BUSINESS CONTINUITY STRATEGY 2014-2017

This strategy covers the period 01 April 2014 – 31 March 2017 and was approved by the Major Incident Working Group 19.03.2014

Caroline Rushmer
Major Incident and Business Continuity Manager

Document Name:	Oxford Brookes University Business Continuity Strategy 2014-2017
Document Owner:	Caroline Rushmer

Version Control		
Version	**Date**	**Change**
0.1	24.05.2013	First draft
0.2	09.01.2014	Second draft
0.3	19.03.2014	Approved by MIWG

Sign off Control		
Version	**Committee Name**	**Date of Final Sign Off**
0.3	Major Incident Working Group	19.03.2014
0.3	Executive Board	31.03.2014

Contents

Acronyms used in Oxford Brookes Major Incident and Business Continuity documents:

BC	Business Continuity
BCM	Business Continuity Management
BIA	Business Impact Analysis
CIO	Chief Information Officer
IT DR	Information Technology Disaster Recovery (Plan)
MI	Major Incident
MIBCM	Major Incident and Business Continuity Manager
MIP	Major Incident Plan
MIT	Major Incident Team
MIWG	Major Incident Working Group
MADL	Maximum Acceptable Data Loss
MAPD	Maximum Tolerable Period of Disruption
MIBCM	Major Incident and Business Continuity Manager
RTO	Recovery Time Objective
SMT	Senior Management Team

Introduction

Oxford Brookes University has a robust business continuity methodology and processes. Over the past three years many improvements have been made including the publication of an updated BC plan (BCP) in line with the University's redesigned Major Incident Plan (MIP), both of which are aligned to sector good practice. An updated Business Continuity Policy has been published and a Major Incident and Business Continuity Google site has been developed as a central repository of key documentation. Staff receive regular training and are involved in MI and BC exercises.

The following document outlines the strategy to achieve an integrated business continuity and major incident management process for Oxford Brookes. The overall objective of the strategy is to try and ensure that organisational resilience is effective and becomes embedded as part of good management practice.

The strategy identifies the measures that should be taken over the next three years to ensure that Oxford Brookes develops a resilience in terms of preventing or minimising the effects of a major incident, whatever the cause, and ensuring the swift recovery from it.

The strategy starts by defining business continuity in an operational framework followed by 6 key aims. It then moves on to identify 5 key objectives and methodologies for obtaining the objectives stated.

Business Continuity Management Framework

Business Continuity Management is defined as an operational framework that seeks to:

1. Understand its critical activities and maintaining the capability to resume operations within agreed timeframes, following the deployment of a contingency planning response.

2. Increase resilience by protecting critical assets and data (electronic and otherwise) through a co-ordinated approach to management and recovery.

3. Minimise impacts using a focused, well-managed response activity.

OBU Business Continuity Policy Statement 2012

Aim

To improve organisational resilience through robust plans to respond to, manage and recover from any sudden disruption of business. Specifically:

1. Ensure the safety of students, staff, visitors and the local community.

2. Ensure as far as practicable that critical processes and resources are recovered in the event of major incident before their non-performance threatens the long term performance of part, or all, of the University.

3. Maintain the reputation of the organisation.

4. Complement the university's Risk Management framework by identifying and planning for high impact scenarios where BCM is the appropriate risk mitigation strategy.

5. Provide a framework of management and decision making that will result in an agreed recovery program that has minimised the impact of the event.

6. Comply with good practice and sector standards.

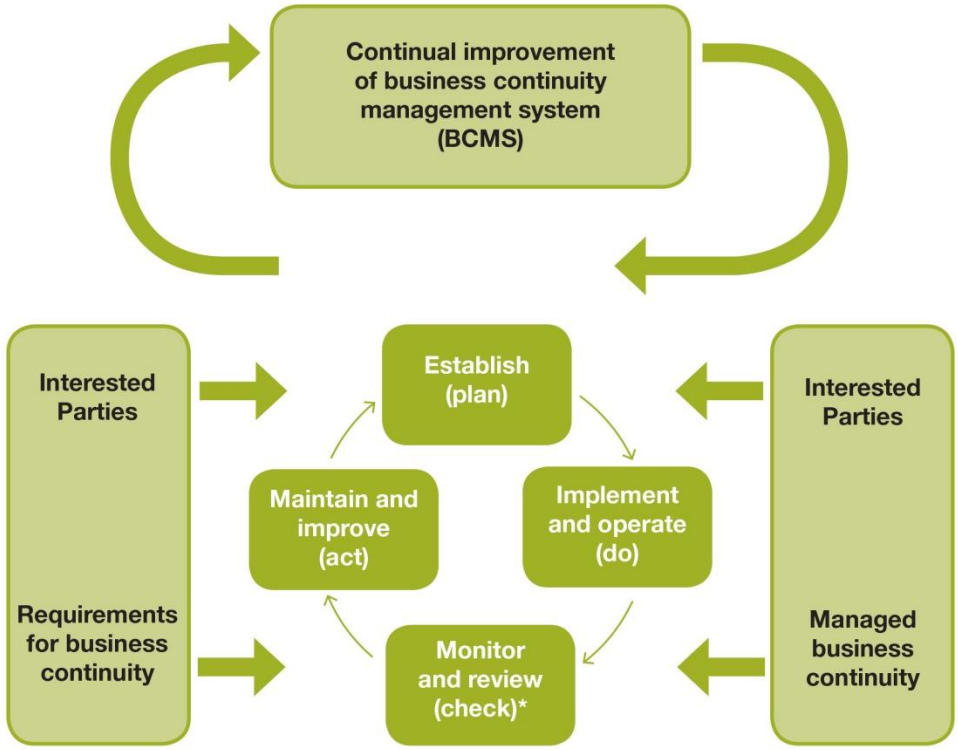
Key Objectives

1. Maintain, develop and review directorate and faculty BCPs and BIAs and IT DR plan.

2. Ensure that we have knowledgeable, experienced and effective BC teams within faculties and directorates through BCP exercises and testing, including the Information Technology Disaster Recovery Plan (IT DR).

3. Embed BCM within the organisation and create an ethos whereby building resilience and mitigating vulnerability should be regarded as an aspect of normal business under strategic direction (BCPs).

4. Increase risk awareness and horizon scanning.



PLAN-DO-CHECK-ACT (PDCA) MODEL APPLIED TO THE BUSINESS CONTINUITY MANAGEMENT SYSTEM PROCESSES

Plan — *Establish* BC policy / objectives / targets / controls / processes and procedures to improve BC. Outcome will be to deliver results aligned to OBU's policies and objectives.

Do — *Implement and operate* BC policy / controls / processes and procedures.

Check — *Monitor and review* against BC policy and objectives. Report results to senior management for review. Identify learning outcomes and implement change.

Act — *Maintain and improve* the BC process by taking corrective action, based on results of the review. Review scope of BC policy and objectives.

ISO22301:12 follows on from BS25999

Key Objective 1 – Maintain, develop and review directorate and faculty BCPs and BIAs and IT DR plan

Ref. No	Methodology	Lead	Dependencies	Timeline
1.1	BCPs will be reviewed annually as a whole and individual plans as required following the occurrence of an incident or following recommendations from an exercise	MIBCM/BCP owners	Review dates in diaries and staff tasked	Annually on anniversary of publication
1.2	BCPs will have 6 monthly updates to contact details	MIBCM/BCP owners	Review dates in diaries and staff tasked	Annually in November and May
1.3	BIAs will be reviewed annually as a whole and individual plans as required following the occurrence of an incident or following recommendations from an exercise	MIBCM/BCP owner	Review dates in diaries and staff tasked	Annually on anniversary of publication
1.4	Review faculty and directorate BCP and BIA plans annually to ensure that they are current and meet the needs of the University	MIBCM	Completion of annual updates	Annually (July) and report to MIWG
1.5	BCP and BIAs to be updated within 6 months of any organisational change	MIBCM / BCP owner	Diaried time	Within 6 month of change
1.6	Ensure up to date BC and BIA plans are available to relevant staff via the University MIBC Google Site	MIBCM	Updates received from plan owners	Diaried 6 monthly
1.7	Review IT DR plan annually to ensure that they are current and meet the needs of the University	MIBCM	Updates received from OBIS	Annually (August)
1.8	Review, update and publish Campus Closure Plan	MIBCM	Updates received	Annually (December)
1.9	Ensure up to date copy of University Flu Pandemic Plan and Meningitis Plan is available on the MIBC Google Site	MIBCM	Updates received	Annually (December)
1.10	Maintain and update contact lists for MIT	MIBCM	Receiving updates from MIT	Twice yearly – December and July and on staff changes
1.11	Following incidents, workshops, exercises or audits, follow up and implement any recommended actions	MIBCM with those listed for actions	Diaried time	Within 3 months

Key Objective 2 – Ensure that we have knowledgeable, experienced and effective BC teams within faculties and directorates through BCP exercises and testing, including the Information Technology Disaster Recovery Plan (IT DR)

Ref. No	Methodology	Lead	Dependencies	Timeline
2.1	Run a rolling programme of exercises for faculty and directorates so as to validate plans are complete and accurate and to familiarise staff with the contents and their roles within BC plans	MIBCM	Participation by faculty and directorate staff. Diaried time	Rolling programme
2.2	Post BCP exercise, produce a report and recommended actions. Follow up and implement any recommendations. Ensure documents updated and re-published	MIBCM	Diaried time	Within 3 months of test
2.3	Run a IT DR plan exercise so as to validate plans are complete and accurate and to familiarise staff with the contents and their roles	MIBCM/CIO	Diaried time	Annually
2.4	Post IT DR exercise, produce a report and recommended actions. Follow up and implement any recommendations. Ensure documents updated and re-published	MIBCM	Diaried time	Within 3 months
2.5	Biennial exercise of the MIP with the MIT	MIBCM	Agreed aim of exercise and MIT participation	Bi-annually in October
2.6	Ensure that all first responders receive regular training on correct response and procedures	MIBCM with EFM	Diaried time	Annual training in July

Key Objective 3 – Embed BCM within the organisation and create an ethos whereby building resilience and mitigating vulnerability should be regarded as an aspect of normal business under strategic direction (BCPs)

Ref. No	Methodology	Lead	Dependencies	Timeline
3.1	Regular training and exercises throughout the organisation to continuously develop responders knowledge and capability	MIBCM	Participation by faculty and directorate staff. Diaried time	Rolling programme
3.2	Provide new members of University, Faculty and Directorate SMT with an introduction to MIP, BC and BIA plans within first 3 months service	MIBCM	Participation by new staff and diaried time	On going
3.3	Work with Corporate Affairs to ensure effective communication policy / strategy is maintained and updated	C/A	Availability of CA staff	Review January and June
3.4	Review BC capability of key suppliers of services and goods as per agreed policy and report back results to MIWG	MIBCM	FLS applying policy	Rolling programme
3.5	Ensure MIT Command Centre locations are ready for operations by testing telephones, data points and battle boxes	MIBCM	Diaries dates	December and August
3.6	Maintain and develop the Google Site for Major Incident and Business Continuity Management so that key documents and contact lists are available on and off-campus	MIBCM		Ongoing

Key Objective 4 – Increase risk awareness and horizon scanning

Ref. No	Methodology	Lead	Dependencies	Timeline
4.1	Increase risk awareness through training and exercises.	MIBCM	Participation by University SMT, faculty, directorate staff. Diaried time	Rolling programme
4.2	Liaise with Police, Oxfordshire Resilience Group, HE Business Continuity Network. Attend meetings, courses and conferences.	MIBCM	Diaried meetings and E-mail updates	Annual conference, quarterly meetings

Key Objective 5 – Roles and responsibilities

Ref. No	Methodology	Lead	Dependencies	Timeline
5.1	The Board of Governors has responsibility for overseeing the Major Incident and Business Continuity Management within the University as a whole.	Registrar		Rolling programme
5.2	The Registrar is responsible for development specific programmes and procedures for establishing and maintaining major incident and business continuity development and testing activities	Registrar		Rolling programme
5.3	The Registrar is responsible for co-ordinating the University's response to a major incident in line with the Major Incident Plan	Registrar		Rolling programme
5.4	The Registrar is the Chair of the Major Incident Working Group which meets quarterly and oversees the development of formal incident and business continuity procedures	Registrar		Rolling programme