Public Health England

Guidance for Business Continuity Management System

Date of issue: **October 2018**
]

Date of review: No later than three years from date of issue

Document code: BCM\001B

Version: 02.00

Author: Strategic Business Continuity Manager

National Executive Member responsible for this policy: Name Redacted

THIS DOCUMENT IS VALID ONLY WHEN VIEWED VIA THE INTRANET. IF IT 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 ONLINE. PRINTED DOCUMENTS ARE UNCONTROLLED COPIES

1. AMENDMENT HISTORY

Version	Date	Author	Description	Approval
01.00	October 2015	Name Redacted	Endorsed at EPRR OG	EPRR OG
02.00	October 2018		Completed whole document review and consultation process. Agreed by EPRR DG	

2. BACKGROUND

2.1 The Public Health England (PHE) Business Continuity Management Policy requires all of its, sites, departments and Directorates to implement effective business continuity arrangements. This requirement supports the organisation's obligation to meet its responsibilities under the Civil Contingencies Act 2004 and that its business continuity activities are aligned to the International Standard for business continuity management, ISO22301 – Societal Security – Business Continuity Management System - Requirements.

2.2 The organisation's Business Continuity management Policy states:

> "PHE is committed to the delivery of a robust business continuity management system (BCMS). This policy provides a statement of commitment to ensure that business critical activities can be maintained during a disruptive incident, such as denial of premises, staff absence, supply-chain interruption (including loss of utilities) and ICT failure".

2.3 Business Continuity Management is a reporting requirement for the following:

(a) PHE internal assurance

(b) Civil Contingencies Secretariat, National Capabilities Survey

(c) NHS England Information Governance tool kit, Requirement 309

3. SCOPE

3.1 The scope of this document includes all Business Continuity Management lifecycle activities are within scope of the organisation's Business Continuity Management programme.

3.2 Lifecycle activities assure continual improvement through a process of exercising, testing, review, and update of plans and strategies to ensure alignment with current and changing delivery requirements of PHE.

3.3 The PHE Records Management Policy and operating procedures are to be followed and applied to all BCM documents.

3.4 The scope is to consider the appropriate response to the impact of a business continuity incident, not the root cause of the incident.

4. PURPOSE

4.1 The purpose of this document is to give guidance for the business continuity activities to be undertaken across the organisation, including those for documentation and the frequency and principles for exercising, maintaining and reviewing the Business Continuity Planning documents and other arrangements. This approach reflects the ISO22301 business continuity management model of "Plan-Do-Check-Act".

5. POLICY

5.1 The PHE Policy for Business Continuity Management is aligned to the International Standard for Business Continuity Management, ISO 22301. The PHE Guidance Notes for Business Continuity Management are aligned with its Business Continuity Management Policy.

(a) Ownership

(i) The Policy is managed by PHE Strategic Business Continuity Manager on behalf of the owner, the Director for Corporate Affairs.

(b) Approval

(i) Approval of the policy, through EPRR Delivery Group and Risk Leads Group, Endorsement is the responsibility of the Corporate Policy Group on behalf of the National Executive.

(ii) Approval must be reaffirmed no later than three years from the date of issue.

(c) Maintenance

(i) The Business Continuity Management Policy will be reviewed by the PHE Strategic Business Continuity Manager and updated as necessary.

(d) Compliance

(i) It is mandatory for all PHE Locations and Offices, Directorates and Divisions or Departments to comply with the Business Continuity Management Policy.

(ii) Compliance will be measured through a combination of self-assessments, assurance and audit reviews

6. RISK ASSESSMENT

6.1 Risk Assessment is one of the fundamental components of BCM it considers the impact of remaining identified threats on the operation.

6.2 Business Continuity will consider and plan for residual risks and ensure a response capability is in place to manage incidents where the threat has previously not been identified or that the likelihood of occurrence is very low.

6.3 Risk Assessments are completed in accordance with PHE Risk Management Policy, Procedures and guidance. Also refer to Annex A: BUSINESS CONTINUITY MANAGEMENT APPROACH TO RISK MANAGEMENT

7. SERVICE IMPACT ANALYSIS (SIA)

7.1 Each of the PHE Locations and Offices, Directorates and Divisions or Departments is responsible for analysing the impact of disruption on the delivery of services to maintain PHE corporate priorities. This is achieved by performing Service Impact Analyses. It is recognised that there will be similarities of functions in Directorates

across different locations and for this a template can be developed within the directorate and this used to ensure consistency.

7.2 A tool is available for completing the Service Impact Analysis although this is not mandated.

(a) Ownership

(i) Service Impact Analyses are owned by the Locations and Offices, Directorates and Divisions or Departments managers.

(b) Approval

(i) It is the responsibility of the owner to provide approval and sign off for the Service Impact Analysis for which they are responsible.

(c) Maintenance

(i) The owner of the SIA must ensure that it is reviewed and updated at least annually or as a consequence of significant organisational or operational change

(d) Compliance

(i) Evidence of the review and any changes made are to be recorded.

8. INCIDENT MANAGEMENT

8.1 To ensure effective management of an incident an Incident Management Team will be defined along with the procedure for authority to declare a Business Continuity incident and activate the Team to manage the response. The incident director will be the site director, nominated deputy, or Director on-call.

8.2 The model for the Incident Management Team to manage a business continuity incident is recommended to be based on the structure and roles and responsibilities described in the National Incident Emergency Response Plan.

8.3 For incidents that are 'Routine', these will be managed without interrupting operational capability. A 'Routine' incident will not require activation of the Business Continuity Management response but is within normal management operational capability.

8.4 A 'Standard' business continuity incident will elicit a local Incident Management Team will be activated. The incident director will be the site director, Director on-call, specialist service director or, nominated deputy. Furthermore, a Standard level incident may require the national EPRR team to run a cell supporting the ID with liaison with national agencies or stakeholders. This is separate from an NICC.

8.5 Business Continuity Management incidents that are 'Enhanced' will require, national oversight or full national management of the response. The National Incident Emergency Response Plan will therefore be activated.

8.6 During 'Enhanced' incidents, local Business Continuity Management plans will also be activated. Situation Reports (SitReps) will be sent by ICCs into the NSAC as

required by the Battle Rhythm set at the National level through activation of the National Incident Emergency Response Plan.

9. BCM CONTINUITY AND RECOVERY STRATEGY

9.1 The strategy is determined and applied in response to the threats, outstanding risks and results of the Service Impact Analysis. This strategy includes the options for protecting the organisation's critical activities and the resources that are required to support them. The strategic resources will include: People; Premises; Technology and Supply chain.

9.2 The identified strategy should ensure that cost effective resilience is factored into operating environments whether physical or virtual. Resilience must nevertheless be proportionate to and in accordance with the risk appetite but also to ensure that the organisation's statutory and regulatory obligations can be maintained.

9.3 Where appropriate, reciprocal or mutual assistance arrangements e.g. between different parts of the organisation, other public sector bodies or the private sector may be used to optimise resilience and exploit opportunities to assure continuity.

9.4 Home or remote working arrangements should be supported where this is appropriate however guidance must be sought before any personal premises are allocated or used for any Team or group departmental activities.

NB. Consideration must be given e.g. Health & safety at Work Act, Display Screen Assessment, Insurance liability etc.

9.5 Home working arrangements must consider the availability of suitable technology to ensure effective working and this may include the requirement for staff to transport PHE laptops as a routine part of their operational role.

9.6 Laptops or other equipment at all times must be transported using a container that is appropriate for the purpose. This will be different for each individual and may include but not necessarily be limited to: Ruck-sack bag, shoulder bag, trolley-bag. Individuals should assess what is appropriate for them and include: what will normally be transported; the typical journey; method of transport used (walk, cycle, drive, bus, train, etc.); physical capability.

NB. Consideration must also be given to the PHE Information Security Policy to ensure compliance with the elements of data security (Confidentiality, Integrity, Availability).

(a) Ownership

(i) Each site, Directorate and department, is responsible for developing and implementing its own Business Continuity response strategy.

(b) Maintenance

(i) The response strategy must be reviewed and updated at least annually or as a consequence of significant operational or organisational change.

(c) Compliance

(i) All sites, Directorates and departments must comply with the requirement to implement their BCM response to ensure key / critical functions will at least meet the Recovery Time Objective as identified in the Service

Impact Analysis. The Recovery Time Objectives must be aligned with supporting the PHE Corporate priorities but take into account that immediate Recovery Time Objective whilst preferred, may not be practical or achievable because of cost or with the resources available.

(ii) The BCM response solution(s) will be approved locally by the responsible officer prior to implementation.

10. BUSINESS CONTINUITY MANAGEMENT PLAN

10.1 Business Continuity Management Plans must be developed and implemented to ensure coverage across all operational levels of PHE.

(a) Ownership

(i) Business Continuity Management Plans are owned by the Director or Manager who is responsible for the delivery of the service or availability of the site.

(ii) The property owner must be satisfied that Business Continuity Management Plans are developed and implemented for all business units at the site. Relevant Business Continuity Management Plans should be cross referenced.

NB. The Corporate level Business Continuity Management Plan (Strategic level) is encompassed by the National Incident Emergency Response Plan.

(b) Approval

(i) The plan owner is to approve and sign off of the Business Continuity Management Plan for which they are responsible.

(c) Maintenance

(i) Business Continuity Management Plan owners must ensure that plans are regularly maintained.

Business Continuity Management Plans should be reviewed regularly and at least in compliance with the guidelines given in the following table:

Plan Maintenance	Quarterly	Annually	Time of change
Contact Information	**X**		
Critical Functions		**X**	**X**
Strategy		**X**	**X**

(d) Compliance

(i) Business Continuity Management plans must include a document history to evidence the reviews and summarise the changes that have been made.

10.2 Components of the Business Continuity Management Plan

(a) Background

(i) The background to the plan to be detailed including what the drivers are and the organisational structure explained.

(b) Activation

(i) Describes who is responsible for activating the Business Continuity Management Plan;

(ii) The process for activating the Business Continuity Management Plan;

(iii) The method of notifying the activation of the plan, including cascade and escalation as appropriate;

(c) Ownership

- The Director or Manager that is responsible for the site, Directorate or department is responsible for the process to ensure that the Business Continuity Management Plan can be activated with appropriate authority and within acceptable time scales based on justifiable assessment of the impact information that is available at the time of an incident.

- Activation will include notification to those responsible for activating the Business Continuity Management plan and managing the incident.

(ii) Notification will also include call cascade to relevant staff, stakeholders and escalation within PHE as appropriate.

(d) Approval

(i) Approval for activation of the Business Continuity Management plan must be justifiable based on analysis of the impact information available at the time.

(e) Maintenance

(i) It is the responsibility of the owner to ensure that the activation process and contact details of stakeholders is maintained

(f) Compliance

(i) Ensure effective activation and operation of the Business Continuity Management plan through a program of exercising and training.

10.3 Communication

(a) Ownership

(i) It is the responsibility of the plan owner to ensure that the activation of the Business Continuity Management plan can be communicated in a timely manner to appropriate parties.

(b) Approval

(i) Approval for notification is the responsibility of the manager who is appointed as Incident Director for managing the incident and mobilising the resources required for the incident response.

(ii) Notification must be timely and effective with staff and as appropriate other stakeholders and partners.

(c) Maintenance

(i) The contact details must be regularly reviewed and updated to ensure that they remain current

(d) Compliance

(i) Regular testing of contact details will verify the currency of the data and aim to ensure staff and stakeholders are prepared to respond appropriately when required.

(ii) The notification method should follow existing PHE methods e.g. call cascade methodology or use tools approved for corporate notification where available.

11. PEOPLE

11.1 People are the most important and valuable asset for any organisation. Without its staff it will not be possible for the organisation to function or recover from a business continuity incident.

11.2 Good Business Continuity Management planning will protect employment, contribute to maintaining good levels of staff morale and give confidence in PHE being an employer of choice. A content workforce will more likely be motivated to protect the reputation of the organisation, especially during times of operational stress.

11.3 It is important to ensure that corporate knowledge is protected, staff skills developed and maintained and a record of skillsets kept.

11.4 To ensure resilience in the workforce, a program of cross training for at least all key roles and critical functions will help to avoid the dependency on individual members of staff. Furthermore, cross training facilitates staff development which gives opportunity for staff also to open doors to furthering their career and therefore be of greater value to PHE.

11.5 Over time, for a variety of reasons, all organisations experience staff turnover or staff may be unavailable such as during a pandemic infection outbreak. The reasons are numerous, including when staff may choose to change roles or employers. This can be relatively sudden or unexpected. A resilient organisation will ensure that succession planning is in place to protect against loss of skills and corporate knowledge. An inclusive approach contributes to the increased resilience of PHE.

(a) Ownership

(i) Managers are responsible for the identification and recording of key skillsets and ensuring that programs of cross training and succession planning are developed and implemented locally.

(ii) A record of competencies, academic and professional qualifications, learning certifications and experience should be maintained as this can prove important in identifying key staff and contribute to the improved resilience of PHE during incident response capability.

(iii) Staffing levels should be maintained at all times to ensure that at least critical functions can be continued during disruptions or incidents such as infectious disease (e.g. influenza, Norovirus, industrial action, etc.).

(b) Approval

(i) Managers are responsible for approving the strategic approach to ensure that key skillsets, cross training and succession planning are in place and that programs meet the requirements of ensuring that PHE is a resilient organisation.

(c) Maintenance

(i) The records of skillsets must be regularly reviewed and maintained to reflect changing circumstances such as staff rotation, changes in staff skills, experience and the organisation or its operations.

(ii) Contingency plans will include the prioritisation of critical functions to be maintained when incidents occur.

NB. The percentage of staff and therefore skills available will depend of the nature and acuteness of the incident and therefore consideration should be given to evidence from previous incidents and current knowledge e.g. the science regarding highly contagious disease infections, severe weather, environmental and geographical circumstances, union membership and militancy, economic factors, lottery syndicates, etc.

(d) Compliance

(i) The benefits and performance of effective cross training and succession planning must be verified through exercising, lessons identified and appropriate records kept.

(ii) All sites and at each organisational level of PHE, management must ensure that reviews are undertaken of staffing and contingency planning arrangements for unavailability of skilled staff.

12. PREMISES

12.1 Effective contingency planning will include the loss or unavailability of PHE premises or leased premises, etc. where PHE staff are hosted.

12.2 Premises will include the site, all buildings, perimeters, infrastructures and services, including utilities.

12.3 Premises must be appropriate for their intended use and maintained to an appropriate level, taking into account risk management, health and safety, security, infrastructure resilience, etc.

12.4 PHE BCM Plans must include planning for the relocation of staff and / or reallocation of functions to alternate locations.

12.5 The re-provision of new premises, if the usual location is unavailable for a prolonged period of time or permanently, must be requested from PHE Estates and Facilities in the first instance. However this does not preclude local arrangements for mutual aid agreements to be established with other PHE offices, science and laboratory based locations and that these may include non-PHE partners.

(a) Ownership

(i) Premises may be owned or leased by PHE. Premises may be sole or shared occupancy.

(ii) PHE may also be an occupant of shared premises where it is not the owner or leaseholder.

(iii) Assessments of risk relating to all aspects of the premises should be completed and recorded. This will include where PHE is a hosted organisation.

(iv) Risk assessment of premises should be completed to recognise threats and potential single points of failure and taking into consideration: locality; neighbourhood; local environment; services infrastructure and resilience.

(v) The strategy for alternate working arrangements must be planned in preparation for incidents when premises may be unavailable for either a short / temporary period of time e.g. denial of access / exclusion zone because of an incident in the nearby vicinity. Planning will also include long-term or permanent unavailability or loss of the site because of direct impact e.g. fire, flood, contamination, subsidence, etc..

(b) Approval

(i) Local management should approve the acceptance of the premises based on the operational demand priorities and having assessed the associated risk profile.

(ii) All risks must be identified, recorded in the appropriate risk register, ownership assigned and approval given for acceptance, mitigating actions or transfer of risk.

(iii) Approval of the strategic planning and response will be given by the plan owner.

(c) Maintenance

(i) The strategy and planned solutions must be reviewed and maintained to ensure that they remain appropriate for the continuance of key and critical functions when the Business Continuity Management plan is activated in response to an incident.

(d) Compliance

(i) Reviews of the Risk Assessment are to be completed in line with PHEs established Risk Assessment guidance and these reviews must be recorded along with changes to the Business Continuity Management plans.

(ii) Regular exercising is to be designed and undertaken to verify the effectiveness of the strategy if activated.

(iii) Lessons identified must be completed after each exercise or activation and improvements from the learning implemented expeditiously.

(iv) Further exercises must be undertaken within reasonable timescales to verify the lessons learned.

13. TECHNOLOGY

13.1 Various technologies are fundamental and critical to all operational functions. The criticality of each technology is determined in the Service Impact Analysis.

13.2 Technology will comprise of a number of components that may include all or some of: hardware (including scientific equipment); software; network infrastructures and; data.

13.3 The list of Information Communication Technology assets is maintained in the 'TrackWise' system.

(a) Ownership

(i) IT systems and services are typically provided by PHE ICT department, although there are exceptions.

(ii) It is necessary to clearly identify the components concerned, their owners and who is responsible for monitoring, operating and maintaining each component.

(iii) The system owner may be different from the provider of the service. It is therefore essential that the requirements for business continuity in terms of resilience, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are identified in the SIA and communicated to the service provider through the associated ICT Account Manager or service provider.

(iv) The user recovery requirements must be realistic, achievable and evidenced by an agreed SIA.

(v) The component owner or service provider must be able to demonstrate their ability to deliver the service to meet the user defined RTO and RPO through a programme of exercising. Alternatively, negotiation must agree what RTO and RPO can be achieved and this evidenced through exercising. Acceptance of compromise of the ICT resilience capability must not cause unacceptable impact to operational recovery capability.

(b) Approval

(i) The owner / user must have confidence that the level of service is satisfactory in its provision, resilience and contingency, to meet the operational requirements in support of PHEs responsibilities under the Civil Contingencies Act 2004.

(ii) The user is to manage their requirements with the owner or service provider as appropriate and approve the service and operating level agreements.

(c) Maintenance

(i) Service provider must inform of the impact of technical changes to the owner / user of the capability and of any additional enhancements that will be required for the RTO and RPO achievable.

(ii) Maintenance should, whenever possible, be planned and agreed in advance through a formal change management process.

(iii) Emergency changes should only be made by exception and the impact fully understood and agreed so as to minimise interruption or maintain continuity of service.

(iv) Users to review their requirements to ensure that they reflect continuity of critical functions.

(d) Compliance

(i) Owners and service provider must verify their capability through a program of exercising. Exercising must demonstrate the ability to recover the service to the required Time and Point Objectives to prove the resilience of the service and recovery procedures.

(ii) Records of proposed changes should be maintained and available for owners and users to review and approve or challenge as necessary.

(iii) A record of approval for changes to be made should be maintained.

(iv) Reporting should verify the actual uptime availability and resilience of the service.

(v) Continuity exercising must demonstrate the ability to recover the service and the business continuity preparedness of ICT department in being able to respond to an interrupting event.

14. SUPPLY CHAIN MANAGEMENT

14.1 Supply-chain includes those that supply products, goods and services to any part of PHE and those to whom any part of PHE provides products, goods or services. Supply-chains therefore include those that are internal to PHE or provide outsourced services e.g. ICT, Estates and Facilities, Payroll, Emcor, other third parties, etc.

14.2 For any Business Continuity Management Plan to be effective in operation the supply chain must be managed. Primarily this will be through the conditions of the associated contract including Service Level and Operating Level Agreements, performance monitoring, reporting and review. However, certain parameters should

be considered as a standard requirement for all key contracts and therefore considered for removal from contractual terms and conditions only by exception.

14.3 Suppliers must be considered as contacts to be notified of a business continuity event that may impact the usual arrangements for supply and delivery of products or services, including the variance of volumes or where they may be delivered to, collected or originate from.

14.4 Parameters for inclusion are: the requirement to have Business Continuity Management plans and contingency arrangements in place that are appropriate to the criticality of the service or products dependency and availability of alternatives.

(a) Agreement and confirmation that the supply of key goods or services that are at least equal to the PHE demand when contingency is activated can be provided or maintained to the PHE Recovery Time Objective required by PHE.

(b) Consideration should be given to the risks associated with single supplier contracts.

(c) PHE may require operational surge capacity of supplies in response to a health emergency situation. However this may be considered aside from specific Business Continuity requirements.

(d) Ownership

(i) The owner of the supplier contract and service management is responsible for ensuring that the contract, through audit and observation or participation in exercising, is able to meet the PHE business requirements, which include assurance relating to the PHE obligations under CCA2004.

(ii) The selection of key suppliers should consider their level of compliance with ISO22301.

(e) Approval

(i) All contracts must be formally approved by following agreed policy and procedures and managed appropriately.

(ii) In consideration of Business Continuity, it is essential that the contract owner or user, includes the appropriate level of business continuity, end-to-end, throughout the supply chain. Where possible this should be achieved by obtaining assurance of key suppliers' Business Continuity Management Plans and their existing exercising and maintenance programmes.

(f) Maintenance

(i) Contracts must be reviewed by their owner regularly to ensure that the terms and conditions are understood with regard to their possible impact on the organisation's ability to deliver its critical services or to plan for circumstances where the service provided to PHE is interrupted.

(g) Compliance

(i) All sites, departments and Directorates must undertake reviews of their supply chain management processes in consideration of their Business Continuity requirements and to ensure resilience.

15. AWARENESS AND TRAINING

15.1 The purpose of Awareness and Training is to facilitate learning of Business Continuity Management across PHE.

15.2 All staff should have an understanding of the concepts and principal of Business Continuity Management as they relate to the responsibilities of PHE

15.3 Training should be targeted to those who may have an active role in supporting the response to a BC incident;

15.4 Training may be included as part of the review or exercising of Business Continuity Management plans.

15.5 Training materials are available from Civil Service Learning, PHE eLearning and third party specialist providers such as the Emergency Planning College and Continuity Shop etc..

(a) Ownership

(i) PHE Business Continuity training materials are developed by the Strategic Business Continuity Manager.

(ii) Business Continuity awareness should be included as part of induction for all staff

(iii) Managers must ensure that staff are aware of the local business continuity plans and actions which they should take during a business continuity incident.

(b) Approval

(i) Approval of the PHE Business Continuity training materials is the responsibility of the Emergency Preparedness Resilience Response Delivery Group.

(c) Maintenance

(i) The materials will be reviewed by the owner to reflect best practice.

(d) Compliance

(i) Staff should maintain a record of the training which they have completed.

16. EXERCISES

16.1 As an enabler that supports improvement in Business Continuity Management Planning, it is necessary to regularly exercise plans. Exercising provides opportunities to train staff, raise awareness and confirm that plans are robust, remain valid and identify where change may be required.

(a) Ownership

(i) It is the responsibility of plan owners to ensure that plans are regularly exercised.

(b) Approval

(i) Approval of the exercise schedule is the responsibility of each plan owner.

(c) Maintenance

(i) A rolling annual schedule should be agreed by the plan owner for the exercising of all Business Continuity Management plans for which they are responsible. This will ensure that adequate time is available for the planning and coordination of exercises and ensure the availability of resources that may be required to support the exercise.

(d) Compliance

(i) A schedule for exercises is suggested in the table below (see section 16.3).

17. EXERCISE SCHEDULE

17.1 Exercise schedules are to give point in time assurance of a Business Continuity Management Plans' capability and the staff capability to be able to respond appropriately to a BCM incident.

17.2 On implementation, any new plan will need to be exercised along with those that are responsible for activating and operating the plan during an incident. Exercising may include: desktop walk-through; scenario based walkthrough exercise; a communication exercise and an operational recovery exercise.

17.3 The following table provides a framework schedule for the **on-going** exercising of plans. It may not be possible or appropriate to exercise all aspects of the plan in a single exercise[1].

Exercise	Half Yearly	Annually	Time of change
Desktop walk-through	**X**		**X**
Communication (call-tree)	**X**		
Operational Recovery		**X**	**X**

NB. Where an exercise is conducted to verify a change, the exercise date can then be reset to half year or annual from that last exercise date.

17.4 Exercise Definitions

(a) *Table top*

(i) To try out the capability without any actual physical actions being taken. An example is a scenario based event when decision making abilities during a major incident are examined. Alternatively it can be a walk-through of the plan as a familiarisation exercise.

(b) *Communication*

(i) To verify that contact information is current and correct and that staff and other stakeholders can be contacted and are contactable if or when an incident occurs, including outside of normal working hours.

(c) *Operational Recovery*

(i) Exercising the response to an incident that can include relocating staff and / or operations to preferred alternate locations to verify that the chosen solution(s) will, during an incident, operate effectively. This type of exercise can be carried out as a rehearsal to verify relocation procedures only, without actually relocating staff or operations e.g. redirection / transfer of telephony, availability of required critical systems or services at alternate location(s). This tests the technical recovery procedures and capability.

18. LESSONS LEARNT

After any exercise or BCM incident, staff must be debriefed and any lessons that are identified, recorded and actioned in accordance with the PHE Lessons Learnt policy. BCM Enhanced level incidents should adopt the IERP Learning from Incidents and Exercises guidance.

Lessons learnt must be reflected as changes in the Business Continuity Management plan or other recovery procedures and these changes must then be exercised to prove the modified approach or to identify what further changes may be required.

(a) Ownership

(i) As a general principle, the identification of a lesson arising from an incident is the responsibility of all PHE staff.

(ii) The Incident Director is responsible for ensuring that incident or exercise debriefs are completed and lessons recorded.

(b) Approval

(i) The Plan owner is responsible for approving changes that are required from Lessons Identified debriefs.

(ii) Consideration must be given to sharing lessons identified where there may be wider implications across PHE.

(c) Maintenance

(i) Lessons identified must have actions associated to ensure that the lessons are learned so as to mitigate the likelihood of recurrence.

(ii) Lessons that cannot be learnt or that cannot be justified economically for controls to be implemented must be recorded as a risk on the appropriate register and then subject to the established risk management procedures.

(d) Compliance

(i) The final text of the lessons learnt should be authorised by the appointed incident director or nominated deputy with delegated responsibility.

19. REPORTING

19.1 Reporting supports the embedding of BCM into the culture of the Organisation; that Business Continuity Management Plans are in place, being maintained and exercised, thereby providing assurance of the planning and response capability.

19.2 Business Continuity Management assurance reporting is an ongoing activity however a snapshot will be taken annually and a PHE wide capability report will be compiled to demonstrate preparedness across PHE.

(a) Ownership

(i) All BCM plan owners are responsible for the completion of BCM self-assessment returns.

(ii) Self-assessments should be completed when Business Continuity Management documents are reviewed or exercises completed.

(iii) Reporting will be managed through compliance self-assessment. Updated self-assessments must be sent to the PHE Strategic Business Continuity Manager (gary.dade@phe.gov.uk).

(iv) The strategic Business Continuity Manager reports on the current PHE wide BCM preparedness to the Emergency Preparedness Resilience and Response Delivery Group, and Management Committee.

NB. The self-assessment is a component of continuous development and should be completed in conjunction with any Business Continuity Management activity. Furthermore the self-assessment enables identification of points for development within the Business Continuity Management programme.

(b) Approval

(i) Plan owners should approve the self-assessment returns prior to submission to the PHE Strategic Business Continuity Manager

(ii) The PHE Strategic Business Continuity Manager will obtain approval of the consolidated reports from the Emergency Preparedness Resilience Response Delivery Group before presenting to the Management Committee

(c) Maintenance

(i) Self-assessments are to be reviewed and updated following any Business Continuity Management activity and the updates sent to the PHE Strategic Business Continuity Manager.

(ii) PHE Strategic Business Continuity Manager will update the consolidated Business Continuity self-assessments report to the EPRR DG.

(d) Compliance

(i) The Strategic Business Continuity Manager prepares a report for the PHE Management Committee annually in March that demonstrates the current PHE wide preparedness assessed against Business Continuity Management Policy.

(ii) Analysis of the self-assessment to be shared by the Strategic Business Continuity Manager with National Directors and Business Continuity Leads.

20. BCM RISK ASSESSMENT GUIDANCE

This guidance facilitates the identification of risks to inform contingency planning. It is not intended to provide detailed operational guidance for individual risks but to suggest holistic approach to risk management that can improve understanding of risk to operational capability.

The information from the risk assessment will enable decisions to be taken to manage down the level of risk to be acceptable; to improve resilience or to inform decisions about response strategies for contingency planning.

In practice, such risk assessments would normally be localised to the site, however they should take into account existing resilience and contingency planning arrangements, the PHE Corporate priorities and the PHE business Plan.

BACKGROUND

A risk assessment, that focuses on the issues of operational and geographical resilience should be completed for each location, reviewed at least annually to reflect improving knowledge and changing circumstances, and updated accordingly.

The Risk Management procedure and methodology are set out in the PHE Risk management Policy and Procedures document. These procedures should be adopted and followed for BCM purposes.

The Business Continuity Management risk assessment will consider the risks that may impact operational continuity locally. In general terms it will focus on the loss or unavailability of: premises (taking into account the local environment and neighbourhood); ICT (including data); key staff; supply-chain (including utilities).

These points are not exhaustive but indicate the areas to consider for closer examination and inclusion in a risk assessment for the purposes of Business Continuity Management.

OBJECTIVE

The objective of this guidance document is to enable risk assessment authors to provide a broad view of risks that may impact operational continuance or capability.

SCOPE

This guidance is specific to risks that should be considered as part of a business continuity programme and that may otherwise be overlooked.

This guidance is intended to compliment PHE Risk Management Policy and develop thinking around the subject in terms of business continuity.

APPROACH

The risk assessment considers and records any aspect that may have a risk associated with it. See section below: "Additional Information Sources" which includes web links where information relating to the local area and environment which can facilitate discovery of threats. Consideration should be given to include the following high level aspects:

- Staff, staffing and HR;
- Premises;
- Assets (facilities, resources, equipment and plant);
- Local environment physical natural environment, the built environment, and neighbourhood);
- Transport and travel (transport links and services);
- IT systems, services networks and infrastructures;
- Supply-chain resilience (upstream – suppliers and, downstream – customers, external and PHE internal);
- Security (physical, personal, information & data, ICT systems, network and infrastructure, environmental).

It is necessary to assess the site itself, the networks and infrastructure and the surrounding area and environment.

Actions will be taken to either reduce the level through risk controls to bring the level of risk to be acceptable, acceptance of the risk at the current level or transfer the risk to be managed by a new owner. Note however that it is not possible to abdicate responsibility of risk ownership.

POINTS FOR CONSIDERATION

The following table identifies certain points for consideration however, these may already have been included in risk assessments that should have been completed by a relevant PHE department, division or directorate such as Estates and Facilities, ICT etc. or that are covered under other subject policies etc. such as Health and Safety Risk Assessment - Arrangements and Guidance

The following list is not exhaustive and indicates aspects to be considered as a starting point for local discussions. The risk assessment for Business Continuity Management purposes should be approached openly and must consider any aspect that could have a risk associated with it.

ANNEX A: BUSINESS CONTINUITY MANAGEMENT APPROACH TO RISK MANAGEMENT

Risk Type	Risk Sub-heading	Examples
Building, Site and Local environment	Give an overview of the building, its location, the surrounding environment and neighbourhood.	To indicate from where threats may emanate, either natural or man-made such as local industry, flooding, geology

Risk Type	Risk Sub-heading	Examples
	An assessment and description of the building's construction, (approximate) age, location, whether it is on a business or industrial park, in conservation area or listed etc. should be made. Also at this point consider the general condition of the building.	Operational departments should be aware of such assessment and have opportunity to comment on the acceptability of the accommodation in relation to their operational requirements and acceptance level for any associated risks. Assessment may indicate whether there may be planning issues if changes are required such as in conservation areas or listed building status. Also whether the building or its infrastructure may be at risk of infrastructure failures such as electrical, IT, Communications, heating and ventilation systems, other specialist services, utility supplies etc. NB it is not mandatory that a full buildings condition survey will be undertaken in all circumstances; only note the general condition of maintenance. The condition may also include an assessment of general building management in terms of maintenance schedules and include assessments emergency evacuation escape routes, signage etc. If there is indication that there may be more serious underlying issues with the building or its infrastructure services then these should be investigated further by a subject matter expert e.g. Chartered Building Surveyor, mechanical and electrical engineering consultants etc.. Advice should first be sought from PHE Estates and Facilities or on site PHE estates and engineering managers in the case of PHE specialist sites. Underlying issues may go beyond the condition alone. Hidden risks such as the presence of asbestos or radon gas should also be considered. Buildings built after 2000 are unlikely to have any asbestos however, a development after that year on a brown field site can still be at risk of the site being contaminated.

Risk Type	Risk Sub-heading	Examples
	Consider the local environment, neighbourhood and identify potential threats such as road and travel access e.g. one road in / out. Are there alternatives such as park remotely and walk using alternative foot-path routes, etc.?	Assess the options for travel to mitigate the risk of single points of failure both in terms of road infrastructure, footpaths, cycle ways etc. and also methods of travel (private and public transport options) that may otherwise facilitate access to or egress from the building / site.
	Does the building or PHE part(s) have suitable access controls to prevent unauthorised access? Describe the access controls e.g. electronic locks, turnstiles, etc.	Physical access control barriers should restrict unauthorised access or attempts of malicious access. Consider also the risk of ability to 'tailgate' to gain unauthorised access.
	To prevent unauthorised access, do procedures exist for managing access control for visitors and when staff (permanent, part-time or temporary) join or leave PHE?	A record of visitors is maintained and retained for an appropriate and minimum specified period.
	Do access controls and procedures cover whole building or only PHE areas when in a shared occupancy building?	If shared occupancy, there may be a risk to PHE if other occupants control procedures are less rigorous than our own.
	Out of business hours what access controls and security procedures are in place? Are security staff present on site, when, or between what hours?	On-site security staff typically have a role that is wider than only monitoring and managing threats from visitors or intruders. This may include general site security and safety in the event of problems such as fire, flood or other incidents where a response to an alert is required. Gaps in either of the days / time or scope of responsibility and the associated risks should be recorded.
	Is the building or the parts occupied by PHE fitted with intruder detection and alarm systems or is this considered necessary?	If a shared building, it may be appropriate for PHE to have in place its own monitoring rather than rely on whole building control or alarm systems. As appropriate, refer to PHE Head of Security and Sustainability.
	To where do intruder alarms alert and who is notified of any detections?	Alarms may alert remotely such as the services provided by ADT or BT RedCare, these types of solutions will have different risks associated with them.

Risk Type	Risk Sub-heading	Examples
	Is the building fitted with external surveillance security cameras? If so, do they cover all aspects of the building either as fixed cameras or, of the tilt, pan and zoom type.	In risk mitigation, it is useful to monitor what is happening outside. Furthermore the visibility of security cameras can deter malicious actions.
	Are security cameras present internally, especially in public areas, corridors and passageways etc.?	This may be appropriate, especially if the building is shared with other occupants and in areas where visitors may not be escorted.
	Where security cameras are installed, are they monitored and images recorded?	Active monitoring enables identification of issues in real-time. Consider also how long recordings are kept and also whether copies of records are secured off site? Also consider the implications of GDPR for the retention and storage of images.
	Is camera monitoring performed on-site or remotely?	On-site monitoring can avoid possible delay in responding to incidents as notification alerts are not required or are managed locally with response staff already on site.
	Do procedures exist for secure back-up and storage, including off-site, of security recordings	It is recommended that data is held securely and that this includes an off-site copy being retained for a suitable period of time in case it is required for review and that the originals have been lost. Also consider the implications of GDPR for the retention and storage of images.
	How long are security recordings retained for?	It is recommended that recordings and their back-ups are retained for at least 30 day after the date of the recording
	Are recordings periodically checked to assure quality of images and to prevent recording failures?	The quality of recording can be known to deteriorate or be lost completely as a consequence of media, hardware or network failures; therefore they should be periodically checked for completeness and quality.
	Is the building secure or can it be secured? Windows and doors that can be opened should be fitted with working locks that are secured when areas are not occupied.	It should be possible to deter and detect unauthorised entry to buildings.

Risk Type	Risk Sub-heading	Examples
	Is there an alarm and / or fire suppression system installed and maintained in the building or PHE parts of it?	It should be possible to alert staff effectively and the systems should be maintained to ensure reliable operation and to mitigate the likelihood of false positive alerts.
	Is the alarm and or fire suppression system automatic or is manual intervention required?	Preferably alert systems should avoid manual intervention as this will then require active monitoring by staff, which may not be possible for all areas.
	Is the building / site owned or leased?	The status of the building or site can impact the ability of the occupants to undertake modifications or changes, including the installation of equipment that can monitor for or protect against incidents occurring.
	Is the building sole occupancy or shared with others?	Working in multi-occupied premises can affect security or introduce additional risks that are brought about by non PHE activities or business.
	Who are the other occupants and what is the nature of their business?	Assess the risks associate with multi occupancy, non-PHE occupants and their business.
	Are there any known risks from the other occupants or their business e.g. do they use or store hazardous materials or does the business itself contribute to increased risks?	Hazards can increase the likelihood of occurrence of an incident that impacts PHE.
	Does PHE have on site a local IT / server room and that is segregated from areas occupied from staff?	Server rooms should be separate and secured with access controls enabling only staff to have access that routinely have a need to do so.
	Are the server room walls solid and built from floor slab to ceiling slab?	For both security and fire containment and suppression, server room walls should be built from floor slab to ceiling slab, not only to the suspended / false floor or ceiling level (refer to ICT and Estates & Facilities as appropriate). Appropriate 'stopping' should also be in place so as to protect the server room, the equipment and external space.
	Is a fire suppression system installed and maintained?	ICT services are now a necessity for most functions to be able to be performed in modern industry, it is therefore recommended for these assets to be protected effectively.

Risk Type	Risk Sub-heading	Examples
	What type of suppression system is installed (e.g. reduced oxygen)?	Suppression systems should be contained to the area in which they are designed to protect and should be prevented from ingress or contamination of other areas, especially those occupied by staff, visitors etc.
	Are ICT systems actively monitored and alarmed to alert at the time of interruption or failure?	Automatic system alarms and monitoring should be in place to detect and early-alert failures or performance degradation.
	Consider the utility services to the building; are there any critical services that require a gas supply? If so, is there a single supply line?	What is the risk of likelihood of interruption and the level of risk associated with this and what will be the impact of interruption?
	Is the building at risk of frequent power interruptions?	Is there a history of regular or frequent power interruptions, if so, is there a common cause and can this be mitigated?
	Is there a single electricity supply to the building and if so is this a single point of failure	Consider the impact of power failures and whether some or all of the following are required: Dual diversely routed power supply; uninterruptable power supply for critical or all equipment and services; Back-up generator(s). Investigate the schematic of the services with suppliers to identify actual or near single point of failure.
	Are critical services protected by UPS?	Are local IT systems protected by UPS? For how long is this designed to last e.g. to enable controlled close down or ongoing maintenance of the service? Is UPS maintained in accordance with manufacturers / suppliers instructions?
	Is a standby generator ready for providing backup power supply?	What is the capacity i.e. all or only critical equipment, services and lighting? How long can the generator run for without needing to be refuelled?
	Is the standby generator tested regularly (refer to Estates and Facilities or site manager?	Regular testing must be completed and fuel stocks replenished. If diesel powered, be aware of the risk from fuel hygroscopy.

Risk Type	Risk Sub-heading	Examples
	What is the adequacy of fuel stocks for standby generators and can at least critical activities be maintained as required by the current National Risk Assessment Planning Assumptions	H31 - Actual or threatened significant disruption to fuel supplies including as a result of industrial action by tankers drivers or refinery staff, or blockade at key refineries/terminals by protestors ➢ October 2016 = organisations now have to plan on how they can now maintain 10 days fuel supplies for essential service delivery. This is the government expected level of BC H41 - Total failure of UK National electrical Infrastructure ➢ October 2016= Organisations are to plan for a 14 day power outage
	Are any critical functions dependent on a reliable water supply?	Loss of water supply can introduce health and safety dimension due to the impact on bathroom or cleaning facilities. It is important also that availability of refreshments can be maintained.
ICT	Consider all systems and services and assess the risks that may be associated with them	Systems and services that are most critical should have the highest level of resilience associated with them to mitigate the risk of interruption. Consider Recovery Time Objectives and whether contracts, SLA, OLA specify these requirements and what testing has been conducted to demonstrate that these RTO and RPOs can be met.
	Are data backups regularly taken and copies stored securely off-site?	Back-ups may include replication between servers in different locations rather than necessarily physical back up to tape etc. What is the Recovery Time Objective and does this meet your operational requirements? Recovery Time Objectives must consider the corporate priorities.
	Is the WAN resilient, having at least 2 network connections and are these diversely routed?	It should be understood if there is a single point of failure or what WAN resilience exists to aid contingency strategy. Investigate the topography of the services with ICT or if appropriate, directly with suppliers to identify actual or near single points of failure.

Risk Type	Risk Sub-heading	Examples
	Is the LAN resilient such that not the whole building / site can be impacted by a LAN failure?	It is recommended that the LAN should be resilient and not dependent on single components, i.e. user connections should be shared across multiple switches etc.
Local Environment	Is the building in a flood plain?	Is there a risk of flooding: Fluvial (river), Pluvial (surface water); or coastal (usually sea water)?
	How is and can the site be accessed e.g. is there more than one road or route in and out?	Business parks especially can have been developed in such a way that there is only a single access route by road, although there may be multiple footpaths or cycle-ways.
	What transport options are available locally to enable staff and visitors to be able to travel to and from site?	What are the risks to disruption to modes of transport? If there are options for travel then this can reduce the risks.
	Is there adequate parking available, including secure parking for bicycles?	Especially if options for travel are restricted, adequate car parking is essential although from an environmental and sustainability perspective, cycling and walking, as the most common forms of low carbon options, should be supported and promoted.
	Is there any gas or oil storage facility nearby?	Consider the security of possible threat sites and the controls in place.
	Is there an electricity sub-station nearby?	Consider the security of possible threat sites and the controls in place.
	Do high voltage power cables run overhead or nearby?	Consider the risks associated with these especially related to severe weather.
	Is the site or building under a flight path?	Although aviation is a 'safe' mode of transport, when accidents do occur, the effects can be significant. Are there any risks associated, especially during take-off or landing sequences? Is there any risk of disruption from excessive noise?
	Does a rail line run next to or near by the building?	What is the position and elevation of this relevant to the building?

Risk Type	Risk Sub-heading	Examples
	Does a motorway or major road run next to the building?	Although statistics indicate that motorways and other major roads are safer than more minor roads, they still pose a threat and accidents, when they do occur, can be major, causing severe disruption and that can include wider impact to the surrounding area. Furthermore, motorways and other major roads are more likely to be used by HGV and vehicles that carry potentially hazardous products.
	Consider tall trees that may be a hazard during high winds or adverse weather conditions	Risk of disruption to transport and travel and can affect power lines and communications.
	Consider geohazards such as: coastal erosion; collapsible or compressible ground; ground sinking and swelling; landslides; seismic hazard; soluble rocks. There is a wide difference of likely impact across different regions, some being more susceptible than others. (See "additional information sources" for useful web links).	Is there a recognised risk of disruption? Ensure that such hazards are identified, assessed and planned for, including minor disruption through to unavailability of site or facilities should a risk materialise.
	Crime	Consider risk of the prevalence of crime in the area. This may be in many forms such as theft, vandalism, crime against the person etc. being aware of the risks associated with crim can enable informed decisions to be taken as to whether the location is appropriate for PHE to have a facility and if so, what plans can be implemented to manage or mitigate the threats
Travel and Transport	Consider the likelihood of disruption to transport systems (refer to environmental risks). These should include road, and rail.	Assess for available options, reliability of services, single points for possible disruption.

Risk Type	Risk Sub-heading	Examples
	Assess the risks of disruption to all dependent users of transport systems, including staff, suppliers, and other stakeholders and partners.	What is the likelihood for disruption to transport systems and the impact in terms of unavailability of staff, deliveries of supplies ability to provide services? Assess what stock of critical supplies should be held so as to mitigate the effects of possible disruption and also consider the effects of a strategy to rely on 'Just In Time' supply.
Supply-chain	Have key or critical external and internal suppliers been identified.	Has the impact of a critical supplier failure been assessed? Are appropriate SLA / OLA in place? Are contingency plans shared with critical suppliers and has assurance of their capability been measured and proven through exercise?
	Supplier strategy	Single suppliers can be an opportunity to drive down cost on the basis of economies of scale however there is a risk that if supplier should cease trading or choose to stop producing or supplying a particular product or service. Multiple suppliers require more resource to manage the relationships but offer the opportunity to drive down cost through competition and reduce the risk of likely disruption.
HR / Staff	Are staff trained in personal security and safety?	Maintaining confidentiality, discretion, awareness of social engineering, the use of social media etc.
	Cross training and Succession planning	Knowledge should be shared to ensure that there is no dependency on individual members of staff. Resources should be managed in such a way so as to ensure that critical services can continue to be delivered in line with identified key priorities. It is not always possible to know when a key member of staff will not be available and therefore never too early to take steps to protect against this risk.
	Skills database	A record of required skills and staff that have been trained or hold those skillsets should be maintained. ESR has capability to record skillsets, competencies, etc. under the 'Talent profile'.

Risk Type	Risk Sub-heading	Examples
	Critical services should be mapped to the skills database	To assure maintenance of at least the critical priorities, key skills should be mapped to critical services and the individuals that hold those skillsets. This approach supports both Business continuity and health emergency planning and response.

ADDITIONAL INFORMATION SCOURCES

The following web-sites can be interrogated for information; including environmental matters relating to a neighbourhood check of the local area e.g. crime levels and other threats that will support the completion of a BCM focused risk assessment.

http://www.findahood.com/articles/guides/neighbourhood-statistics-up-my-street/44

http://www.police.uk/

https://www.gov.uk/government/organisations/ministry-of-housing-communities-and-local-government

https://www.gov.uk/government/organisations/environment-agency

http://www.highways.gov.uk/traffic-information

Flightradar24.com - Live flight tracker!

http://www.bgs.ac.uk/home.html?src=topNav

Also refer to Local Authority, utility provider websites.