ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-002 - Business Continuity Management and Planning Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	06/03/2017
Document Security Level:	**PUBLIC**
Document Version:	1.10
Document Ref:	EA-ISP-002
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/EA-ISP-002-Business-Continuity-Management-and-Planning-Policy.pdf
Review Date:	March 2018

EA-ISP-002 - Business Continuity Management and Planning Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	ESA	Initial version drafted	08/02/2014			
0.91	SF, PD	Head of School of Computing, Associate Professor	Added in changes recommended	05/03/2014			
0.92	PF	ESA	Finished the appendix (explanatory notes)	19/03/2014			
0.93	PF	ESA	Moved to new document template	10/03/2015			
1.00	PW, AH, GB, CD, PF	IT Director, TIS HoS & EA	Approved document	13/03/2015	Paul Westmore	IT Director	13/03/2015 11:15
1.10	PF, CD	ESA & EA	Revised document to use new University risk register rating	06/03/2017			

EA-ISP-002 - Business Continuity Management and Planning Policy

Introduction

The Business Continuity Management and Planning Policy sets out the process for assessing and addressing risks to business continuity and defines the responsibilities for preparing and implementing business continuity plans (BCP).

This policy is however, specifically focussed around business that necessitates the use of technology to continue business-as-usual (BAU), it should complement the University's Disaster Recovery & Business Continuity Plan[1], which is held and maintained by Finance and Sustainability.

Usually there will be a number of systems, each with different continuity requirements depending on the level of criticality to the organisation. The risk assessment process to classify systems should be aligned with the organisations risk register that uses the categories very low, low, medium and high, this allows appropriate business continuity plans for each system or classification can then be produced.

Please refer to the appendix for further explanation of the points below.

1. Definitions

Very Low Criticality Systems	Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Business can continue using manual processes for up to the RTO timescale.	Business can continue using manual processes for up to the RTO timescale.	Business can continue using manual processes for up to the RTO timescale.	Business can continue using manual processes for up to the RTO timescale.
A replacement for the failed system must be in place within the RPO value.	A replacement for the failed system must be in place within the RPO value.	A replacement for the failed system must be in place within the RPO value.	A replacement for the failed system must be in place within the RPO value.
Relevant departmental plans accommodate a failure up to the RTO timescale.	Relevant departmental plans accommodate a failure up to the RTO timescale.	Relevant departmental plans accommodate a failure up to the RTO timescale.	Relevant departmental plans accommodate a failure up to the RTO timescale.
Awareness of system needs to be included in information systems continuity.	Purchasing strategies/plans incorporate their role in information systems continuity.	Estates, purchasing and insurance strategies/plans incorporate their role in information systems continuity.	
Recovery Time Objective (RTO) The target time to recover your systems and business activities after a disaster has struck.			
Twelve weeks	Four weeks	Five days	Two days
Recovery Point Objective (RPO) The amount of data loss that is tolerable for the affected systems.			
Four weeks	One week	One day	Four hours
Example System			
Display Screen Equipment	Inter Library Loans System	Staff Records System	Digital Learning Environment (DLE)

[1] University Emergency Business Continuity Plan

Changing Criticality	Certain systems may become more critical at certain times of the year than others, for example, the University telephony service may be deemed to be of a medium criticality, but during Clearing its criticality may be raised to ensure business as usual will be restored quicker than if left as originally defined.
Defining Criticality	When a system is designed or significantly upgraded (such as a service pack or major release version change) the criticality will be defined for the system and stored for ease of reference at a later date.

2. Initiating the BCP Project

2.1 The Technology and Information Services management team are required to initiate a business continuity plan.

3. Processing the BCP Security Risk

3.1 The Technology and Information Services management team are required to undertake a formal risk assessment in order to determine the requirements that should inform the business continuity plan.

Very Low Criticality Systems	Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
A few systems have been assessed against the most likely risks to occur.	A small sample of systems have been assessed against the most likely risks to occur.	A large sample of systems have been assessed against known risks.	All systems have been assessed against known risks.
Simple steps have been taken to mitigate against obvious risks.	Simple steps have been taken to mitigate against obvious risks.	Steps to mitigate against the most likely risks have been identified and implemented where appropriate	All feasible steps to mitigate against risks have been implemented.

4. Developing the BCP

4.1 The Technology and Information Services management team are required to develop a business continuity plan which covers all essential Information Technology business activities.

Very Low Criticality Systems	Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
There is a documented recovery procedure.	There is a documented recovery procedure.	Continuity plan covers: • Recovery procedures for most likely scenarios • Any temporary arrangements	Continuity plan covers: • Recovery procedures for most likely scenarios • Any temporary arrangements • Disaster recovery

			contracts • Replacement equipment arrangements • Relocations arrangements

5. Testing the BCP

5.1 The business continuity plan is to be periodically tested to ensure that the management and staff understand how it is to be executed.

Very Low Criticality Systems	Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Continuity plans are tested on a few systems after any major system change.	Continuity plans are tested on a small sample set of systems after any major system change.	Continuity plans are tested on a sample set of systems after any major system change.	Continuity plans are tested on a sample set of systems every six months and after any major system change.

6. Training and Staff Awareness on BCP

6.1 All appropriate staff must be made aware of the business continuity plan and their own respective roles.

7. Maintaining and Updating the BCP

7.1 The business continuity plan is to be kept up to date and retested periodically.

Very Low Criticality Systems	Low Criticality Systems	Medium Criticality Systems	High Criticality Systems
Continuity plans are reviewed periodically, for example, when any major service change occurs.	Continuity plans are reviewed periodically, for example, when any major service change occurs.	Continuity plans are reviewed annually.	Continuity plans are reviewed six monthly.

Appendix

2. Initiating the Business Continuity Plan

Explanatory Notes
The Business Continuity Plan (BCP) project needs to be initiated, formerly approved and supported by the board and governing body of the organisation.

Scope of the Business Continuity Plan
For each system, it will be necessary to assess the longest period for which the system could be unavailable without serious detriment to the organisation. This will indicate the criticality of the system.

3. Processing the BCP Security Risk

Explanatory Notes
Risk assessment, as part of business continuity planning, analyses the nature of such unexpected occurrences, their potential impact, and the likelihood of those occurrences becoming serious incidents.

Risk Assessment for the BCP
Risk assessment should be undertaken for all systems which form part of the organisations infrastructure.

The outcome of the risk assessment should be the classification of the systems according to their criticality to business processes.

Systems where a failure would result in the loss of service or where only a small number of people would be affected will have a low criticality whereas systems where failure would be catastrophic or would affect many people will have high criticality.

4. Developing the BCP

Explanatory Notes
The business continuity plan is a project plan which is likely to be complex and detailed.

Irrespective of the nature of the organisation, it should probably contain a series of critical actions to be taken in the event of a failure or disaster which should culminate in a return to normal operations.

Information security issues to be considered when implementing the policy should include:

- When the need arises to trigger the BCP, but:
  - It does not exist, or
  - Is untested, or
  - Is non-viable, or
  - Fails when activated.

The organisation's operations may not be able to recover – ever.

5. Testing the BCP

Explanatory Notes
Testing your organisation's business continuity plan (BCP) assess its viability, and ensures that your staff are conversant with the proposals.

6. Training and staff awareness on the BCP

Explanatory Notes
If a business continuity plan is to be executed successfully, all personnel must not only be aware that the plan exists, but also know its contents, together with the duties and responsibilities of each party.

7. Maintaining and Updating the BCP

Explanatory Notes
The maintaining and updating of the business continuity plan (BCP) is critical if its successful execution is to be relied upon.