Meeting the Requirements

Business Continuity

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

In the event of a major disruption such as cyber-attacks, floods and supply failures the organisation needs to be able to continue to function with as little disruption as possible, with vital business processes still needing to be carried out. Having documented business continuity plans and procedures assists this process, enabling all staff to know how to keep going under any circumstance.

Business Continuity Plans (BCPs) represent an attempt by organisations to predict, assess and counteract threats and risks that may lead to events that seriously disrupt or curtail all or part of their business functions. Business Continuity Assessments analyse the probability of untoward events occurring, and their likely impact. They determine what the organisation can do if they happen, and how the organisation systematically goes about recovering from these events.

The organisation can consider including data security content in its BCP; alternatively, it can consider developing a separate IT disaster recovery plan. Whichever route the organisation chooses data security should be included in any plan, even those not related to cyber security incidents.

GMPs may require support from their appropriate commissioning Health Board to put appropriate plans and procedures in place.

How do we reach Attainment Level 1?

It is vital that organisations can still operate day-to-day functions should a major disruption occur, and should therefore have a Business Continuity Plan in place. In order to develop a business continuity plan, an assessment is required of all the business functions to analyse the probability of untoward events occurring. Consideration should be given to the likely impact on the organisation, what the organisation can do if they happen, and how the organisation systematically goes about recovering from these events.

Whilst the organisation may prefer to manage business continuity through group work, it is generally best to identify a senior staff member to act as the Business Continuity Lead for the organisation to oversee risk assessments and coordinate an overall assessment plan.

When developing a Business Continuity Plan, the organisation should identify and document all the critical resources needed to run the organisation. This may include computer systems and files, physical documents, specialist equipment; the things that would severely disrupt the work of the organisation if it no longer had them and could not easily replace them. These resources are also likely to include key staff; what would happen if several staff were absent due to sickness at the same time? If access to resources was restricted temporally, how long could the organisation manage without them before it needed to take emergency action? Critical resources that are also information assets should be captured in the organisation's information risk register.

Critical information systems should include all systems containing patient data and communication systems necessary for transmitting patient information. Critical processes should include those necessary for the delivery of patient care.

Risks to the confidentiality, integrity and availability of systems and processes should be assessed. The impact of threats should be assessed to determine priorities and plans put into place to counter the threats. Critical times (those affecting the potential to deliver adequate patient care) should be assessed and counter measures put into place to ensure system or process recovery occurs within agreed time limits.

Consider all the potential threats or points of weakness in the working environment and the impact these may have. NHS Digital (NHS England) have some useful resources including a 'BCP Checklist', but each organisation will have different features and arrangements that need to be considered.

The actions, which the organisation would need to take if the workplace was affected by an incident, should be considered. The organisation will need a plan to assess the extent of the disruption and decide what to do next. An 'Impact Analysis and Action Plan Outline template' are available on the NHS Digital website (NHS England).

How do we reach Attainment Level 2?

Once the major risks to the organisation's business continuity have been assessed and action plans developed for responding to the most likely disaster scenarios, the Management Team need to approve the work and be satisfied that it is robust and comprehensive.

Staff need to be given clear guidelines on what to do in the face of an emergency or a disaster. These should be extracted from the action planning section of the risk assessment and presented in a short note; preferably a single side A4, which staff can access and/or is pinned to a communal noticeboard.

How do we reach Attainment Level 3?

A review group should be established to take responsibility for review, coordination and testing of the plan. A regular review and testing timetable should be established and conducted on an annual basis. Reviews should also be carried out following significant system changes, relocation of facilities and staff reorganisation.

The contingency plan should be tested to ensure that all staff are aware of what to do in an emergency or unusual situation. All staff are familiar with carrying out a fire drill; this is the same sort of thing, but for different circumstances.

Some elements of the plan could be worked through in discussion whilst others may benefit from walking staff through the required steps. Notes should be kept of anything that didn't work well, so that changes can be made to the plan as necessary.

Supporting Resources

NHS England: BCP Checklist

NHS England: Impact Analysis and Action Plan Outline template

NHS England: Emergency Preparedness, Resilience and Response (EPRR)

Summary Requirement

Attainment Level	Summary Requirement
1	There has been an assessment of the risks to all information systems where information is critical to the running of the organisation
2	The Business Continuity Plan has been approved by the Management Team and all relevant staff are made aware of its implications
3	The Business Continuity Plan has been tested and is regularly reviewed