



For the future you want



BUSINESS CONTINUITY MANAGEMENT FRAMEWORK & POLICY

BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

Page

01

Introduction

02

Framework Statement

03

Business Continuity Management put into context

Page

05

The Business Continuity Management Lifecycle

09

Business Continuity Management Governance

Edinburgh College

RECEPTION ▲

♿ DISABLED PARKING ▲

Please Drive Carefully 10

1. INTRODUCTION

Business Continuity Management (BCM) is the framework for Edinburgh College to update, control and deploy an effective process to prepare for, respond to and recover from major disruptive events, which could detrimentally affect College operations.

The source of the disruption may be caused by internal events such as loss of key staff, loss of use of a building, or a technological systems failure, or, it might be caused by an external influence such as bad weather or a utility-related incident.

Edinburgh College has the following BCM objectives:

- To identify the major risk areas which could cause disruption to college business
- To establish defined plans to respond to critical incidents that cause a major disruption
- To establish BCM arrangements to respond to all identified risks
- To conduct regular reviews, audits and table top exercises of BCM plans, to ensure fit for purpose which lends itself to continuous improvement
- To raise the profile of BCM within Edinburgh College, and raise awareness to staff of BCM plans currently in place
- To work in partnership with other organisations to improve joint BCM planning, testing and review

2. FRAMEWORK STATEMENT

This Framework demonstrates how the College improves its resilience to major disruptions, so that key business systems and processes can be recovered, and business as usual restored as quickly as possible.

The Framework identifies four steps to embedding the BCM framework and policy within the College which constitutes the BCM life cycle:

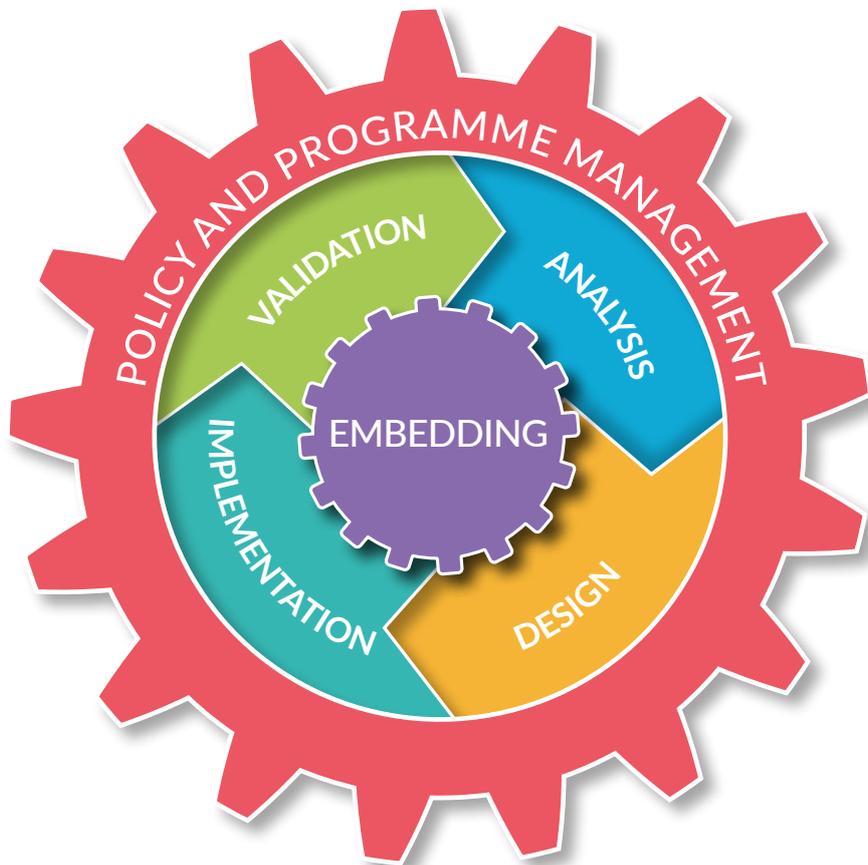
Step 1 – Analyse the risks to major disruption of College business through risk and business impact assessments, and identify recovery time objectives (RTOs) and recovery point objectives (RPOs) for identified critical services.

Step 2 – Design business continuity management plans (BCM plans) to respond to the major risks.

Step 3 – Implement BCM plans in response to critical and major incidents, and regularly test and review BCM plans.

Step 4 – Validate BIAs and BCM Plans through evaluation and audit of real incidents, tests and reviews to ensure continuous improvement.

The implementation of the BCM framework and policy is overseen by good policy and programme management through the College's Programme Management Office (PMO).



3. BUSINESS CONTINUITY MANAGEMENT PUT INTO CONTEXT

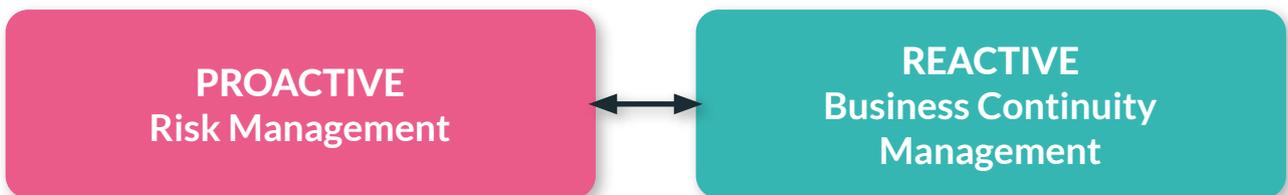
BCM and Risk Management

The College’s approach to BCM has a close relationship with the approach to risk management, and follows a similar methodology, focusing on prevention, preparedness, response, and recovery. The BCM framework also aligns to the ‘three lines of defence model’ (explained later in the governance section).

It is important to note that whilst similar, the two approaches are quite distinct. Risk management is concerned with minimising the probability and impact of a wide variety of risks relating to all areas of college business. Risk management alone will not completely prevent a critical or major disruptive event, as not every event is completely preventable. For example, adverse weather.



Consequently, a distinct approach to BCM is required to ensure a more detailed reactive approach to preparedness, response and recovery, with regards to significant and complex disruptive risks and events that may affect critical services.



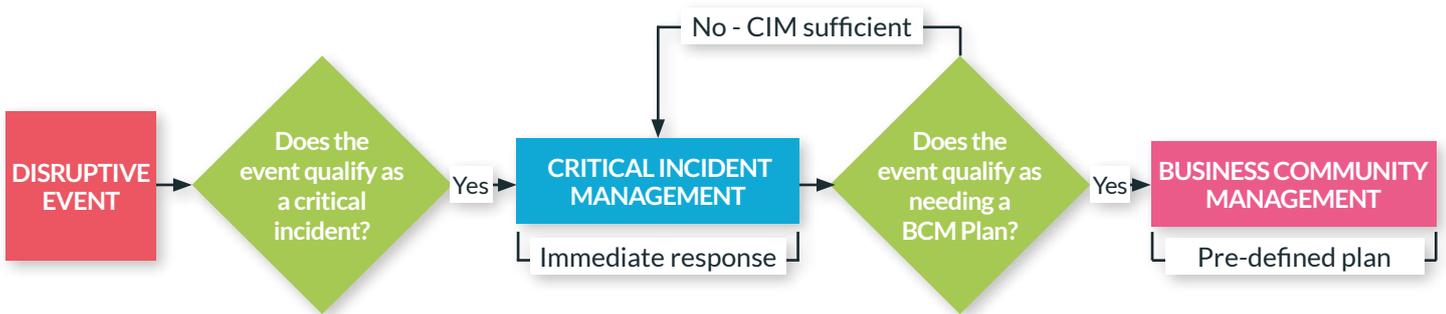
BCM and Critical Incident Management

While approaches to critical incident management (CIM), sometimes called emergency management, and BCM have overlapping interests, and both constitute reactive responses to major disruptive events affecting critical services, their primary goals are different.

CIM seeks to safeguard people and the college from significant harm as a result of a major disruptive event, and most often manifests as the actions that are taken immediately after an incident/accident occurs. CIM tends to be

more tactical in nature and has an initial focus on stopping/minimising the impact of the incident followed by decisive recovery actions.

BCM is focused on the restoration of services and returning to business as usual as quickly as possible after the critical incident has occurred. BCM is more strategic in nature and includes pre-defined plans that address the aftermath of specific wide-spread critical incidents and ensures the College is in a position to continue to operate and sustain long term recovery.



The diagram below demonstrates the relationship between the different elements of risk, critical incident and business continuity management, and their relationship to prevention, preparedness, response and recovery.

RELATIONSHIP BETWEEN RISK, EMERGENCY AND BUSINESS CONTINUITY MANAGEMENT

PREVENTION & PREPAREDNESS	EVENT	RESPONSE	RECOVERY
RISK MANAGEMENT <ul style="list-style-type: none"> H&S activity risk assessments Strategic risk management Operational risk management Sound risk management practices should seek to identify, assess, communicate and mitigate any business disruption related risks.	Incident/Accident (including injury or work hazard)	Routine Response (BAU)	
	Serious Incident/Accident (including out of hours response)	Non-Routine Response	
PLANNING <ul style="list-style-type: none"> H&S Policy/Procedure/Guidance Records Emergency Incident Policy & Procedure Testing/drills eg fire Critical/Incident management policy procedure Business impact assessments (BIA) to determine risks to college Business continuity plans (BCP) BCP testing/training exercises Lessons learnt from Post test report & Major incident report Systematic reviews of policy/procedures Planning should seek to build and maintain relationships and reinforce awareness of responsibilities	Disruptive Incident/Event (significant impact to College requiring principal/executive involvement)	HEALTH & SAFETY H&S incident and accident reporting via SHE portal	
	Business Stoppage (pre-planned response to critical incident)	EMERGENCY/IMMEDIATE INCIDENT TREATMENT Emergency Incident Policy & Procedures (RED folders Reception/Boardrooms)	
		CRITICAL INCIDENT MANAGEMENT <ul style="list-style-type: none"> Critical Incident procedure (RED folders Reception/Boardroom) Department BCM Plans (if required) Major Incident report	
		BUSINESS CONTINUITY MANAGEMENT <ul style="list-style-type: none"> Department BCM Plans (if required) Corporate BCM Plans (RED folders Reception/Boardroom) Partner Agency BCM Plans Major Incident report	

4. THE BUSINESS CONTINUITY MANAGEMENT LIFECYCLE

Step 1: Analysis

Gather and analyse information on the critical services provided by each department/faculty of the college and across the whole college, and identify what the main disruptive risks are to those services, through a process of business impact assessment.

Business Impact Assessment (BIA)

The BIA is a comprehensive analysis of critical business functions or services, and is designed to provide a high-level indication of the possible impacts, associated timescales and subsequent resource requirements, in the event of a major disruptive event.

A critical function / service is defined as:

- A service or function that underpins the capability to respond to emergency incidents and to take effective action to reduce, control or mitigate the effects of an emergency;
- The loss of a service or function could cause significant impact on human welfare or the environment;
- The service is legally mandated i.e. there is a statutory requirement to provide the service with the threat of litigation if the service is not delivered or delivered inadequately;
- The loss of the service would cause significant financial implications to the College;
- The loss of the service would significantly damage the reputation of the College.

Step 2: Design

Using the BIAs completed at step 1, step 2 involves designing BCM plans to identify what action must be taken, by who and by when, in response to a major disruptive event impacting on critical functions or services.

There are three types of business continuity management plans used in the College:

1. Departmental BCM plans

(Tier 3: Operational) – which address responses to major disruptive events specific to a certain department, faculty or area. e.g. Halls of residence plans for serious unplanned events, obtaining alternative facilities to deliver courses for serious unplanned events, etc.

2. Corporate BCM plans

(Tier 2: Tactical) – which address responses to major disruptive events that affect more than one department or college-wide services/functions. e.g. Adverse weather resulting in College closure.

3. Partner Agency BCM plans

– which address responses to major disruptive events which have an impact on the College, but which are developed and owned by partner agencies, who take the lead role in BCM implementation. e.g. NHS BCM plan for meningitis outbreak.

Both departmental and corporate BCM plans are reviewed by the head of the owning department before being submitted to the Risk Management and Assurance Group for approval. Once approved all documents are to proceed through the **Edinburgh College Corporate Documentation Procedure** before being published.

Step 3: Implementation

There are three elements to implementation (i) awareness and access (ii) real life incidents, and (iii) training and testing.

Awareness and Access

Once BCM plans have been developed and approved, it is important to ensure that staff across the College are aware of, and have access to, the range of BCM plans in place, in the event of a major disruptive event.

A list of all existing Corporate and Departmental BCM plans in place within Edinburgh College, are available on the intranet, college website and Executive Team and Senior Management Team laptops. Physical copies of all BCM plans can also be found in the red emergency folders available in the Boardroom at each college campus (x4).

Real Life Incidents

Implementation of BCM plans will take place in response to real life events, and as indicated above, such responses will be linked to the College's Critical Incident (emergency) Management Policy and Procedure.

Real life events, whilst sometimes tragic, can provide for a highly reliable form of test. Lessons learnt from the incident are likely to be absorbed as they are directly related to day to day experiences. These incidents tend to require limited resources other than those already deployed for day-to-day business.

After a BCM plan has been invoked in response to a real life event, an evaluation report should be produced to assist in the validation and continuous improvement process.

Testing/Training

Testing and training are critical steps in the implementation of BCM plans across the College. They are efficient ways to demonstrate how effective the developed BCM plans are, and how prepared the College is to respond to major disruptive events.

Testing and training also help find areas for improvement in BCM plans, which supports validation and continuous improvement of the approach to BCM in the College.

The table below provides guidance on the different approaches to testing and associated timescales. After each form of test some sort of evaluative report must be produced to assist with validation and continuous improvement.

APPROACH	WHAT IS INVOLVED?	BENEFITS/CHALLENGES	SLA
Component Test	Confirming that a key procedure or piece of equipment that is relied on in an incident works. Could be as simple as checking that contact procedures work (e.g. checking phone numbers on an emergency contact list).	<p>Benefits: Provides a more focused method of testing key procedures and equipment that are central to a plan are sound. Limited resources and time needed to implement this option. Enhances familiarity with the plan and encourages key people to question and challenge the assumptions made by getting them to think about real life scenarios.</p> <p>Challenges: Limited to testing a discreet area of your plan – unlikely to test your plan in a holistic way.</p>	<p>Frequency: As required - scheduled testing, after component failure or if recommended after walkthrough, rehearsal or real life incident.</p> <p>Responsible: Component owner/s.</p>
Walkthrough	A structured discussion involving key people responsible for responding to service disruptions. Involves discussion of how the team would respond in the event of different types of incident.	<p>Benefits: Enhances familiarity with the plan and encourages key people to question and challenge the assumptions made by getting them to think about real life scenarios.</p> <p>Challenges: Limited realism of approach and there is a danger the team could digress into theoretical discussion.</p>	<p>Frequency: Min. once per calendar year for each Department and Corporate BCM Plan or when requested by SMT/Exec Team.</p> <p>Responsible: Plan owner</p>
Rehearsal / Table Top	Key people who you rely on to respond to College disruptions rehearse their recovery, in real time to an incident. People play set roles either as participants or as facilitators. The scenario is highly controlled, with use of a script to prompt interactions to strict timescales.	<p>Benefits: A very realistic exercise type which provides a reliable test of the plan. It is dynamic, which ensures that lessons learnt and the value of business continuity is strongly reinforced. Highly effective form of training as this allows people to practice how they would respond to an incident in a way which is very memorable.</p> <p>Challenges: Resource intensive, requiring considerable time spent in planning and preparation as well as delivery of the event. Requires a number of people supporting the rehearsal who also require training to be able to carry this out. May involve short term disruption to business as usual.</p>	<p>Frequency: Min. once per calendar year for each Corporate BCM Plan. Department BCM Plan rehearsals completed if/as required or requested by SMT/Executive team.</p> <p>Responsible: SMT/Executive team.</p>

Step 4: Validate

The validation step will ensure BCM plans are fit for purpose, and will enable continuous improvement in the College's approach to BCM.

Work relating to the validation step should be informed by reports arising from testing and training activity and / or real life events (see step 3). There are two types of reports to be utilised in the College for this purpose:

Testing Report

Reporting on the outcomes of all conducted tests is important to support understanding and reflection on any lessons learnt. A post-test report is generated at the end of each test

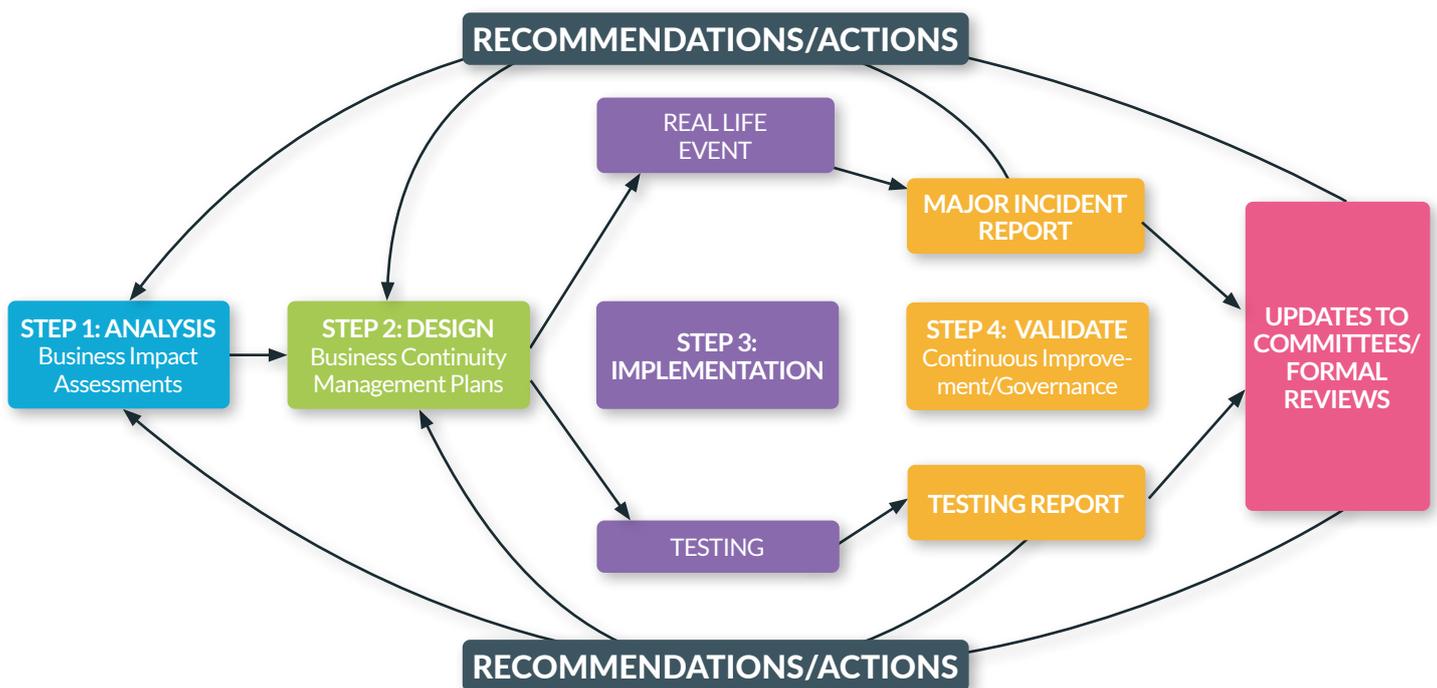
(as described in the above table) and includes the key actions to be put in place to improve resilience throughout the College.

Major Incident Report

Similarly to the recommendations garnered from testing, lessons learnt from real life major incidents (especially when a BCM plan is invoked) are crucial for building greater resilience within the College. A major incident report outlining the details of the incident and recommended actions for the BCM plan should be completed whenever a BCM plan is invoked.

Business Continuity Lifecycle Flow Chart

The diagram below demonstrates all four steps of the Business Continuity Lifecycle and the relationship between them all:



5. BUSINESS CONTINUITY MANAGEMENT GOVERNANCE

Listed below are the various internal and external arrangements which provide good governance of the BCM framework and policy:

GROUP	BCM ROLES AND RESPONSIBILITIES
Head's Departmental Management Team Meetings	Responsible for overseeing all BIA, BCM plans, implementation and validation activities at departmental level. Responsible for discussing and review the departmental approach every 3 months at management team meetings.
Risk Management and Assurance Group (RMAG)	Responsible for the corporate management and review of all BCM framework and policy matters within the College. Responsible for linking the BCM framework to the risk management arrangements within the College. Responsible for authorising analysis, design, testing and validating BIAs and BCM plans.
Senior Management Team (SMT) & Executive Team (ET)	Responsible for the BCM Framework and Policy and any changes to the framework and policy. Provide reports to Audit and Risk Assurance Committee / Board of Management. Coordinating internal and external audit activity with regard to BCM. Responsible for leadership in respect of critical incident management and invoking BCM plans.
Audit and Risk Assurance committee + Board of Management	Responsible for strategic scrutiny and assurance of the BCM framework and policy, and ensuring internal controls are in place.
Internal Auditors	Responsible for providing an objective analysis and evaluation of the BCM framework and policy, BIAs and BCM plans, and proposing any consequent improvement actions.

6. FURTHER INFORMATION

Further information about the Edinburgh College BCM framework and policy can be obtained from:

Nick Croft

Head of Communication Policy and Research
and Secretary to the Board of Management

Tel: **0131 344 7179**

Mobile: **07969 955386**

email: **nick.croft@edinburghcollege.ac.uk**



BUSINESS CONTINUITY MANAGEMENT FRAMEWORK & POLICY

For the future you want

For more information please visit:

edinburghcollege.ac.uk

or call +44 (0) 131 669 4400

 **EdinburghCollege**

 **#edinburghcoll**

 **EdinburghCollege**

 **edinburghcollege**

