional Service Group representatives
- Development and management of University-wide BC arrangements
- Integrating BCM into the University's incident response structure and notification and escalation procedures
- Monitoring the review cycle for University BC plans to ensure they remain current
- Establishing the standard for BC plans
- Preparing reports and compiling evidence to give assurance to internal and external audit that BCM procedures are fit for purpose
- Submitting reports and making BCM recommendations to Committee, as appropriate
- Providing specialist BCM support and advice across the organisation
- Developing and delivering a programme of BCM training, exercising and promotion
- Assisting Schools / Departments to develop strategies to mitigate BC-related risks as identified in their risk registers

- Sharing good practice and liaising with peers in other higher education institutes and across other sectors, as appropriate.

5.7 The Resilience Working Group (RWG) consists of the BC Manager, the Emergency Manager and a representative from each College and Group and from specialist areas. Members will be responsible for:

- Monitoring the BCM's programme of work
- Providing input and guidance in the development of overarching documents, templates, methodologies and strategies to ensure they are fit for purpose for all areas of the University
- Sharing good practice and experience across the wider organisation
- Supporting each other and the efficient development and delivery of quality BCM arrangements and identifying inter-dependencies.

5.10 All Staff are responsible for ensuring they are aware of:

- The critical services within their area
- Their own role and responsibilities during a disruptive incident (including contact arrangements)
- The importance of effective BCM and the implications if it is not in place
- This BCM policy.

6.0 Information and References

6.1 Standards, Policy and Direction

- The University of Edinburgh's Business Continuity Management Toolkit
- BS ISO22301:2019 (Security and resilience – Business continuity management systems)
- The University of Edinburgh's Major Incident Plan
- Preparing Scotland: Having and Promoting Business Resilience, Scottish Government (2013)
- Preparing Scotland: Exercise Guidance, Scottish Government, 2018
- The Business Continuity Institute's (BCI) Good Practice Guidelines, 2018.

6.2 Related Policies

- Risk Management
- Health and Safety

SECTION B: BUSINESS CONTINUITY MANAGEMENT (BCM) APPROACH

The University's BCM approach reflects the Business Continuity (BC) Lifecycle as documented in *BS 25999-1:2006 Business Continuity Management.*

Where possible, the University's BCM remains flexible to ensure BC arrangements developed by Schools and Departments are fit for their purposes and reflect their individual needs and priorities. However, to support an effective response, (particularly in the event of large incidents) it is necessary to implement some University-wide methodologies and templates. Further details can be found in the University's BC Toolkit.

1.0 The Business Continuity (BC) Lifecycle

The BCM Lifecycle has 6 elements as illustrated below:

(BS25999-1:2006)

1.1 BCM Programme Management

The University's overall BCM Programme Management is managed by the BC function (located in Corporate Services Group). It involves:

- Determining the scope and approach of the University's BCM
- Development of the *BCM Policy and Framework* including roles, responsibilities and authorities
- Establishing the governance structure and process
- Development and management of the University's overarching BCM work programme.

Success of the BCM Programme is underpinned by the commitment of senior management and the allocation of resources for its implementation, maintenance and improvement.

1.2 Understanding the Organisation

Business Impact Analysis (BIA) are undertaken by Schools and Departments to determine the organisation's critical services (i.e. services that must be given priority following an incident in order to mitigate impacts) and the resources needed to maintain delivery of these critical services at acceptable levels. This BIA process ensures actions to mitigate the impacts of an incident are appropriately targeted.

All BIAs undertaken at the University will use the same methodology to ensure activities have been assessed in a consistent way.

The risk assessment process identifies and assesses the risks to these critical services to support effective, focused planning.

1.3 Determining the BCM Strategy

Response and recovery strategies are developed to mitigate the impacts on the critical services during a disruptive incident.

1.4 Developing and Implementing BCM Response

Response and recovery information is documented in BC plans for use during a disruptive incident. Every School and Professional Services Department has a documented BC plan. Some cross School / Departmental plans may also be developed to reflect interdependencies of critical services. Location (building) specific BC plans may be developed dependent on the building users and critical services being delivered there. Additional plans and arrangements are also in place (or being developed) for specific scenarios (e.g. unexpected absence of the Principal, severe weather, etc.). These are developed based on the risk requirement and good practice.

IT Disaster Recovery (DR) plans are included in the scope of this BCM framework and form an integral part of the University's BC response. These plans are developed, managed, reviewed and monitored by ISG and extend to cover eLearning and Library Services as part of a broader ISG Business Continuity framework which is aligned with this policy. All top Priority ISG Services are expected to have a BC plan and DR plans as standard and ISG have a role in influencing the uptake of this approach across all University IT Services.
.
Note: DR plans do not need to include the same required elements that BC plans must include.

BCM training is delivered to staff who have a direct response and/or recovery responsibility. Training is needs-based and reflects the competencies required to plan for, respond to, and recover from incidents.

1.5 Exercising, Maintaining and Reviewing

BC plans and arrangements are reviewed and exercised every two years using a variety of scenarios and exercise types. This ensures plans and procedures remain valid and effective and are consistent with the University's BCM objectives. The University's exercise programme will include cross-University exercises and involve colleagues from all levels of the organisation, as appropriate. Exercise planning will consider participation of colleagues with a direct business continuity responsible as well as their deputies.

The University's BCM approach places a strong emphasis on exercising as a tool to develop and validate arrangements, rehearse our response, share information across areas, support continual improvement and provide staff with valuable training to meet their required competencies. The University's BCM Programme and local BCM Programmes reflect this focus.

1.6 Embedding BCM in the Organisation's Culture

BCM is promoted across the organisation at all levels through education and information sharing to facilitate its successful embedment into normal business processes.

2.0 Emergency Incident Management

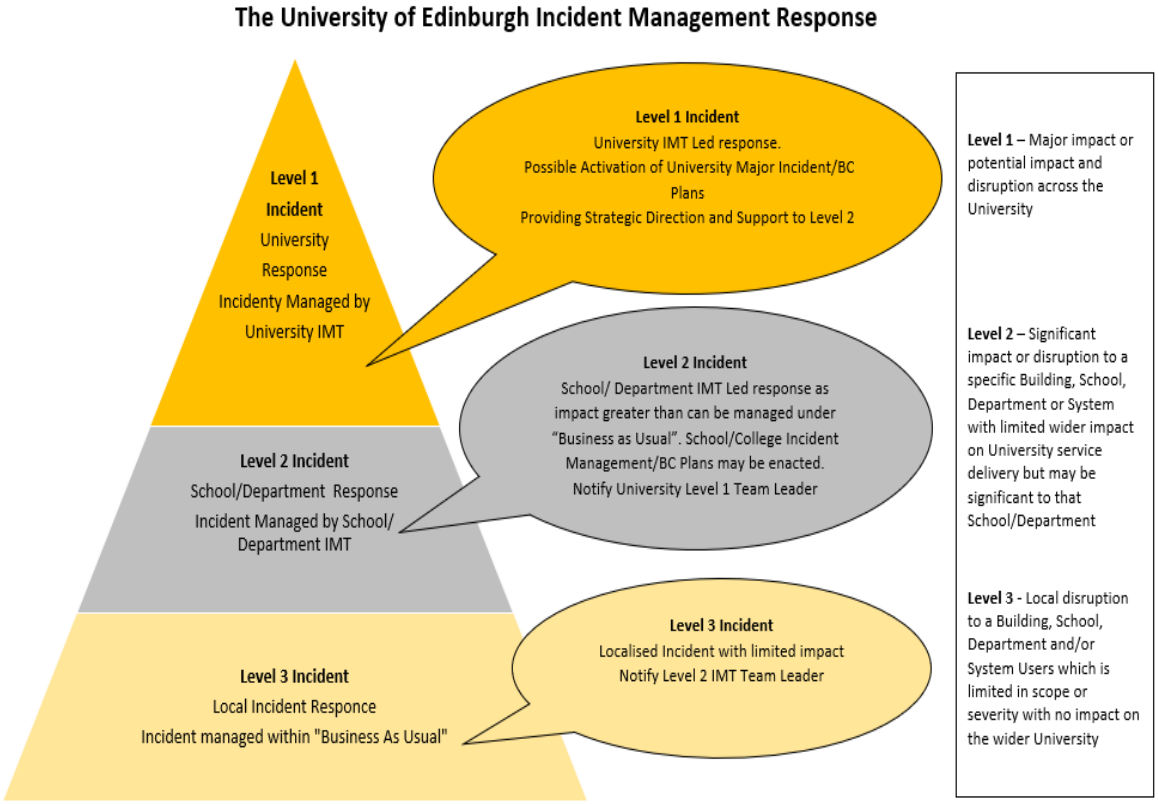
Incident management procedures are documented in the University's Emergency Incident Management Framework Policy.

The policy and supporting plans and procedures help ensure that the University is prepared to deal with emergency situations. Its purpose being to maintain safety whilst assessing, stabilising and managing an incident and in conjunction with business continuity teams and plans, restoring the university back to an acceptable level of operations as quickly and effectively as possible.

Emergency incidents can be classified as Localised, Significant or Major. While each may pose a risk to the continuity of core University-wide operations, the severity or scope determines the level of response which have been categorised into the following three levels:

Incident Category	Response Level	Managed by
Localised	Level 3	Business As Usual Measures & Procedures
Significant	Level 2	School/College/Department IMT
Major	Level 1	University IMT

These category levels and incident criteria are detailed in the Criticality Model shown below.



3.0 Governance

3.1 University Executive and Risk Management Committee

The University Executive has overall accountability for the University's BCM. The Risk Management Committee has responsibility for the review and approval of this BCM Policy and Framework, provides oversight of the University's BCM and approval of key BC methodologies and templates.

3.2 Internal Audit

Internal audits are conducted in line with the Internal Audit Programme. Recommendations identified as part of the audit process are included on the BCM Programme and monitored through to resolution as part of the audit process and to support continual improvement.

3.3 The Resilience Working Group (RWG)

The Group is chaired by the University's Business Continuity Manager and Emergency Manager with a representative from each College and Professional Services Group in addition to representatives from specialist areas including Estates, Communications and Marketing, HR, Information Services and Health & Safety.

The Group develops and agrees university-wide methodologies, templates and strategies and, where appropriate escalates them to the Risk Management Committee for approval. It also ensures identified lessons are integrated into BC arrangements as part of continual improvement and provides a forum to share experience and good practice. The Group's remit is available from the Business Continuity Manager.

3.4 Annual Review

The Business Continuity Manager conducts an annual review of the University's overarching business continuity arrangements to ensure they comply with the requirements set out in this *BCM Policy and Framework*. Actions from the Review are captured in the BCM Programme and monitored through to resolution to support continual improvement. Outcomes from Review will be reported to the Risk Management Committee as evidence of the University's compliance to this *BCM Policy and Framework*.

4.0 Performance (See also 3.4. Annual Review)

4.1 Performance Indicators

BCM performance indicators have been developed to help monitor and measure the performance of the University's BCM against the requirements set out in this *BCM Policy and Framework* document. Results will be reported to the Risk Management Committee as evidence of the University's compliance to this *BCM Policy and Framework*.

4.2 Continual Improvement

The University will demonstrate continual improvement of its BCM by ensuring improvements and non-conformities identified through the following are progressed to resolution and, where appropriate, reflected in BCM arrangements during reviews.

- Incidents and incident debriefs
- Exercise evaluations
- Training evaluations
- Risk Registers
- Meeting Minutes
- Internal Audit reports
- Annual Review.

5.0 Document Management

5.1 Version Control

All BC documents across the University use version control. All documents generated by the Business Continuity function in Corporate Services include the following:

- The document title and version
- Date of last update
- Document file location.

Note: A draft version is indicated by a part number e.g. v0.1, v0.2, etc. and a final version is indicated with a whole number v1.0, v2.0, etc.

5.2 Records Management

All BC documents are be kept in accordance with the University's Records Management Guidance (Records Management Guidance). All personal data used as part of BC arrangements (e.g. staff contact lists) should be developed, stored and managed in accordance with the Records Management Guidance and the General Data Protection Regulations (GDPR).

External documents will be identified and controlled, as appropriate.

5.3 BCM Repository

A central 'repository' primary solution has been developed in SharePoint, offering a secure, user-friendly platform for authorised staff. Each school and department will be allocated its own folder within the repository. The repository may also be used to hold Incident/Emergency Management and Disaster Recovery plans. If the primary repository is inaccessible for any reason (cyber-attack, power outage etc), a secondary 'back up' repository will provide access to copies of the documents held on the primary repository. This is an offsite Google Cloud solution.

To ensure documents held within the primary and secondary repositories are secure and only accessible by authorised individuals, access permissions will be allocated to each school and department. User Services Division will support the ISG section of the repository and the University Business Continuity manager will support the rest of the schools and departments.

SECTION C: GLOSSARY

Business Continuity	BC	The capability of an organisation to continue delivery of products or services at acceptable pre-defined levels following a disruptive incident
Business Continuity Management	BCM	Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, brand and value-creating activities
Business Continuity Coordinator		Representative from each College and Group who acts as a single point of contact for BCM issues and is supported by a deputy
Business Continuity Specialist		Representative from specialist areas (i.e. Estates, HR, Communications, Health and Safety, IS) who acts as a single point of contact for BCM issues and is supported by a deputy.
Business Continuity Deputy		Representative who acts as a depute for the BC Coordinator or BC Specialist of their College, Group or specialist area
Resilient Working Group	RWG	University-wide group which guides the development and provides sign-off for University-wide BCM methodologies, templates and strategies
Business Continuity Plan	BCP	Documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption
Business Impact Analysis	BIA	Process of analysing activities and the effect that a business disruption might have upon them
Competence		Ability to apply knowledge and skills to achieve intended results
Continual Improvement		Recurring activity to enhance performance
Crisis		An abnormal, unstable and complex situation that represents a threat to the **strategic** objectives, reputation or existence of an organisation
Essential services		A service to which priority must be given following an incident in order to mitigate impacts
Disaster Recovery	DR	The strategies and plans for recovering and restoring the organizations technological infra-structure and capabilities after a serious interruption
Emergency		An event or situation which threatens serious damage to human welfare, the environment or security of a place
Exercise		Process to train for, assess, practice, and improve performance in an organisation
Incident		Situation that might be, or could lead to, a disruption, loss, emergency or crisis
Maximum Acceptable Outage	MAO	Time it would take for adverse impacts, which might arise as a result of not providing a product / service or performing an activity, to become unacceptable.
Recovery Point Objective	RPO	Point to which information used by an activity must be restored to enable the activity to operate on resumption
Recovery Time Objective	RTO	Period of time following an incident within which an activity must be resumed
Risk		Effect of uncertainty on objectives
Risk Assessment		Overall process of risk identification, risk analysis and risk evaluation
Testing		Procedure for evaluation; a means of determining the presence, quality, or veracity of something

Note: Definitions above are from the British Standards Institute (ISO22301) and the Business Continuity Institute.