www.happyhealthylives.uk

NHS
Coventry and
Warwickshire
Integrated Care Board

Business Continuity Management System Policy

2023

Reference Number:	
Version:	1
Name of responsible Committee and date approved or recommended to Governing Body:	Audit Committee
Date approved by Governing Body (if applicable):	
Next Review Date:	
Expiry Date:	
Name of author and title:	Sabin Bran-C – interim Head of EPRR
Name of reviewer and title:	Rachel Danter, Chief Transformation Officer and Accountable Emergency Officer
Department:	Transformation & People Directorate, Emergency Preparedness, Resilience and Response (EPRR) Department

VERSION HISTORY

Date	**Version**	**Changes made to previous version**	**Engaging and Endorsing Stakeholders, Committees / Meetings / Forums etc.**
12.08.2023	1	N/A	Chief Transformation Officer, Director of Transformation, Information Governance Team, Finance and Procurement Team, Communications Team, Finance Team, SIRO and IT Team, Audit Committee

Contents

1. Introduction

The NHS needs to be able to plan for and respond to a wide range of incidents and emergencies that could affect health or patient care. Additionally, the NHS needs to be able to continue to deliver its services in the face of disruptive incident. The purpose of this Policy is to outline the Coventry and Warwickshire Integrated Care Board's (CWICB) Business Continuity Management (BCM) Strategy.

This document describes how CWICB will meet the requirements of EPRR obligations set out in the Civil Contingencies Act (CCA) 2004 and the NHS Act 2006 (as amended by Health and Social Care Act 2012 and Health and Care Act 2022) alongside applicable NHS England EPRR Guidance.

The ICBs Business Continuity Management Strategy provides the methodology by which the organisation establishes and maintains a comprehensive Business Continuity Management System (BCMS) that is align to ISO 22301, PAS 2015 the NHSE Business Continuity Management guidance. The policy also defines the guiding principles, which the organisation follows and measures its performance against.

This document should be read in conjunction with the ICBs incident response and business continuity plan, and other EPRR related guidance and plans, which detail the operational response to be implemented by the ICB to any incident.

2. Strategic Context; Statutory, Regulatory and Contractual requirements

ICBs are defined as category 1 responders under the Civil Contingencies Act (2004). This means they are at the core of the response to most emergencies. Category 1 responders are subject to the full set of civil protection duties as listed below.

- Assess the risk of emergencies occurring and use this to inform contingency planning
- Put in place emergency plans
- Put in place business continuity management arrangements
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency
- Share information with other local responders to enhance co-ordination
- Co-operate with other local responders to enhance co-ordination and efficiency.

To ensure that the ICB is carrying out its statutory duties under the Civil Contingencies Act 2004 it must put in place plans to ensure its service delivery continue to operate during any emergency, as defined by the Act, that impacts on the Category 1 responder.

The Care Quality Commission also requires Business Continuity arrangements to be put in place, and Contractual duties requirement under contract with the Commissioner to ensure the ICB can maintain services during any disruption with minimal disruption to services.

The ICBs EPRR programme will adhere to the underpinning principles set by the NHS EPRR Framework 2022:

- Preparedness and anticipation
- Continuity
- Subsidiarity
- Communication
- Cooperation and integration
- Direction

The minimum requirements that commissioners and NHS-funded organisations must meet are set out in the current NHS EPRR Core Standards. This is achieved through the collaborative production of plans for incident response, business continuity and recover in accordance with guidance. Key services that must be maintained under the aforementioned requirements include:

Coventry and Warwickshire ICB Directorates and Associated Services

The CWICB Organisational Chart categorises the services provided by the organisation and categorises then into the core directorates responsible for their delivery.

Interest of Stakeholders

Where possible the business continuity plans of the ICB have taken into account the interests and requirements of key stakeholders and been developed in partnership with these where necessary. Key stake holders include, but are not limited to:

- University Hospital Coventry and Warwickshire NHS Trust
- Coventry and Warwickshire Partnership NHS Trust
- South Warwickshire University NHS Foundation Trust
- George Elliot Hospital NHS Trust
- West Midlands Ambulance Service University NHS Foundation Trust
- Warwickshire County Council (Warwickshire Local Resilience Forum)
- West Midlands Conurbation (West Midlands Conurbation Local Resilience Forum)
- NHS England (Midlands)
- The Department of Health and Social Care

Under the Data Protection Act (2000) the organisation is a legally accountable ‘data controller’ and will ensure there are appropriate safeguards in place to protect sensitive and personal data as part of on-going business practices, and ensure this data is protected and recoverable in a Business Continuity scenario. It is therefore a requirement that Disaster Recovery Plans are in place and maintained relating to the technical infrastructure, assets and systems the organisation is responsible for. Overall responsibility for this area rests with the Senior Information Risk Owner (SIRO).

3. Aim and objectives

The aim of this strategy is to support the ICB in anticipating business continuity risks for the purpose of mitigating them and having robust plans in place to minimise the impact of such events that causes major disruption to the ICB’s normal service delivery.

The objectives of this strategy are to:

- Identify and develop preventative measures to reduce the risk of a business continuity disruption occurring
- Ensure the ICB can identify and continue to deliver its critical functions during an incident, ensuring that statutory requirements are maintained
- Ensure appropriate management oversight of the business continuity programme
- Set standards for the development of business continuity plans

4. Policy Statement

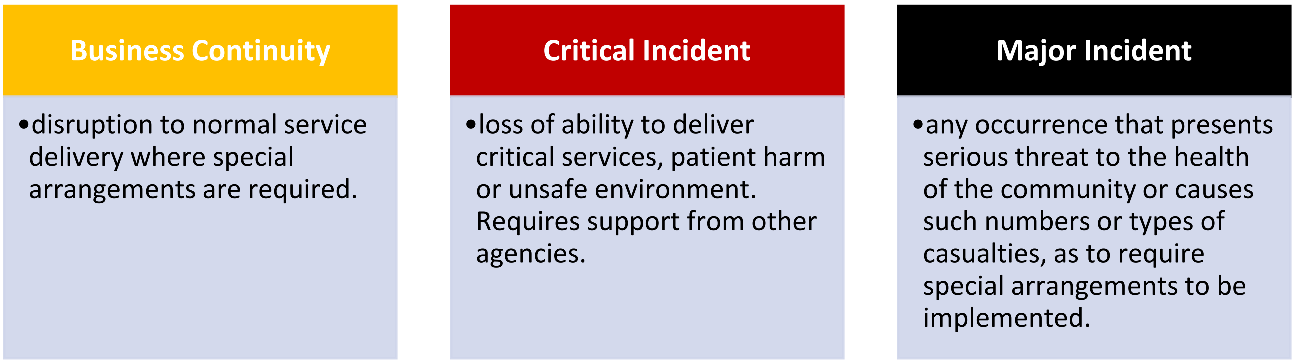
The Business Continuity Management approach for Coventry and Warwickshire Integrated Care Board (CWICB) will align to the CWICB EPRR Policy, NHSE BCM guidance, ISO 22301, Business Continuity Institute Good Practice Guidelines and legal requirements. The CWICB accepts and abides by their statutory duties as a Category 1 responder under the Civil Contingencies Act 2004 (CCA).

This Policy represent the overarching document that establishes the Business Continuity Management programme for the Coventry and Warwickshire Integrated Care Board, provides the strategic direction from which the programme is delivered, defines the way in which the organisation will approach business continuity, and how the programme will be structured and resources.

This policy is intended to be used in conjunction with the overarching Emergency Preparedness, Resilience and Response (EPRR) Policy. The CWICBs Business Continuity Management System aligns with the organisation’s strategy and objectives.

5. NHS Incident Classification

The NHS defines three incident categories depending on the nature and impact of the event.



Business Continuity

- disruption to normal service delivery where special arrangements are required.

Critical Incident

- loss of ability to deliver critical services, patient harm or unsafe environment. Requires support from other agencies.

Major Incident

- any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented.

Figure 1 NHS Incident Classification

Business Continuity Incident

A business continuity incident is an event or occurrence that disrupts, or might disrupt, an organisation's normal service delivery, below acceptable predefined levels, where special arrangements are required to be implemented until services can return to an acceptable level.

6. Roles and responsibilities

The roles and responsibilities associated with the successful implementation and management of the ICB's BCMS are described below. The ICB will ensure that all staff have access to relevant resources for the management and creation of plans and exercises to support the BCM programme.

6.1. Accountable Emergency Officer (AEO)

Appointed by the Chief Executive to be responsible for the overall management of the BCMS and establish the strategic direction of the ICB with regard to business continuity. This role is currently undertaken by the Chief Transformation Officer. They will also act as the Lead Director for Business Continuity Management and will oversee the process and implementation of the BCMS whilst providing the strategic leadership surrounding Business Continuity. In line with the NHS Core Standards, they are also responsible to ensure "that their organisation, any providers they commission, and any subcontractors have robust business continuity planning arrangements in place which are aligned to ISO22301".

6.2. Information Governance Lead

In line with Information Governance Toolkit requirements, the ICB's Information Governance Lead should 'ensure that a business continuity strategy is in place for all critical information assets and critical processes, including those provided under service contract or agreement by third parties.'

6.3. Senior Information Risk Owner (SIRO)

The SIRO is accountable and responsible for information risk across the organisation. The responsibilities of the SIRO aligned to Business Continuity Management will cover areas such as:

- Identifying and assigning Recovery Classes to technical assets
- Arranging off-site support and recovery
- Security of critical & vital electronic records
- Recovery of critical & vital systems, assets & infrastructure

6.4. Procurement Team

The team must ensure that all parties providing goods and services to the ICB's critical services provide assurance to the organisation that they can continue delivery in the face of disruption in line with ISO 22301.

6.5. Emergency Planning Team

The Emergency Planning team will develop and update templates and exercises to ensure that the ICB is using the most up to date documents. The team will maintain an Organisational Business Continuity plan and centrally monitor compliance with business Continuity across the ICB, including validity and version control of the plans. The team will work to compile the results of the Business Impact Analysis (BIA) and assist the completion of local Business Continuity Plans. They will also carry out annual audits to ensure that the ICB is up to date with their requirements, and that plans are reflected upon and updated following activation of the plans or at the planned review stage, whichever comes first. The Emergency Planning team will ensure that appropriate training, in line with the ICB's Training Needs Analysis and supporting material is available for the development of local Business Continuity Arrangements.

6.6. Directorate Leads

Directors Leads will ensure that all services that they are responsible for are sufficiently covered within a Business Continuity Plan. They are responsible for ensuring that risks on a local and corporate level are appropriately reported, addressed or accepted on the required risk registers. The Director/ Department lead will be responsible with ensuring that a Business Continuity Lead has been identified for their Directorate.

6.7. Directorate Business Continuity Lead

The Directorate Business Continuity Lead (DBCL) will be assigned this role by their Directorate's Officer / Department lead. The DBCL will be responsible with overseeing all Business Continuity related activity for their respective Directorate and report into the Director/ Department Lead on BC related activity and progress.

Other responsibilities include:

- Act as the single point of contact for the Emergency Planning Team in relation to Business Continuity
- Oversee the progress of Business Continuity planning for the Directorate in conjunction with the Emergency Planning Team
- Conduct a yearly audit on the directorate's business continuity arrangements, supported by the Emergency Planning Team
- Support and enable the Team/ Department Managers to complete the required Business Continuity Plans and associated BIAs

6.8. Team / Department Managers:

Service heads and managers are required to complete the required business continuity plans, including their BIA, and work to develop resilience within their local area and overseen by the Directorate's Business Continuity Lead.

This will be achieved by ensuring:

- Effective plans are in place to respond to a range specific departmental type incident
- Considerations are made based on the agreed criticality of Departmental processes
- Staff are made aware of their actions, during incidents, both on and offsite
- Arrangements are made to ensure the continuation of critical Departmental processes
- The Director is consulted as necessary when processes are either reduced or stopped altogether

6.9. All staff

All staff are required to ensure that any risks and disruptions are immediately highlighted to their line manager. Staff are required to follow any emergency instructions that are given to them in the event of an incident to maintain the safety of themselves, other staff members, visitors and any potential patients. Staff are required to familiarise themselves with Business Continuity arrangements and the escalation protocol.

7. Integrated Care Board Business Continuity Management System

7.1. Business Continuity Management Approach

The BCM System is an ongoing process, which adapts in response to the changing nature, of an organisations internal and external operating environment. The CWICB adopt a holistic management process that identifies potential threats and the impacts of those threats to business operations. A business continuity system is put into place, to implement the business continuity policy. A vital part of the programme is the ability to manage documentation to aid the implementation, where appropriate.

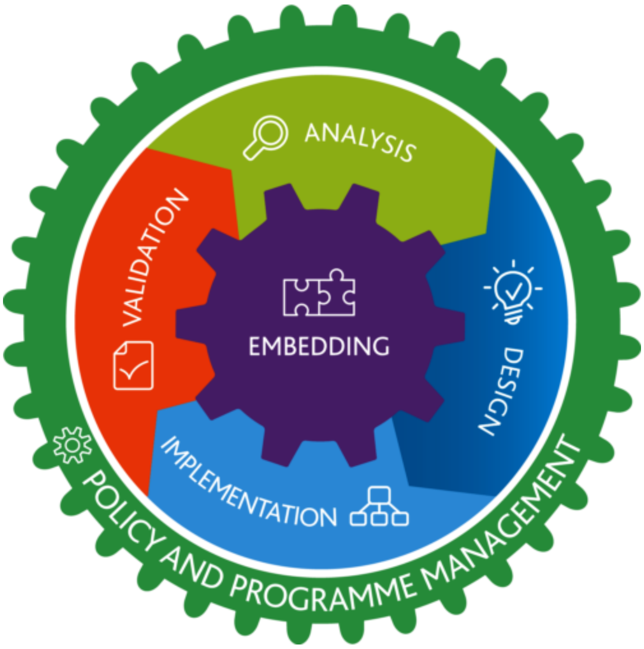


Figure 2 - Business Continuity Planning Cycle

The Business Continuity Institute's six professional practices that form the Business Continuity Planning Cycle, depicted in Figure 2, represent the activities the organisation will follow in implementing the BCM System for the CWICB.

The practices are aligned to the ISO 22301 Plan, Do, Check, Act (PDCA) Model, presented in Figure 3. The International Standard applies this methodology to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the effectiveness of an organization's BCMS.

The first step is to Analyse what the Critical Activities are for an area. These are the critical functions within an area that must continue and/or be recovered as quickly and as effectively as possible.

The second step is to Design a BC Plan which outlines the aforementioned activities, what they require in order to continue, how they link in with other internal teams and external stakeholders, and what alternatives there are if these activities suffer disruption.

The third step is to Implement the BC Plan. This involves agreeing the BC Plan with key staff members and stakeholders and actively working to embed the plan and its guidance into team culture, understanding and training.

The fourth step is to Validate the BC plan, which is a cyclic, ongoing element. BC Plans are required to be reviewed and tested every 12 months. Key staff from the team take part in a scenario-based exercise at least every 12 months to test the BC plan 'in action' and ensure that it is up-to-date and fit for purpose.

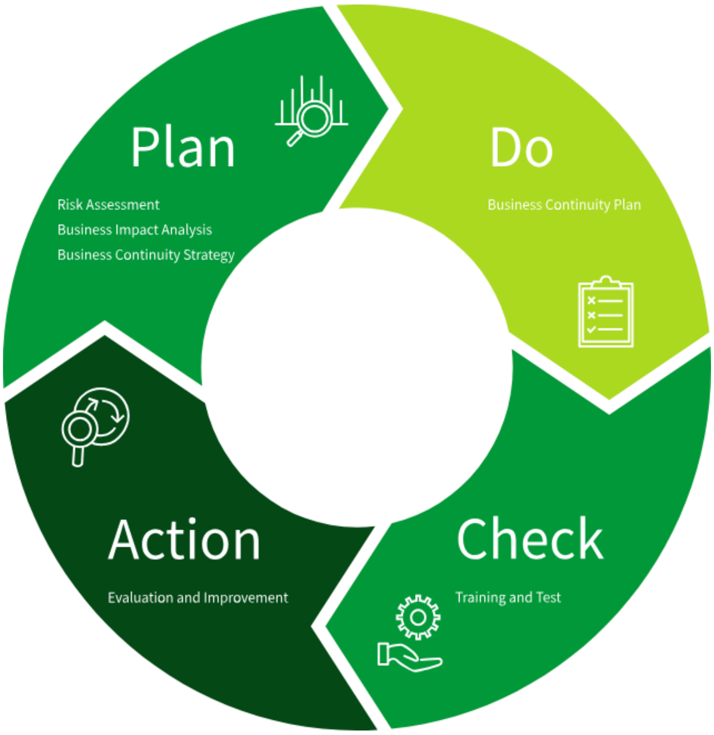


Figure 3 - PDCA Model of ISO22301

8. Analysis

8.1. Risk Assessment

The duty to carry out a risk assessment of an emergency occurring within the geographical area of Coventry and Warwickshire ICB is carried out at Coventry and Warwickshire, and West Midlands Conurbation Local Resilience Forums. The identified risks are then documented on the local Risk Register and fed to the Local Health Resilience Partnership for a review of impacts on the health system. Once these risks have been identified, the Emergency Planning team work to ensure that the relevant risks are also on the ICB Risk Register. Additionally, internal risk assessments are conducted in line with the ICB Risk Policy.

8.1.1. Documenting and Managing Risk

All identified risks will be added to local and the corporate Risk Register as required. Oversight of this Risk Register is maintained by the ICBs risk team and falls outside of the document control of the BCMS. Responsibility for updating of the corporate risk register sits with the relevant risk owner. Local service leads are responsible for identifying and managing risk locally.

The risk management process is further detailed and included in the ICBs EPRR Policy and Risk Policy.

8.1.2. Acceptable Risk

The level of acceptable risk addressed in this document is defined as:

Acceptable risks are those risks which have been identified and measured according to the risk grading tool and for which risk mitigation action plans have been developed. Such risks are deemed to be acceptable depending on the nature and grade of the risk. Acceptable risks should be monitored, reviewed and entered onto the appropriate risk register. Risks will be reported in line with ICB EPRR policy and ICB Risk Policy.

8.2. Business Impact Analysis (BIA)

For the ICB to meet its overall Strategic Objectives, it depends on the uninterrupted running of all its products and services. Each of the services provided by the ICB is important, however during a major disruption it will be extremely difficult or almost impossible to maintain a normal level of service delivery.

The BIA is the first stage of the BCP development process where services will be required to consider what the impact would be on both its own service, and its stakeholders if the delivery of a key function or service would be disrupted for any reason. The BIA process should be part of a yearly review cycle conducted by the plan owner and can be supported by the Emergency Planning Team. BIA information will be collated by the Emergency Planning Team and processed to assist in ICB wide planning and for audit purposes.

For the purposes of the BIA the cause of the disruption is considered on the basis of loss of, People, Premises, Processes (including ICT, electronic systems etc) and Partners. Where a risk identified via the local risk assessment or the local Risk Register poses a threat to People, Premises, Processes (including ICT, electronic systems etc) and Partners, the Business Continuity Plan of the affected Directorate will be updated to reflect this.

8.2.1. Business Impact Assessment Method

The BIA template in the form of a questionnaire will be emailed out to the Plan Owner for completion with the offer of support from the Emergency Planning Team. Additionally, a workshop/ team meeting can be used to facilitate the completion of the BIA.

The BIA information collected will include the identification of all products and service, processes, and activities. Once collated, the BIA will then be used to assess the impact of any disruption affecting the below criteria over a period of 0-24 hours, 24 hours – 7 days, or 1 week and longer.

The six criteria applied to measure the impact of a disruption to a service are as follows:

- Safety of patients, staff or public
- Statutory/ regulatory duty
- Adverse publicity / reputation
- Finance, including claims
- Service /business interruption / environ impact
- Information Security

A scoring system on a scale from 1 – 5, with 1 representing a negligible risk and 5 representing a risk with the potential to have a major impact, will be used. The score sum will then rate the activity as being: Critical (sum score > 9.9); Urgent (sum score > 4.9); or Non-urgent (sum score < 5).

The level of required service is established for set time frames and the links to the other areas of the ICB and key suppliers identified. Information on this is then used to inform planning on the business continuity plan and identify resources across the ICB suitable for potential redeployment.

Following the impact assessment, each of the activities, depending on their final rating, will be assigned a:

- Recovery Time Objective (RTO)
- Maximum Tolerable Period of Disruption (MTPOD)
- Recovery Point Objective (RPO)

It is recommended that the following RTO, MTPOD, and RPO timeframe limits are applied against each activity aligned to their rating. These timeframes are indicative and serve only as a suggestion. Depending on the nature of the activity, the timeframes can be amended where deemed necessary by the Plan Owner.

Rating	**RTO** (< MTPOD)	**MTPOD**	**RPO**
Critical	0	<24h	<24h
Urgent	1 Day	<7 Days	<7 Days
Non-urgent	7 Days+	7 Days+	7 Days+

Services with the shortest Maximum Tolerable Period of Disruption (MTPOD) are deemed as highest priority therefore must be Resumed or Recovered as soon as possible following a disruption.

8.2.2. Data collection

Responding effectively to a Business Continuity incident/s is underpinned by a sound understanding of the business and the services it provides. This understanding is achieved though the collection and analysis of data, including:

1. Activities conducted as part of normal business operations at service level
2. What the priorities of the service/ directorate are
3. What is required to deliver these priorities
    - Staff numbers
        - Including the current work placement requirements of staff (i.e Home working)
    - Equipment
    - Premises

*Staff home working should not affect the running processes of the Business; therefore, home working is not an impact for analysis.

8.2.3. Use of BIA information

The outcome of the BIA provides an overview of the critical services delivered within the ICB. The information gained from the BIA will likely allow for the team to identify interlinks between services, including any dependencies that impact on the recovery time of services.

9. Design

9.1. Business Continuity Plans

9.1.1. Business Continuity Management Planning Overview

Developing BCM Plans enables staff and managers to prepare and respond more effectively to incidents. The continuation of services can be affected by any number of incidents that may differ in terms of size, scope, cause, and effect.

To respond to this, the CWICB operates three levels of planning which are undertaken on a regular basis:

- Team / Departmental Planning
- Directorate Planning
- CWICB Strategic Planning

Business Continuity Plans will be put in place at organisational level, directorate level, and where required team / service level for complex services that required specialised planning at a more granular level than their directorate's plan.

Each Directorate should have a nominated Business Continuity Lead to champion business continuity planning within their respective directorate. These individuals will also be the Plan Owners for their respective Directorates.

9.1.2. Minimum standard for plans

Plans will contain the following:

- Escalation and Activation method including management of the incident
- Communication methods and channels
- List of services and their criticality (achieved though BIA)
- Resources required and actions to ensure that services can be maintained (achieved though BIA)
- Actions for the response to disruption to staff numbers, premises, suppliers, IT services, specialist equipment and data (where applicable)
- Specific roles required to respond
- Internal and external interdependencies (achieved though BIA)
- Decision support checklists
- Details of meeting locations
- Links to other plans and procedures
- Version control

9.1.3. Directorate & Team / Service Business Continuity Plans

Team / Service Business Continuity arrangements are included in their respective Directorate Plan to which the Team / Service belongs. In addition to the aforementioned items, these plans will include localised information such as:

- Staff contact details (accessed via ESR with support from CSU – including CSU OOH team)
- Team estate locations and contact details for relevant line manager if remote working is utilised.
- Business Impact Assessment to support decision making on service prioritisation during an incident.
- Annual Action plans to improve team/departmental resilience.

9.1.4. Plan Updating, Monitoring and Review

Plans will be updated, monitored and reviewed in line with the EPRR policy. This means at least once a year, once exercised or tested via incident response or once updated legislation or guidance published; whichever comes soonest. Plans are also required to be reviewed following activation of the plans to ensure that any learning can be reflected in the updated plans. Plan owners are responsible for their maintenance and upkeep. Historical documents will be identified and archived in the EPRR team's central repository.

Procedural and technical issues that are of an internal departmental nature should be addressed to the DBCL for subsequent changes in Directorate Business Continuity Plans and the Organisation's Business Continuity Plan if appropriate. It will be necessary to then review the current plans and implement any changes in management methods or training needs identified.

Version control

Any plan or documentation related to BC will be subject to strict version control. This includes a version number, issue date and the date of next planned review date. This will be centrally monitored by the Emergency Planning Team. See Appendix C for Mandatory Business Continuity Plan Document Control.

9.1.5. Plan Retention and Storage

Plans are to be held by the Plan Owner, and a copy of the plan will be shared with the Emergency Planning Team. An electronic copy of all plans will be kept on the Emergency Preparedness, Resilience and Response page on SharePoint, ensuring that a history of all plan versions is stored virtually for a minimum of 10 years. A hard copy of every Business Continuity Plan and Organisational BIA will be held by the Emergency Planning Team in the Incident Response Box found in the System Coordination Centre of Westgate House, Warwick, CV34 4DE.

9.1.6. Plan Dissemination

Once approved, this plan will be circulated to appropriate members of staff via email and will be referenced in local training.

9.1.7. Planning Assumptions

The following assumptions should be considered when developing Business Continuity Plans:

- In the event of a major incident, existing business premises could, potentially, be out of use for up to 5-7 days, possibly months in the event of floods or fire related incidents
- In recovery from the 2020 Covid Pandemic, workplace guidance for home-based working is in place.
- In the event of a less significant disruption some of the existing premises would remain in use alongside remote working preferences.
- Where a generator is not available loss of electricity supply across a region could last for up to 1-5 days.
- The mains water supplies and sewerage services may be interrupted for up to 3-5 days.
- Availability of the IT network historically runs at over 85%. In the event of a partial failure of a server the network could be unavailable for up to 12-24 hours.
- In the event of loss of IT connection during home working for 4 hrs or more, staff should make their line Manager aware and then attend one of the CWICB estate locations to complete essential work.
- If the server were to be completely lost it could take up to 1-3 days to restore a limited desktop service (Microsoft package, e-mail and Internet access). Other software could take even longer to restore.
- A cyber-attack carries the risk of a potential of significant data loss for considerable periods of time
- Availability of the internal telephone network historically runs at 100%. In the event of a failure there could be loss of service for up to 8-12 hours.
- Access to the public telephone network and mobile communications could be lost for up to 3 days during a Major Incident.
- In a pandemic 25% - 50% of staff could be off work at any one time. This will include those who are sick, those caring for others and the 'worried well' who are simply too scared to come to work. On average people will be absent for 5-7 days, but some may take longer to return.
- In a fuel crisis only, staff involved with delivering critical services, or on call, are likely but not guaranteed to have priority access to fuel.
- Consider short term and long term impacts in line with climate change adaption planning

10. Implementation and Validation

10.1. Training

10.1.1. Assessing training needs

Training of all staff will be conducted based on the CWICB's Training Needs Analysis which will outline the competencies required by different groups of staff involved Business Continuity planning. This will allow for training to be targeted in a proportional way, providing an appropriate level of knowledge to each employee.

The Emergency Planning Team is responsible for maintaining the Emergency Planning Training Needs Analysis, which as a minimum will cover the Accountable Emergency Officer, Emergency Planning Team, Directors, SIRO, and other key staff identified in a BCP.

10.1.2. Training delivery

Training delivery and frequency will be determined by the need to ensure that a role can be carried out effectively when needed. Training can be delivered by the EPRR team or an external specialist party though in person sessions, virtually though the use of MS Teams, or other media engaged by the ICB. Where there is a legal requirement to train on a regular basis, this will be considered annually unless a greater frequency is required by law.

10.1.3. Training records

All training and exercising records are maintained by the Emergency Planning Team and all training that is carried out across the ICB, including local level, is captured in the ICB's training records detailing:

- Who has received training
- What training they have received
- When they were trained
- The level of skills/competence, education, qualifications
- Further training required

10.1.4. Training evaluation.

All training that is conducted is evaluated at the end of each training session confirming if learners feel that the aims and objectives of the session have been sufficiently met. Learners will also be required to carry out an online questionnaire (MS Forms) to provide more detailed feedback to allow for improvement for future training.

EPRR Lessons Register

All incident and debrief reports will capture learning and recommendations. These will be recorded in a register held by the EPRR Team who will also monitor their implementation with the support of the AEO. The register will be published internally and will be shared with the ICB Executive Team though the EPRR WG and the Audit Committee as often as changes occur and in line with the schedule of the meetings. Additionally, the EPRR Team will also identify applicable learning from other NHS organisations for the improvement of plans and response.

10.2. Exercising

The ICB has a statutory duty to exercise Business Continuity Plans on an annual basis. This can be done as part of an ICB wide exercise, at a departmental level or in an actual incident, as per the ICB's EPRR policy.

10.2.1. Exercise Debriefing and Reports

Exercises are evaluated by the participants against the aims and objectives of the exercise; this is done at the end of the exercise in a hot debrief carried out in line with the EPRR policy debriefing arrangements. The exercise is also followed up with an evaluation sheet to record any learning and an exercise report.

This report will include an action plan to address any concerns and preventative actions required to improve the business continuity plans and strategy issued within 4 weeks of the exercise.

10.2.2. Exercise Records

All training and exercising records are maintained by the Emergency Planning Team and all exercises that that are carried out are stored in a central repository consisting of the exercise material and the Exercise Report, including:

- List of participants, including directorates they represent
- The exercise aim and objective
- The Exercise scenario and injects
- The skills/competence tested by the exercise
- When the exercise took place
- The outcomes of the exercise
- Further training required
- Actions/ recommendations that are aimed at addressing the exercise outcomes

10.3. Communication

10.3.1. BC Awareness Communication Methods

In order to ensure that this strategy is communicated a variety of mediums will be used:

- **CWICB All Staff Briefing** – briefing on documents and information regarding the business continuity processes, introducing and directing staff to relevant Business Continuity information.
- **Internet** – publishing of information relating to business continuity and the ICB's intent on the internet allowing engagement with stakeholders and partners.
- **Directly** – direct contact with those implementing the processes in this strategy via a variety of routes including email and face to face contact. This method will also be used to engage with partners and other stakeholders where required. Emergency communications will be sent out using direct contact. Additionally, the Emergency Planning Team could take the opportunity to organise awareness sessions and workshops, for example during the Business Continuity Awareness Week.
- **Staff Newsletters –** promoting relevant Business Continuity information in the regular email communications to all staff, sent every Monday and Friday.
- **New Starter Inductions –** incorporating details of Business Continuity plans within the New Starter Induction Booklet and induction process, ensuring that new members of the organisation are aware of relevant procedures.

10.3.2. Frequency

Frequency of communications varies according to the type used. Most information is available constantly via the internet, but other direct methods will vary according to the need and nature required of the information.

10.3.3. Evaluating Communication

Communications regarding the business continuity programme are evaluated though the annual Business Continuity Audit conducted by the Emergency Planning Team as a figure indicating the number of staff that acknowledge they are familiar with the ICBs current Business Continuity arrangements and that they are aware of the first steps they should take in the event an incident.

10.3.4. Warning and Informing Staff and the Public

The CWICB maintain arrangements to make information available to the public on emergency preparedness matters and to warn, report and advise the public in the event of an incident. The ICB Communications Team informs the public during incidents via the ICB Internet page and can deliver communications by a variety of routes for specific events if necessary. These arrangements are detailed in the *Incident Communication Plan maintained by the ICB's Communications Team.

10.4. Resource Management

The management of resources for the ICBs Emergency Preparedness, Resilience and Response arrangements is detailed in the overarching EPRR policy, including the provision of adequate resources and approval of budget.

10.5. External Suppliers and Contractor

As part of the tendering process of any new contract or agreement for the provision of goods and services to the ICB's critical services as identified in the organisational BIA, all involved parties are required to provide a statement and evidence of Business Continuity arrangements.

Plans will be reviewed as part of this process to ensure suitable arrangements are in place for the provision of the goods and services they are being contracted for. This function will be supported by the Emergency Planning Team as appropriate and before a contract is awarded.

A signed statement or declaration by the providers attesting their Business Continuity arrangements will be considered acceptable assurance, however a copy of the Business Continuity plan would be preferred.

As a minimum, Business Continuity Plans/ Statements being reviewed must provide assurance to the organisation that in the event of a disruption, arrangements are in place to ensure the continuation of the delivery of the services they are contracted for, recovery time and maximum tolerable period of disruption.

External BCPs will be maintained by the EPRR team in an access controlled central repository.

10.6. Mutual Aid

During incident response an organisation's capacity and / or capability to provide safe and effective patient care may be exceeded. Once internal business continuity arrangements have been exhausted, it may be necessary to seek support from other organisations in a formal, documented way. This formalised support is referred to as 'mutual aid'.

Please refer to the Regional Mutual Aid guidance outlining the response to a significant health related incident or emergency, as well as the associated CWICS Mutual Aid Agreement and Memorandum of Understanding and associated local agreements. The Mutual Aid Agreement and relevant associated processes and documentation are also referenced in the ICB's Incident Response Plan and EPRR Policy.

11. Governance & Audit of Business Continuity System

11.1. Governance

11.1.1. Document review and approval

Documents within the Business Continuity Management System will be reviewed by the plan owners and the Emergency planning Team, where required. These will be reported to the EPRR WG, in line with the group's Terms of Reference (EPRR WG ToR), for final approval, at least once a year.

11.1.2. Reporting arrangements

A BC Audit Report will be shared with the Board via the appropriate EPRR governance route and in line with the ICBs EPRR Policy. The report will be produced following an audit process, described below, and will be signed off by the organisation's AEO.

11.1.3. Monitoring

Motioning of progress made against achieving full compliance with the Business Continuity Standards within each Directorate will be executed as one of the functions of the EPRR Working Group, as per EPRR WG ToR. Each DBCL will be reporting on progress made, challenges and support required to achieve full compliance on a yearly basis.

11.2. Audit

In order to maintain oversight of the ICBs Business Continuity arrangements, a yearly internal audit will be conducted by the Emergency Planning Team and will be supported by the Directorate Business Continuity Leads (DBCL) and overseen by the Accountable Emergency Officer (AEO).

The audit will, as a minimum, address the following Key Performance Indicators:

- Risk (are current risks addressed by the plans)
- BIA (number of BIA in place and in date) %
- BCP (number of plans in place)
- Training (staff undergone training in role)
- Exercising (plans exercised in past 12 m)
- Debriefs (debriefs completed in required time)
- Lessons (time to address lessons, average)
- Awareness (% staff aware of role)
- Supplier contracts (number of key suppliers audited in year or similar)

11.2.1. Auditing Method

The organisational audit will comprise of the collated audit data produced as a result of Directorates level audits conducted by the DBCL and the EPRR Team. The audit will be conducted via MS Forms and collated locally at Directorate level and organisational wide. As the post holding accountability for the organisation, the AEO may also request audits to be undertaken by an external specialised party.

11.2.2. Audit Reporting

The results of the audit will be published in the form of a report on the ICBs current Business Continuity compliance with this policy and all associated statutory, regulatory and contractual requirements. The report will consist of the findings of the audit and actions and recommendations that have been jointly agreed by the EPRR Team and the DBCL. The EPRR team will collate all reports for the organisation and report via the EPRR WG to the AEO. This in turn will be used to produce the yearly report to board.

12. Review, update and compliance

The review, update and compliance arrangements of this and all other plans and policies are described within the ICB's overarching Emergency Preparedness, Resilience and Response (EPRR) Policy. This section of the policy represents an extract of the EPRR Policy and will be updated in line with changes to the EPRR Policy.

12.1. Monitoring Compliance

The Emergency Planning Lead will ensure that the key processes set out in this document are audited. The results will be fed back via the EPRR governance structure.

Where monitoring has identified deficiencies, recommendations and an action plan will be developed to improve compliance with the document. See table below for specific details

12.1.1. Monitoring Table

Aspect of compliance or effectiveness being monitored	Monitoring method (i.e. regular audits/reviews/once exercised or tested via incident response)	Individual/ department responsible for the monitoring	Frequency of the monitoring activity (i.e. Monthly/ Annually)	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
Business Continuity Management System	Yearly review / Once exercised or tested via incident response / Once updated legislation or guidance published (whichever comes soonest)	Head of EPRR/ Chief Executive Officers	Annually	Audit Committee	EPRR Working Group/ Head of EPRR

12.2. Staff Compliance Statement

All staff must comply with this ICB-wide policy and failure to do so may be considered a disciplinary matter leading to action being taken under the ICB's Disciplinary Policy. Actions which constitute breach of confidence, fraud, misuse of NHS resources or illegal activity will be treated as serious misconduct and may result in dismissal from employment and may in addition lead to other legal action against the individual/s concerned.

A copy of the ICB's Disciplinary Policy is available on the Intranet and ICB websites.

12.3. Equality & Diversity Statement

In applying this policy, the ICB will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.
A full EQIA in not required for this policy as this is not a policy which affects the delivery of patient services. Individual BCPs may need to have an assessment to ensure they do not create unexpected inequality during a disruption (eg they have chosen accessible alternative sites, etc).

12.4. Ethical Considerations

The ICBs recognise their obligations to maintain high ethical standards across the organisations and seek to achieve this by raising awareness of potential or actual ethical issues through the Policy consultation and approval process.

13. List of Acronyms and definitions

Term	Definition
AEO	Accountable Emergency Officer
CCA	Civil Contingencies Act
EPRR	Emergency Preparedness, Resilience and Response
ICB	Integrated Care Board
ICS	Integrated Care System
LRF	Local Resilience Forum
NHSE	NHS England
RTO	Recovery Time Objective - a period in time in which the organisation will aim to start recovery and/or return to business as usual after the start of an incident
MTPOD	Maximum Tolerable Period of Disruption - the point in time, following the start of a disruption, within which an activity must be resumed before the disruption compromises the ability to achieve the activity against the categories of impact highlighted in the BIA
RPO	Recovery Point Objective - the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."

14. References and Supporting Documentation

14.1. Legislation and Guidance

The following legislation and guidance have been referenced in the development of this document:

- Civil Contingencies Act 2004
- Emergency Preparedness – Statutory guidance (CCA 2004)
- Emergency Response and Recovery – Non statutory guidance (CCA 2004)
- NHS England EPRR Framework & Guidance
- ISO 22301 Security and Resilience - Business Continuity Management Systems – Requirements
- ISO 22313 Societal Security - Business Continuity Management Systems – Guidance
- PAS 2015 - Framework for Health Services Resilience
- NHS Commissioning Board Core Standards for EPRR
- NHS Commissioning Board Business Continuity Management Framework (service resilience)
- Organisations Business Continuity Policy
- NHS Commissioning Board Emergency Preparedness Framework
- NHS England EPRR BC toolkit
- NHS Standard Contract
- Business Continuity Institute Good Practice Guidelines – A Guide to Global Good Practice in Business Continuity

14.2. CWICB Associated Documents

- Emergency Preparedness, Resilience and Response (EPRR) Policy
- CWICB Business Continuity Plan
- EPRR Working Group Terms of Reference
- Incident Response Plan
- *System Coordination Centre and Incident Coordination Centre SOP
- Mutual Aid Agreements
- *Incident Communication Plan
- Risk Policy
- Coventry and Warwickshire Integrated Care Board - Policy Guidance
- Disciplinary Policy
- CWICB Organisational Chart

The most up to date version of all ICB documents referenced in this policy can be accessed via the ICB Document Library https://www.happyhealthylives.uk/document-library/

*these plans/ policies are currently under development – full compliance will be achieved once these become available

15. Appendices

List of Appendices

Appendix A Mitigation Strategies

This stage of the BCM process is about identifying action that can be taken to maintain the activities that underpin the delivery of the ICB's Critical Functions. Having determined the vital resources through the Business Impact Analysis (BIA) Process, the next step is to develop strategies to maintain local service continuity should any of these become unavailable. The table below provides some of the options that can be considered during the planning and response stage to mitigate against any of their loss – however this should not be seen as an exhaustive list:

Resources	Tactics
People	1. Creating an inventory of staff skills not utilised within their existing roles – to enable redeployment. 2. Process mapping and 'Job cards' – to allow staff to undertake roles with which they are unfamiliar. 3. Multi-skill training of each individual. 4. Cross-training of skills across a number of individuals. 5. Carry out regular succession planning (this will be highly useful during a Pandemic event). 6. Identify possible third party support, backed by either Contractual Agreement(s) or Memorandum(s) of Understanding. Note: Geographical separation of individuals or groups with core skills reduces the likelihood of losing all those capable of undertaking a specific role.
Premises	1. Identifying alternative space(s) within the ICB premises through buddy arrangements. 2. Identifying displacement of staff performing less urgent business processes with staff performing higher priority activity. (care must be taken to avoid backlogs becoming unmanageable) 3. Establishing remote working capabilities – this can be working from home or other locations (provided there are no security issues). 4. Identifying use of premises which are provided by other partner agencies (such as Local Authorities) including those provided by third party specialists. 5. Identifying the needs of staff working under the Equality Act (2010). 6. Exploring the possibility of Temporary accommodation. 7. Identifying possible alternative sources of machinery and other specialist equipment. Note: Not all locations are compliant with the Equality Act; reasonable adjustment will need to be taken into account before displacing any staff.
Information Technology & Communications (ITC)	1. Maintaining the same system at different locations that will not be affected by the same incident. 2. Ensuring data is backed-up and kept off site. 3. Copies of essential documentation are kept off site. 4. Access to emergency Mobiles 5. Installing alternative telecommunication system such as BT Lines
Information / Vital Records	1. Essential documentation is stored securely (e.g. in a fire proof safe) and/or possibly off site 2. Information saved on multiple formats (e.g. Paper, Electronic, Cloud)
Suppliers & Partners	1. Storage of additional supplies at another location. 2. Identifying and creating a list of alternative suppliers. 3. Encouraging or requiring suppliers/partners to have a validated business continuity capability. 4. Having arrangements in place for local purchasing. 5. Consider what Mutual Aid can be put in place. 6. Integrating BC within contract/procurement process.
Key Stakeholders	1. Mechanisms in place to warn/inform key stakeholders 2. Have arrangement in place to meet the needs of vulnerable service users.

The most appropriate strategy/strategies will depend upon a range of factors such as:

- The Maximum Tolerable Period of Disruption (MTPD) of the critical functions
- The costs of implementing a strategy / strategies
- The consequences of inaction.

Appendix B Incident Level Triggers

The level of response for an internal incident will be determined by the type of trigger to the response. Examples of incident levels and their triggers are detailed below.

Incident Level	Description	Action / Escalation
Business Continuity Incident	Routine issues - staff illness, leaks, general maintenance	• Local BCP activated • Co-ordinated locally • Emergency Planning Team informed
	Disruption to IT services, telecoms failure, denial of access to buildings, localised flooding	• Local BCP activated (may be multiple) • Co-ordinated by System Coordination Centre • Tactical Command informed via SCC SPOC
	Loss of critical service(s), infrastructure failure, large-scale and prolonged ICT systems failure	• Organisation BCP activated • Local BCPs activated • ICC set up • Tactical Command activated • Strategic Command informed • NHS England informed • Stakeholders informed
Critical Incident	Loss of multiple critical services, fire resulting in evacuation, prolonged utility failure	• Tactical and Strategic Command Teams activated • NHS England informed • External assistance from other agencies may be required (i.e. NHSE, Local Resilience Forum partners, other stakeholders)

*A decision to escalate an incident from a Business Continuity to a Critical Incident will be made by the ICB Strategic Command and informed by the level of disruption the organisation is experiencing

Appendix C Mandatory Business Continuity Plan Document Control

Document Control

Document Information	
Ratified by:	***e.g. EPRR WG / Directorate Management Group***
Date ratified:	
Principle author(s):	
Accountable Emergency Officer	Rachel Danter, Chief Transformation Officer
Responsible committee:	Emergency Planning Working Group
Date when policy comes into effect:	
Review date:	
Target Audience:	e.g. All staff , all "Directorate" staff
Location of document:	e.g. local repository (include file path); EPRR Team Business Continuity repository; CWICB SCC (Westgate House)

Reviews and updates

Version	Date	Summary of Changes
V1.0		

Dissemination schedule

Target audience(s)	Method	Person responsible
e.g. Executive Directors		
e.g. All staff		
e.g. External Interested Parties		

Business Continuity Plan Review Process

This Business Continuity Plan (BCP) is a living document which is constantly being monitored, reviewed, and amended to reflect learning from incidents, exercises, audits and other sources. All plan holders are responsible for contributing to the review process. The Emergency Preparedness, Resilience and Response (EPRR) Team are responsible for ensuring that this process is carried out, and sign off occurs via the Emergency Preparedness, Resilience and Response (EPRR) Working Group(s).