Business Continuity Management Policy

Contents

Document Control

Review date, owner, classification

Review Date	Owner	Classification
June 2016	Corporate Business Continuity Management Group	Public
October 2014	Corporate Business Continuity Management Group	Public

Approval

Name	Position	Approval Date
SMG	Senior Management Group	27/06/07
CBCMG	Corporate Business Continuity Management Group	07/10/13

Version

Version No.	Date	Change
1.0	14/06/07	Initial document.
1.1	27/11/09	Document review and text corrected.
1.2	13/12/10	Document reviewed and relationship to CBCP added.
1.3	03/05/11	Minor changes and approved by CBCMG.
2.0	07/10/13	Changed to reflect updated system of BCM.
2.1	18/10/16	Document reviewed and text corrected.

If you have any suggested changes to this Policy, please notify:

Aileen Moore
Tel:028 701 23291
Email: aab.moore@ulster.ac.uk

Distribution List

Copy Number	Name	Location
001	Business Continuity website	www.ulster.ac.uk/bcm
002		
003		

References and related documents

Document Title
Corporate Business Continuity Plan (CBCP)
Major Incident Management Plan (MIMP)
Crisis Communication Management Plan (CCMP)
Emergency Operations Centre procedures (EOC)

1. Introduction

All entities of the Ulster University must have detailed Business Continuity Plans in place to ensure that Key Services can be continued in the event that a serious unplanned event occurs, which may disrupt the normal execution of those functions which support them.

2. Scope

This Business Continuity Management Policy covers the functions contained within the University's main campuses. It forms the basis for all Business Continuity Planning activities.

The policy is linked the Corporate Business Continuity Plan (CBCP) which guides recovery activity across the University and is implemented by the Corporate Business Continuity Management Group (CBCMG).

The Policy has two linked processes covered by the Major Incident Management Plan (MIMP) and the Crisis Communication Management Plan (CCMP).

Not all incidents will require their inclusion however, when required, this process has links to the MIMP and / or the CCMP. Refer to Appendix 1 & Appendix 2 for escalation process and diagram.

3. BCP Objectives

In the event of a disaster, it is the Ulster University's aim to meet the following objectives:

- Continue to operate Key Services at a level of operation that is acceptable to management;
- Provide timely availability of the functions necessary to operate Key Services;
- Ensure staff welfare and confidence;
- Maintenance of client / student / University stakeholders contact and confidence;
- Fulfilment of regulatory requirements;
- Control of expenditure / lower extraordinary costs caused by an event;
- Management of risk through the application of a risk management framework to priority areas.

4. Activities

The Business Continuity Management Policy covers the following activities:

Project Phase	Description
BCM Initiation and Management	**Coordination and Management of Business Continuity Planning Activities** This is the ongoing process of ensuring that the Business Continuity measures are coordinated and controlled. There will be a regular review and agreement made to ensure that Business Continuity Planning measures implemented in the various Ulster University locations are uniform, covering the interfaces and inter-dependencies between each location.
BCM Strategy	**Business Impact and Risk Analysis** This is the process for managing overall Ulster University risks by identifying functions which have a business continuity aspect, requiring preparation, active review and management attention. **Business Continuity Strategy Development** This is the process of identifying critical business functions and the personnel, IT and infrastructure required to support these functions in the event of a disaster. It also includes identifying suitable alternative locations, from which work can continue in a disaster and the identification of 'workaround' procedures in the absence of IT functionality.
BCM Documentation	**Corporate Business Continuity Plan** Provides a Corporate overview of business recovery issues across the university and supports the Business Continuity Plans held at Faculty, School, Directorate and Administrative area level. The Corporate Business Continuity Plan gives the agreed Recovery Time Objectives and Minimum Services Levels for Key Services within the University and provides a structure around which the selected recovery strategies for support functions and resources can be implemented. **Business Continuity Plan Development** This is the process of documenting the supporting Business Continuity Plans in the Faculty, School, Directorate and Administrative areas. The plans should contain sufficient detail to allow the resumption of Key Services and the supporting infrastructure identified in the Corporate Business Continuity Plan.

BCM Recovery	**Business Continuity Strategy Implementation** This is the physical provision of the infrastructure and resources required to support the recovery of critical business functions.
BCM Testing and Training	**Business Continuity Plan Tests and Training** This is the verification process, to ensure that employees are familiar with the Business Continuity measures implemented and that the infrastructure functions properly.
BCM Maintenance and Update	**Business Continuity Plan Update and Review** This is the continuous monitoring of the Business Continuity Strategy, plans and measures currently implemented, ensuring that changes in the way business functions are undertaken and changes in the supporting infrastructure are reflected in the Business Continuity Strategy and Plans.

5. Ownership and Responsibility

The Corporate Business Continuity Management Group (CBCMG) is responsible for defining and maintaining the framework for Business Continuity Management (including policy, strategy, corporate business continuity plan, overall implementation, plan documentation structure – including provision of business and support unit templates – tests and training concept, review and change management concept) and for initiating tests and reviews.

It is the responsibility of the business units to ensure that they have enough information in their specific section of the Business Continuity Plan, to enable them to recover from an incident and continue to provide Key Services to clients within acceptable timeframes and service levels as shown in the Corporate Business Continuity Plan.

It is the responsibility of the support units to ensure that they have enough information in their specific section of the Business Continuity Plan, to enable them to recover the infrastructure and services required to support business recovery activities within Recover Time Objectives (RTO’s) and Minimum Services Levels (MSL’s) shown in the Corporate Business Continuity Plan.

6. Audit

The University's Internal Auditor shall consider coverage and review of this policy during the course of the agreed audit programme or for any ad-hoc investigations.

Appendix 1 - BCP Escalation Process

Incidents are defined to be one of four levels of significance.

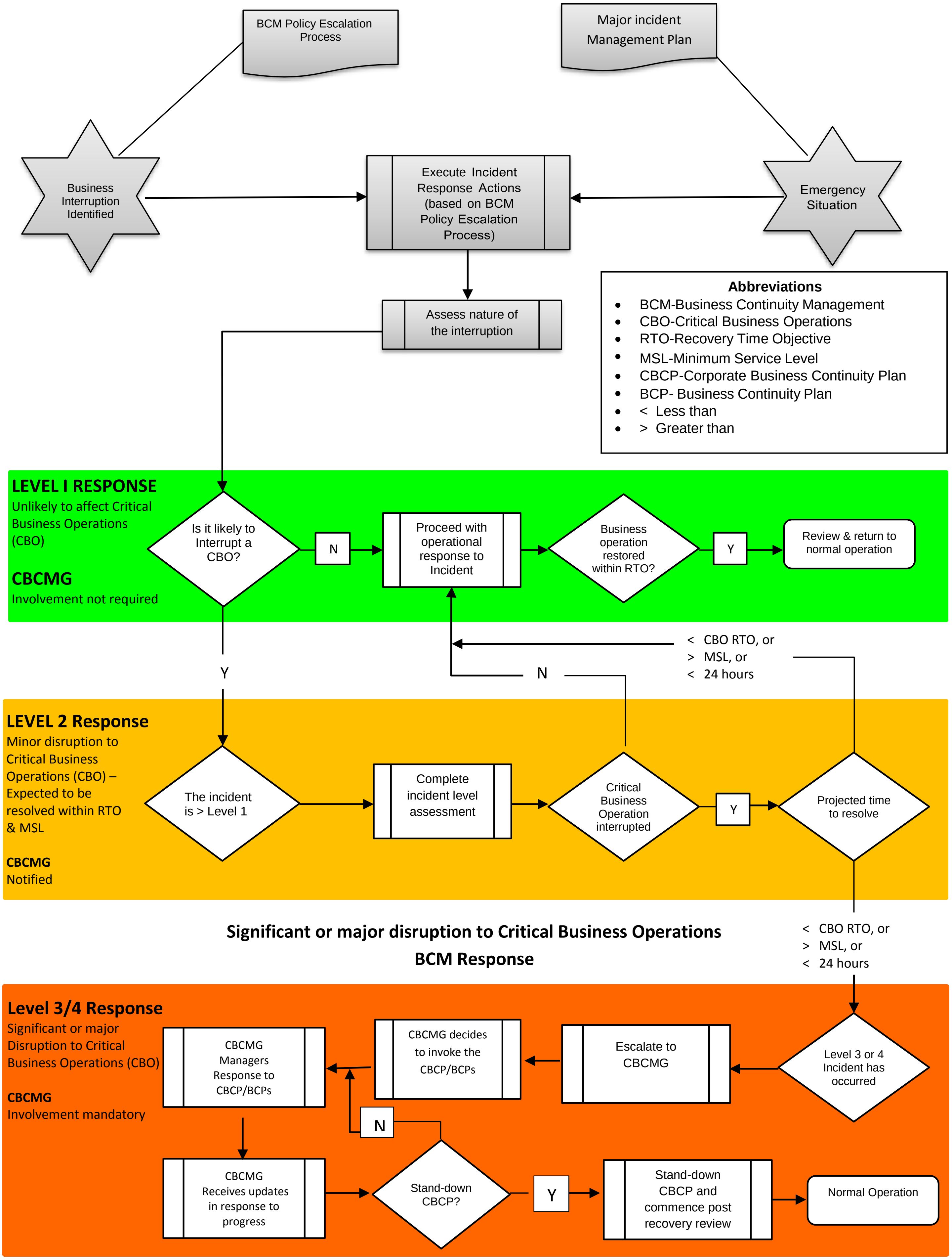
The level of an incident is initially set by the Incident Management Team (IMT); however, the Corporate Business Continuity Management Group (CBCMG) has full discretion over the assigned level.

Typically, full invocation of the Business Continuity Plan (BCP) only occurs given a level 3 or 4 incident and is based on the Recovery Time Objectives and Minimum Services Levels for Key Services given in the Corporate Business Continuity Plan.

The four levels of escalation for an incident are defined in the following table.

Level	Description	One or more of the following apply:
1	**Minor incident** (Normal Operating Procedures Apply)	• The incident is unlikely to affect Key Service operations. • The incident can be dealt with and closed at an operational level by the functional unit. **CBCMG involvement not required.**
2	**Minor disruption to critical business process** (Normal Operating Procedures Apply)	• Key Service function interrupted (expected to be dealt with inside the Key Service Recovery Time Objective (RTO) and Minimum Services Levels (MSL)). **CBCMG notified.**
3	**Significant disruption**	• Denial of access to the work environment, or key facility, key supporting technology component or data that is expected to go beyond 24 hours. • Key Service function interrupted (may go beyond the Key Service RTO or below MSL) **CBCMG involvement mandatory.**
4	**Major disruption**	• Denial of access to the work environment, or key facility, key supporting technology component or data is expected to go beyond the Key Service RTO or below MSL. • Key Service function interrupted (expected to go beyond the Key Service RTO or below MSL) **CBCMG involvement mandatory.** **Corporate Business Continuity Plan invoked.**

Appendix 2 - BCP Escalation Process Diagram


BCM Policy Escalation Process
Major incident Management Plan
Business Interruption Identified
Execute Incident Response Actions (based on BCM Policy Escalation Process)
Emergency Situation
Assess nature of the interruption
LEVEL I RESPONSE
Unlikely to affect Critical Business Operations (CBO)
CBCMG
Involvement not required
Is it likely to Interrupt a CBO?
N
Proceed with operational response to Incident
Business operation restored within RTO?
Y
Review & return to normal operation
< CBO RTO, or
> MSL, or
< 24 hours
N
Y
LEVEL 2 Response
Minor disruption to Critical Business Operations (CBO) – Expected to be resolved within RTO & MSL
CBCMG
Notified
The incident is > Level 1
Complete incident level assessment
Critical Business Operation interrupted
Y
Projected time to resolve
Significant or major disruption to Critical Business Operations
BCM Response
< CBO RTO, or
> MSL, or
< 24 hours
Level 3/4 Response
Significant or major Disruption to Critical Business Operations (CBO)
CBCMG
Involvement mandatory
CBCMG Managers Response to CBCP/BCPs
CBCMG decides to invoke the CBCP/BCPs
Escalate to CBCMG
Level 3 or 4 Incident has occurred
N
CBCMG Receives updates in response to progress
Stand-down CBCP?
Y
Stand-down CBCP and commence post recovery review
Normal Operation

Abbreviations

- BCM-Business Continuity Management
- CBO-Critical Business Operations
- RTO-Recovery Time Objective
- MSL-Minimum Service Level
- CBCP-Corporate Business Continuity Plan
- BCP- Business Continuity Plan
- < Less than
- > Greater than

Appendix 3 - Schedule of Terms

Business Continuity Management (BCM)

The University faces a variety of risks whether they are from external forces or internally. Internal risks arise both at the strategic (organisation-wide) level and at the operational (business process) level.

The objective of business continuity management is to ensure the uninterrupted availability of all key business resources to support essential (or critical) business activities.

Business Continuity Management Policy

A Business Continuity Management Policy sets out an organisation's aims, principles and approach to BCM, what and how it will be delivered, key roles and responsibilities and how BCM will be governed and reported on.

Business Continuity Plan (BCP)

A Business Continuity Plan is a documented plan for use at the time of a business continuity emergency, event, incident or crisis.

The plan covers key personnel, resources, key services and actions required to manage the BCM process in the business units.

Corporate Business Continuity Management Group (CBCMG)

Corporate Business Continuity Management Group is the highest level of management for Business Continuity.

The CBCMG is responsible for invoking the Corporate Business Continuity Plan (CBCP) and for overseeing any recovery efforts, as well as acting as the committee who oversee the on-going maintenance and development of the CBCP.

Corporate Business Continuity Plan (CBCP)

A Corporate Business Continuity Plan is a documented plan for use at the time of a business continuity emergency, event, incident or crisis.

The plan covers invocation, Key Services, their Recovery Time Objective and Minimum Service Level. It also contains the actions required to manage the BCM process in the University.

Crisis Communication Management Plan (CCMP)

The principal function of the Crisis Communication Management Plan is to ensure effective communication, both internal and externally to the University, during an emergency or crisis.

Emergency Operations Centre (EOC)

An EOC is the physical location where key decision makers in an organisation come together during an emergency or crisis to co-ordinate response and recovery actions and resources. The EOC is not an incident command post; rather, it is the centre of operations where co-ordination and management decisions are facilitated.

Key Services

Are those University services, identified in the CBCP, which are essential for the University’s survival.

Major Incident Management Plan (MIMP)

The principal function of the Major Incident Management Plan is to ensure the safety of the campus community. To this end, the co-operation of all persons in observing the MIIP and procedures, and in the event of an emergency the instruction given by Security is required.

It is impossible to plan in detail for every eventuality. This plan therefore attempts to establish a framework for the effective handling of emergencies and/or disasters.

Minimum Service Level (MSL)

Following an incident it may not be practical or desirable to immediately recover a business process to its former state. The Minimum Service Level defines the level to which the process must be recovered during the recovery period, recovery to normal service levels can be deferred until later.

Recover Time Objective (RTO)

A target time set for resumption of product or service delivery after an incident; or resumption of performance of an activity after an incident; or the recovery of an IT system or application after an incident.

Appendix 4 - References

- *BS 25999-1:2006 Business continuity management – Part 1: Code of Practice*

- *The Business Continuity Institute - Good Practice Guidelines*

- *HM Government Emergency Preparedness Guidance on Part 1 of the Civil Contingencies Act 2004*