Business Continuity Policy

Ref:	LSCICB_BC02
Version:	*Version 2*
Purpose	This policy sets out the general principles and framework for the creation and revision of a business continuity management system and business continuity plans relevant to the key business activities / services of the ICB.
Supersedes:	*Version 1.1 January 2024*
Author (inc Job Title):	*Alison Whitehead* *Head of EPRR*
Ratified by: (Name of responsible Committee)	*ICB Board*
Cross reference to other Policies/Guidance	NHS England Business Continuity Management Toolkit April 2023 PR1254 Civil Contingencies Act 2004 Health and Care Act 2022 NHS EPRR Framework ISO 22301:2019 – Security and Resilience - Business Continuity Management System – Requirements ISO 22313:2020 Security and Resilience - Business Continuity Management System – Guidance The Publicly Available Specifications (PAS) 2015 BCI Good Practice Guidelines (2018)
Date Ratified:	15th May 2024
Date Published and where (Intranet or Website):	22nd May 2024 Intranet, Website, Resilience Direct
Review date:	*May 2027 (3 years) or earlier if needed*
Target audience:	All NHS L&SC staff

This policy can only be considered valid when viewed via the ICB website or ICB staff intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one published.

The EPRR Team will ensure that a hard copy of this document (latest approved version) is available in the Incident Coordination Centre.

Copies of all previous versions of this document will be archived by the EPRR Team.

Document control:		
Date:	**Version Number:**	**Section and Description of Change**
24/8/2022	1	Initial draft
13/9/2022	1	Update following feedback from neighbouring ICB, following Major Incident. Changes to section 4.3
19/9/2023	1.1	Updated by Head of EPRR to include Information Governance and Information Technology
29/4/2024	2	Updated / reviewed in line with national guidance and the requirements of the EPRR core standards 2023

Contents

1   Introduction

1.1   NHS Lancashire and South Cumbria Integrated Care Board (NHS L&SC) has a duty to plan for and respond to a wide range of incidents, emergencies or disruptions that could affect the health of the community or the delivery of patient care.

1.2   The Civil Contingencies Act 2004 (CCA) and the NHS Act 2006 as amended by the Health and Care Act 2022 requires NHS organisations to have plans in place to respond to such incidents while maintaining services to patients. This programme of work is referred to in the health community as Emergency Preparedness, Resilience, and Response (EPRR).

1.3   NHS Lancashire and South Cumbria ICB is a Category 1 Responder under the CCA and therefore subject to the full set of civil protection duties, including putting in place robust business continuity management arrangements.

1.4   The NHS Core Standards for EPRR, last revised in 2023, set out the requirement to put in place continuity arrangements for all NHS organisations and providers of NHS funded care. This means that services should be maintained to set standards during any disruption or recovered to these standards as soon as possible. This also extends to services provided through partnerships or other forms of contractual arrangement. This Policy is aligned to the requirements of the relevant business continuity core standards (currently standards 46 to 53).

1.5   A business continuity management (BCM) system provides a holistic management process that identifies potential threats to NHS organisations and the impact to business operations those threats, if realised, might cause. [1] This holistic approach to BCM is an essential tool in establishing an organisations resilience.

1.6   Business Continuity Management (BCM) is a process that seeks to ensure that there is minimal disruption to critical services, information assets and core business in the event of a major interruption / breakdown / incident and assists departments to reinstate normal services as quickly as possible. Business continuity (BC) is a key component of resilience, and all NHS funded organisations have been asked to align their business continuity arrangements with the requirements of ISO 22301 – Business Continuity Management System.

1.7   It is imperative to understand the functions and service interdependencies of the organisation, both internal and external when designing a business continuity system. Therefore, working with key teams such as EPRR, Human Resources, ICT, Health & Safety, Risk Management, and Information Governance, amongst others, is critical to ensure systems align and prevent complications as they are implemented and embedded.[1]

---

[1] NHS England Business Continuity Management Toolkit April 2023 PR1254

2   Purpose and Scope

2.1   Business continuity is defined as the capability of an organisation to continue to deliver services, at acceptable predefined levels, following a disruptive incident (ISO 22301).

2.2   This Policy provides the intentions and direction of NHS L&SC in relation to business continuity management, as supported by the Chief Executive, Accountable Emergency Officer, and Executive Board.

2.3   This Business Continuity Policy outlines how NHS L&SC will implement an effective business continuity management system. The policy sets out the general principles and corporate framework for the creation and revision of a Business Continuity Management System (BCMS) relevant to the business activities of Lancashire and South Cumbria ICB. The policy defines the activities for establishing and maintaining an on-going BCM capability.

2.4   The scope of the BCMS is to practically identify critical business functions, systems and dependencies and risks, ensuring plans are put in place to mitigate these risks.

3   Aims and Objectives

3.1   The aim of this policy is to establish a business continuity management system (BCMS) that enables Lancashire and South Cumbria ICB to be a resilient organisation, capable of maintaining its key services and prioritised activities in the event of a disruption.

3.2   Objectives

- Provide a framework for the development of a robust and consistent BCMS.
- Identify and mitigate business continuity risks to which the ICB may be exposed.
- Protect the wellbeing of its employees and critical assets.
- Undertake business impact analyses and risk assessments (in line with the Risk Management Policy LSCICB Corp12) on key services and their supporting prioritised activities, processes and resources at least annually (more frequently if necessary).
- Ensure that the ICB can continue to meet the needs of its stakeholders in the event of a disruption.
- Provide a whole system approach to the patient care pathway by having realistic resilience and continuity arrangements in place.
- To take into account complex business continuity incidents. Where multiple risks are realised at once (compound failures).
- Identify and implement suitable strategies to mitigate the potential loss of people, information and data, premises, suppliers and contractors and IT and infrastructure

- Ensure that the necessary training and awareness is available to ensure all ICB staff are aware of their roles and responsibilities.
- Promote and maintain the reputational integrity of the ICB.
- Align its BCMS activities to ISO 22301 business continuity requirements and supporting guidance (including the NHS Business Continuity Management Toolkit PR1254 – April 2023)
- Provide necessary assurance to NHS England that EPRR standards relating to business continuity can be met.
- As a Category One Responder under the Civil Contingencies Act 2004 and through compliance with NHS England EPRR Core Standards, preparing to respond to emergencies is an element of business-as-usual activities for staff at all levels.

4 Roles and Responsibilities

4.1 The Chief Executive Officer

4.1.1 Ensures that the Board receives regular reports, at least annually, regarding emergency preparedness and business continuity, including reports on exercises, training and testing undertaken by the organisation.

4.1.2 Will designate an Executive Director of the Board to be responsible for emergency preparedness on behalf of the organisation – the Accountable Emergency Officer.

4.1.3 Will ensure an appropriate level of priority is given to emergency management and business continuity in all strategic planning.

4.2 Accountable Emergency Officer (AEO)

4.2.1 The Accountable Emergency Officer has overall strategic responsibility for ensuring effective business continuity management within the ICB. The Accountable Emergency Officer will be consulted when analysing the Business Impact Analysis (BIA) results to determine priorities for protection and recovery. The Accountable Emergency Officer will take lead on promoting a culture of business continuity within the ICB.

4.3 Head of Emergency Preparedness Resilience & Response (EPRR)

4.3.1 Responsible for overseeing the implementation of the ICB business continuity management system, and for providing assurance of this system part of the EPRR core standards process. They will provide all necessary support and resources to the EPRR Manager and will ensure that the EPRR Manager is delivering on the agreed work programme. The Head of EPRR will also promote a culture of business continuity within the ICB.

4.4 EPRR Manager

4.4.1 The EPRR manager is responsible for the implementation of the ICB's business continuity management system. The EPRR Manager will provide advice and support to directors, managers and other appropriate stakeholders throughout the phases of the business continuity lifecycle. The EPRR Manager will ensure that a culture of business continuity awareness is embedded within the ICB. The EPRR Manager will act on behalf of the Head of EPRR to devise, implement, exercise, and review the business continuity management system, and provide assurance that the business continuity management system is implemented within the ICB. The EPRR Manager will also train individuals in their role within the BCMS.

The EPRR manager will review / audit all directorate business continuity plans and provide advice and guidance on their compliance with the business continuity programme / standards. An annual report on the outcomes of the audits will be presented by the Head of EPRR to Board.

4.5 Executive Directors / Directors of the ICB

4.5.1 Executive Directors / Directors will take leadership of their business continuity arrangements and are responsible for ensuring that their departments comply with this policy. They will follow the lead of the Accountable Emergency Officer in promoting a culture of business continuity within the ICB. The Executive Team will review the BCMS to ensure its continuing suitability, adequacy, and effectiveness.

4.6 Directorate Leads

4.6.1 Directorate Leads will take ownership of their departmental business continuity arrangements and are responsible for ensuring that they support process of regular review, training and exercising. Directorate Leads will engage with the EPRR Manager to improve organisational resilience. They will follow the lead of the Accountable Emergency Officer in promoting a culture of business continuity within the ICB.

4.7 All Employees

4.7.1 All employees of Lancashire and South Cumbria ICB are responsible for ensuring that they are aware of the business continuity arrangements and procedures relating to the activities they are regularly involved with. They will support and engage with the business continuity management process and actively promote a culture of business continuity with the ICB.

5   Governance

5.1   This policy applies to all ICB staff and should be observed by all staff from other organisations providing services on a contractual basis.

5.2   The Chief Executive Officer has overall responsibility for the ICB's business continuity activities.

5.3   The Accountable Emergency Officer will have delegated responsibility for ensuring that the ICB has robust arrangements in place for business continuity management and service recovery.

5.4   The Head of EPRR has responsibility for the day-to-day delivery and maintenance of the BCMS and will provide oversight, scrutiny, and assurance to the ICB Board.

5.5   All Senior Managers are responsible for the execution of this policy within their teams and for the development, review and exercising of their business continuity plans.

5.6   The EPRR Team will undertake an annual internal audit to review business continuity plans and an external audit is recommended every three years. A process is in place to assess the effectiveness of the BCMS and take corrective action to ensure continual improvement to the BCMS.

5.7   The business continuity policy will be reviewed annually and be signed off by the ICB Executive Board.

5.8   The ICB business impact analysis will be reviewed at least annually or whenever significant changes to key internal processes, location or technology occur or whenever significant changes to the external operating environment occur, system or regulatory change occurs or in the event of the deployment of the business continuity plan.

5.9   The business continuity plan will detail how the ICB will respond, recover and manage its services during disruptions and will be tested (exercised) and reviewed on a yearly basis as a minimum, following organisational change or as a result of learning from other business continuity incidents.

5.10   The policy will be circulated to the relevant people holding responsibility for BCM / BCP through email, cascade and publication on the ICB intranet.

5.11   Reports on compliance (Section 8) and the outcome of any exercises, and status of any corrective action will be annually reported to the board.

6 Process

6.1 Directorate Business Continuity Arrangements

6.1.1 The ICB will ensure that business continuity arrangements are in place for all its functions. The EPRR team will provide full guidance and support as required to maintain and updates these arrangements. The ICB business continuity plan template must be completed by all functions of the ICB. The template will take the functional lead through the process, including identification of critical business activities, a business impact analysis, resource requirements, strategies for restoration of critical business activities, roles and responsibilities and escalation processes.

6.1.2 Directorate Business Impact Analysis must consider key risks, including potential loss of people, information and data, premises, suppliers and contractors and IT and infrastructure. Functional Leads should also consider other risks unique to their services and activities when developing their business continuity arrangements. Where appropriate, these risks should be highlighted on the organisational risk register.

6.1.3 Directorate business continuity arrangements must cover all activities identified as critical to the ICB. The arrangements should however cover all activities undertaken by the function.

6.1.4 The organisation has in place a system to assess the business continuity plans of commissioned providers or suppliers; and are assured that these providers business continuity arrangements align and are interoperable with their own.

6.1.5 Completed Business Impact Analysis should be signed off through directorate governance processes and forwarded to the EPRR Manager for review and assessment.

6.1.6 Once reviewed and any necessary changes suggested, the plans should be signed off and made available in hard copies to all staff at all work locations.

6.1.7 Final business continuity plans must be sent to the EPRR Manager(s) for review / audit and publication on the ICB Intranet site.

6.1.8 All business continuity plans will be tested on a yearly basis as a minimum, following organisational change or because of learning from other business continuity incidents.

6.1.9 Following any business continuity incident, a debrief will take place to identify best practice and continual improvement.

6.2   Information Management and Technology Disaster Recovery

6.2.1   The ICB's Information Management and Technology (IM&T) providers will develop an IT disaster recovery plan, which will compliment departmental business continuity arrangements. The IM&T disaster recovery plan will detail computer and communication systems that have been identified as critical. Each of these systems will be given a recovery time objective.

6.2.2   The results of the Business Impact Analysis will be used to support future versions of the IM&T disaster recovery plan, by indicating which services the ICB agrees are critical and how quickly these services need to be recovered. IM&T are only responsible for their own business continuity arrangements, and for recovering systems in the event of a disruption or failure.

6.2.3   The Information Technology department(s) and Information Governance Team will be responsible for certifying that the ICB is compliant with the Data Protection and Security Toolkit on an annual basis.

6.3   Logging and Document Management

6.3.1   All incidents resulting in an adverse impact to the ICB's services must be appropriately documented.

6.3.2   Managers responsible for maintaining or recovering a service during a disruptive event must ensure that their decisions are recorded.

6.3.3   The ICB has a dedicated cohort of trained loggists who can support the tactical and strategic on call manager during the response to an incident. All on call managers have received training on how to work with their loggist, and the process for signing off logs.

6.3.4   All documents produced by the ICB related to business continuity management, and those in relation to a disruptive event, must be marked 'OFFICIAL – SENSITIVE' and as such be stored, handled, and processed appropriately.

6.3.5   All documents relating to a business continuity incident / disruptive event must be submitted to the EPRR department for audit and storage.

6.3.6   These documents will be retained in line with the records retention policy (LSCICB Corp 19 Information Governance & Data Security and Protection Policies)

6.3.7   Documents relating to business continuity management, and in particular those relating to a disruptive event, must not be released to any third party without consultation with the ICB's Accountable Emergency Officer and/or Information Governance Manager.

6.4 Risk Management

6.4.1 The EPRR team will support with the identification of risks relating to emergency planning and business continuity and the AEO will have oversight of these risks.

6.4.2 Risk assessments will be undertaken in line with the Risk Management Policy (LSCICB Corp12), with due consideration for the national and community risks registers.

6.4.3 Risks mitigation and risk escalation will also be undertaken in line with the guidance in the Policy.

6.4.4 EPRR related risks will be reviewed by the EPRR team a minimum of every 6 months and will be escalated to the risk management team as appropriate for inclusion on the corporate risk register

7 Training and Exercising

7.1 The ICB has a duty under the Civil Contingencies Act 2004 (CCA) to have appropriately trained staff and to test EPRR arrangements regularly.

7.2 It is important that staff fully understand the need for Business Continuity Management, as well as their role in response to any invocation.

7.3 To fulfil this obligation the ICB will:

- Develop and deliver an initial training programme which meets the needs of the business continuity requirements for the ICB.

- Develop and maintain an ICB Business Continuity Plan.

- Make all Business Continuity Management Policies and Plans available on the intranet for all staff to view.

- Ensure that the lessons learned from exercises are implemented throughout the organisation to ensure continuous improvement to the BCMS

- Drive improvements in planning and raise the standard of business continuity preparedness through the **Plan, Do, Check, Act** cycle:

8 Compliance

8.1 The following records must be retained and maintained to comply with this policy.

Record	Duration/Validity	Location	Responsibility
BCM Policy	Annual review	Soft copies to be retained on Sharepoint / intranet

Hard copies to be available / distributed across the business functions as necessary

Version control will be maintained | AEO.

Supported by the ICB EPRR team. |
Business Impact Analysis	Annual review or when business unit changes dictate or a major incident occurs		
Physical Risk Assessment	Annual review or when business unit changes dictate or a major incident occurs		
Business Continuity Plan	Annual review		
Incident Response Plan			
Exercise Reports			
Training Materials	Annual review		
Third Party Support Contracts	To be reviewed in line with BC plans and/or on contract renewal	Retained by Contracting.	Contracting

9 Associated Guidance

9.1 The ICB's business continuity policy and plans will be based on the following standards:

- NHS England Core Standards for EPRR.
- NHS EPRR Framework 2022
- ISO 22301- Business Continuity Management Systems - Requirements.
- ISO 22313-Business Continuity Management Systems – Guidance on the use of ISO 22301
- ISO / PAS 22399: 2007 - Guideline for Incident Preparedness and Operational Continuity Management.
- PAS 2015 - provides a resilience framework for NHS organisations and all providers of NHS funded care. PAS 2015 brings together the different strands of resilience planning within the NHS to create a framework that supports organisations efforts to become more resilient
- Business Continuity Institute (BCI) Good Practice Guidelines 2018
- NHS Business Continuity Framework
- Data Protection and Security Toolkit (DPST) – NHS England

10   Consultation

This policy was distributed for consultation to internal stakeholders as follows:

Date Policy Circulated	Name of Individual or Group	Were Comments Received?	Were Comments incorporated into Policy?	If no, why not?
29/4/2024	AEO	No	NA	NA
02/05/2024	Executive Team	Yes	Yes	NA

Appendix 1 – Business Impact Analysis

Front sheet

NHS Business Impact Analysis Template

Template Overview

This template is designed to assist the NHS in England in developing Business Continuity Plans.

Under each tab 'Activity' 'Premises' etc there are red flags located in some of the fields. If you place your curser over these fields, you will see a text commentary box appear, which specifices what is required from each field.

There are 6 activity tabs. Should you wish to add any additional tabs then link the new activity back to the template overview.

Any boxes shaded grey require population.

This template has been adoped by NHS LSC ICB to meet with the NHS core standards for Emergency Preparedness, Reslience and Response (EPRR).

| Activity (1) |
| Activity (2) |
| Activity (3) |
| Activity (4) |
| Activity (5) |
| Activity (6) |
| Premises (BAU) |
| Staff Requirements |
| Activity interactions |
| Data Processes |
| Further guidance |

NHS Lancashire and South Cumbria Integrated Care Board
Emergency Preparedness, Resilience and Response (EPRR)

To add additional activities to the BIA:
1. Right click on a blank activity tab below
2. Select Move or Copy...
3. Highlight staff requirements in the 'before sheet' box
4. Ensure that the create a copy box is checked
5. Click ok.

Cell 'B4' on the new activity sheet will also need to be updated to match the new activity number.

BIA Version:	1
Directorate	
Team/Service	
Name of Author:	
Job Title:	
Contact Details:	
Date of Completion:	
Business Continuity Lead:	
Name & Location of Team:	

Activity

FRONT SHEET

| Activity Reference Number |
| 1 |

Activity Description

Name of Activity:

Description of activity:

Operational Tasks:

Impact Scoring Grid

Impact Scoring Key

1 = **Negligible** - Unlikely to have any impact
2 = **Low** - May have an impact
3 = **Medium** - Likely to have an impact
4 = **High** - Highly probable it will have a significant impact
5 = **Very High** - Will have a major impact

Length of disruption	Category of Impacts (please refer to descriptors in the instructions)								
	Financial	Service delivery	Reputation	Wellbeing, Health & safety	Information security	Statutory / regulatory duty	Business / work plan objective	Impact Score	RAG
0 - 24 hrs									0.0
24 hrs. > 7 days									0.0
7 days +									0.0

Process Frequency (Daily, Weekly, Monthly, Quarterly, Annually, Seasonal, Irregular)

Is this activity Documented? Yes/No

Recovery Time Objective (RTO)	Maximum Tolerable Period of Disruption (MTPoD)

RAG Rating Score

Less than 4.9 is GREEN			Between 5 and 9.9 is AMBER			Over 10 is RED		
RTO	MTPOD	RPO	RTO	MTPOD	RPO	RTO	MTPOD	RPO
7 Days+	7 Days+	7 Days+	1 Day	>7 Days	>7 Days	0 Hours	>24 Hours	>24 Hours

Activity RAG rating

Non-Urgent

Premises (BAU)

FRONT SHEET	**Premises Requirements**

Activity 1 - Premises Requirements

		Considerations
0 - 24 hrs.		Many disruptions can lead to a loss of site/premises access. You must consider having arrangements in place to move to a temporary site/premises during this disruption.
24 hrs. > 7 days		- Agile working - Hotdesks - Workspace requirements - Meeting rooms - Confidential areas - Secure storage - Video conferencing facilities
7 days +		Define existing work area, indicate where you might relocate to if available List relevant estate Provider(s) along with in hours and out of hours contact details.

Activity 2 - Premises Requirements

0 - 24 hrs.	
24 hrs. > 7 days	
7 days +	

Staff requirements

FRONT SHEET	**Staff Requirements**

Activity 1 — Staff Requirements

Length of disruption	Minimum number of staff required	Regular number of staff required	Role Requirements (skills, knowledge & experience)	Key Contacts (Name / Tel / E-mail)		Considerations
				Activity Lead	**Deputy**	Staff play a key role in recovering from a major disruption. Aside from a duty of care to staff, if you cater for your staffs' needs, then they can concentrate on business functions.
0 - 24 hrs						Single Points of Failure is a member of staff who, because of qualification or experience is the only person in the organisation who can deiiver their function - it is important to identify these people in this section of the BIA process.
24 hrs. > 7 days						Some services depend on specific skill sets. List only those essential to maintain service delivery.
7 days +						Some staff may be redeployable to support a higher class of activity.
						Does a contact list exist? Where is it?

SINGLE POINTS OF FAILURE

Location	Record job titles of Single Points of Failure below. A Single Point of Failure is a member of staff who, because of either qualification or experience, is the only person in the organisation who can deliver their function. **Single Point of Failure**	Record job titles of Single Points of Failure below. A Single Point of Failure is a member of staff who, because of either qualification or experience, is the only person in the organisation who can deliver their function. **Single Point of Failure**

Activity interactions

FRONT SHEET	Activity Interactions	

You rely upon	**Rely upon you**	**Considerations**

Internal Stakeholders

List Internal services which your activities rely upon ie HR/IT/Procurement etc

Service	Contact Details

External Stakeholder

List External stakeholders which your activities rely upon ie IT suppliers etc

Stakeholder	Contact Details

Internal Stakeholders

List Internal services which rely upon your activities IT suppliers etc

Service	Contact Details

External Stakeholder

List External stakeholders which rely upon your activities ie IT suppliers etc

Stakeholder	Contact Details

Considerations

The ICB needs to prove that they can operate in all circumstances. Some departments may wish to undergo further audits of their business continuity management system and reliance on internal and external stakeholders.

In tougher times, reliance on a single critical provider can be a greater risk. Even in good times understanding how you would recover from disruption and where you feature in your provider's priorities is important.

e.g. HR, IT, catering, communications etc

Data processes

FRONT SHEET	Data Processes	

Where is the data or files needed to support this process held? Mark appropriate column/s with an "x"

Activity Reference Number	Local Device(C Drive)	Cloud(O365)	ICB Hosted Server	3rd Party Hosted Server	Are there work arounds or manual procedures that could be used during an IT outage? Y/N. If yes please briefly describe process and where it is documented
1					
2					
3					
4					
5					
6					

Alternative systems and specialist ICT requirements/equipment – additional information

Considerations

The failure of IT and telecommunication systems is one of the most frequent disruptions that the NHS could experience.

Critical information needs to be backed up and accessible.

As an organisation we (the ICB) to to understand where all of our data is held.

Define your business-critical software applications.

Define how a loss of software or a general IT failure would affect your service. Indicate how your service would operate pending its restoration.

Define your business-critical communication systems/hardware (mobile phones), including those which are patient and none patient facing.

Define how a loss of communication failure would affect your service. Indicate how your service would operate pending its restoration, and alternative ways of working that may be required.

Appendix 2 – Definitions

The following definitions apply to the terms used in this document in accordance with ISO22301 the international standard for Business Continuity.

Business Continuity Management System - '*A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which builds a framework for building organisation resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating assets.*

Business Impact Analysis - '*The process of analysing activities and the effect that a business disruption may have upon them*'

Prioritised Activities - '*Those activities to which priority must be given following an incident in order to mitigate impacts*'

Key Products/Services - '*Beneficial outcomes provided by an organization to its customers, recipients and interested parties*'

Maximum Tolerable Period of Disruption (MTPOD) - '*The 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 Time Objective (RTO) - '*The period of time following an incident within which a product or an activity must be resumed, or resources must be recovered*'

Recovery Point Objective (RPO) - '*The point to which information used by an activity must be restored to enable the activity to operate on resumption, also referred to as Maximum Data Loss*' *(Detailed on the AGEMCSU Disaster Recovery Plan)*

Business Continuity Plans (BCP) - '*Documented procedures that guide organizations to respond, recover, resume and restore to a predefined level of operation following disruption*'