North Hampshire
Clinical Commissioning Group

NORTH HAMPSHIRE CLINICAL COMMISSIONING GROUP

BUSINESS CONTINUITY MANAGEMENT POLICY (COR/017/V3.00)

Subject and version number of document:	Business Continuity Management Policy and Plan V 3.00
Serial Number:	COR/017/V3.00
Operative date:	31 March 2017
Authors:	R Clarke, Head of Business Development, North Hampshire CCG Jayne Tunstall, North East Hampshire & Farnham CCG Deborah Broughall, Corporate Project Manager, North Hampshire CCG
Links to other Policies:	NHCCG Incident Response Plan NHCCG GBAF and Risk Management Policy
Review date:	This document will be reviewed after 12 months and then every two years thereafter.
For action by:	This policy applies to all directly and indirectly employed staff and other persons working within the CCG.
Policy statement:	CCGs are Category 2 responders and are required by the Civil Contingencies Act 2004 to have Business Continuity Plans, which have been exercised and reviewed on a regular basis. There also requirements in both the Use of Resources and Information Governance Tool Kit to demonstrate that effective business continuity plans and testing are in place.
Responsibility for dissemination to new staff:	The Business Development function of the CCG will disseminate this policy in the first instance and then be published on the CCG's website at: http://www.northhampshireccg.nhs.uk/documents/
Training Implications:	Staff will receive training on this policy on induction and through the course of mandatory training.
Further details and additional copies available from:	All CCG policies ratified by the Governing Body will be published at: http://www.northhampshireccg.nhs.uk/documents/
Equality Analysis Completed?	No
Approved by (date):	V2.00: Integrated Governance Committee V3.00: Executive Management Team
Original ratified by (date):	Governing Body 31/03/2015

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	N/A
Website	Location in FOI Publication Scheme	http://www.northhampshireccg.nhs.uk/documents/
Keywords:	Business Continuity, Incident, EPPR	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1		Appendix	Business Continuity Plan added as Appendix	
2		Sec 8.3 page 5	Wording changed "…..in the Business Continuity Plan"	
3		Sec 10.2 page 6	All exercises will be recorded in the Business Continuity Management Log	
4	31.03.2017	All	Document updated to reflect current organizational structure and roles.	28.03.17
5	31.03.17	Appendix C	Business Continuity Plan removed from policy document and reviewed independently. To be published in tandem with policy.	28.03.17

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
V3.00	March 2017	D Broughall	NHCCG Executive Management Team	See amendments summary

CONTENTS **Page**

Business Continuity Management Policy

NORTH HAMPSHIRE CLINICAL COMMISSIONING GROUP

BUSINESS CONTINUITY MANAGEMENT POLICY AND PLAN
(COR/017/V3.00)

1. Introduction

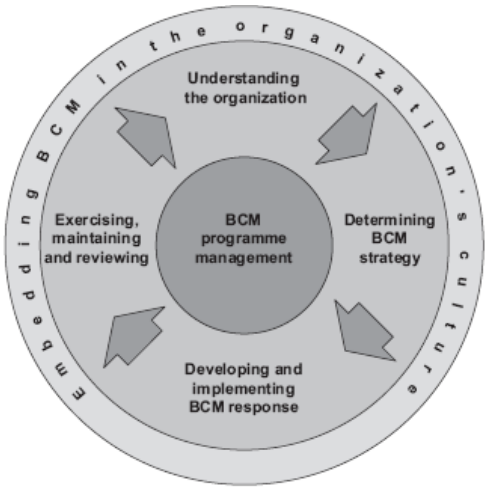
1.1 All Category 2 responders are required by the Civil Contingencies Act 2004 to have Business Continuity Plans (BCPs), which have been exercised and reviewed on a regular basis. These plans sit alongside the Incident Response Plan for NHS North Hampshire CCG. There also requirements in both the Use of Resources and Information Governance Tool Kit to demonstrate that effective business continuity plans and testing are in place.

1.2 Depending on the type of incident occurring, both the Incident Response and the Business Continuity Plans may be activated to deliver the required external and internal response. e.g. if North Hampshire was faced with a water contamination incident both the population of Hampshire and the CCG would be affected. The activation of the plan ensures they fulfil their requirements as part of the Civil Contingency Act and also the organisation can continue to deliver its ordinary business. Local Business Continuity plans need to be aligned to the external Hampshire Local Resilience Forum (HLRF) plans.

1.3 Business Continuity Plans on some occasions may be activated when a major incident response would not be required e.g. if the CCG Head Quarters building suffered a fire, only the CCG would be affected and only an internal business continuity response would be needed.

1.4 With the introduction of the British Standard BS25999, each organisation needs to be able to demonstrate that Business Continuity Management (BCM) has been established and embedded across the organisation. The diagram (Figure 1) below illustrates the BCM Cycle to develop a robust BCM culture across the organisation. (See section 7 for more detail)

Figure 1



2. Aim

2.1 NHS North Hampshire CCG will develop and implement robust BCM plans across the whole organisation so that the strategic and tactical capability of the organisation is maintained, it can respond appropriately to incidents and business interruptions, and enables the organisation to continue its business critical functions at an acceptable pre-defined and agreed level.

3. Objectives

3.1 To achieve this aim, NHS North Hampshire CCG will:

- adopt a holistic management process that identifies potential threats and the impact they may have on the functions of the CCG
- provide a framework for resilience, with the capability for an effective response safeguarding the interests of the CCG's key stakeholders and its reputation
- identify their critical activities for each of the functions of the CCG ie. those activities which have to be performed to deliver the critical services. This process will enable the CCG to meet its most important and time sensitive objectives
- identify the maximum tolerable period of disruption after which the CCG's viability and reputation will be irrevocably threatened if delivery cannot be resumed
- establish robust recovery time objectives for the resumption of activities following the incident or disruption. The recovery time objective has to be less than the maximum period of tolerable disruption. Solutions have to be provided which have undergone cost benefit analysis to measure the cost of implementing that solution compared with the benefits delivered to continue with day to day business
- rehearse all business continuity plans annually in tabletop format in part or whole to ensure they contain the appropriate information that produces the desired result when activated
- ensure every three years that the CCG will carry out a full live test of the Business Continuity Plans

4. Scope

This Business Continuity Management Policy and Plan is to be applied to all services and activities of the CCG with no limitations or exclusions. In addition, the CCG will obtain assurances from its key contractors, providers and suppliers of their effective business continuity arrangements.

5. Definitions

5.1 **Business Impact Analysis:** The process of identifying business functions and the effect a business disruption will have on them.

5.2 **Critical Activities:** Those activities whose loss would have the greatest impact in the shortest time and need to be recovered most rapidly.

5.3 **Risk Assessment:** Process of risk identification, analysis and evaluation using the Risk Matrix.

5.4 **Business Continuity Strategy:** A business continuity strategy considers the alternative operating methods that can be used to maintain an organisation's critical activities after an incident to an acceptable minimum level.

5.5 **Maximum Tolerable Period of Disruption (MTPoD):** This is defined as the duration after which an organisations' viability would be irrevocably threatened if product and service delivery cannot be resumed.

5.6 **Recovery Time Objectives (RTO):** This is defined as a target time for recovery for each activity.

6. Roles and Responsibilities

6.1 This policy will be approved by the Finance and Performance Committee on behalf of the CCG Governing
Body. The key responsibilities across the organisation are outlined below:

6.1.1 The Executive Management Team

The Executive Management Team will:

- authorise the provision of the resources needed to establish, implement, operate and maintain Business Continuity Plans
- support the Emergency Planning Lead to be responsible for co-ordinating the implementation of the Business Continuity Plans irrespective of other responsibilities
- determine the acceptable level of risk in relationship to Business Continuity and management of business continuity risks
- receive annual reviews following management reviews of the Business Continuity Plans
- communicate the Business Continuity Plans to its stakeholders
- communicate to the organisation via the Accountable Officer the importance of:
    - meeting Business Continuity management objectives
    - conforming to the Business Continuity Management Policy
    - continuous improvement

6.1.2 Emergency Planning Lead

The Emergency Planning Lead will:

- be responsible for ensuring an effective system is in place for monitoring, reviewing and exercising business continuity plans
- provide staff with support to develop their business continuity plans
- provide regular training to staff on business continuity
- provide reports on a quarterly basis to the Finance and Performance Committee on business continuity planning

6.1.3 '**Heads of'**

The 'Heads of' the different functions of the CCG will:

- develop business continuity plans for their services
- be responsible for reviewing and monitoring business continuity plans
- be responsible for exercising their business continuity plans
- be responsible for assuring the attendance of staff on relevant business continuity training

6.1.4 **Staff**

All staff will ensure:

- that they remain cognisant of the business continuity plans and their role within their service
- assist in the development and testing of business continuity plans for their service

7. Risk Assessments

7.1 All business continuity plans should be risk assessed using the risk matrix in the Governing Body Assurance and Risk Management Framework at http://www.northhampshireccg.nhs.uk/documents/ . The level of risk needs to be identified as part of the Business Impact Assessment process (**Appendix A**) and included for each critical activity in each plan. Once the plan has been completed a residual risk should be completed using the same methodology. The risk assessment methodology will enable the CCG to understand what are the specific threats and vulnerabilities to all its critical services and this will help the management review process to decide if this is an acceptable level of risk and whether additional resources need to be allocated which may be provided by suppliers or other partners. This will ensure risk 'treatments' (the way of dealing with risks) are relevant to each critical activity.

8. The Business Continuity Management (BCM) Cycle

The Business Continuity Management Cycle is a phased and iterative process that consists of stages (Civil Contingencies Act Guidance 2004):

8.1 Stage One: Understand the Organisation

In this initial stage it is important that a full analysis is done to ascertain what exactly the organisation does to enable the business continuity to be aligned to the organisations objectives, obligations and statutory duties. Once the organisation functions have been identified, a Business Impact Assessment (BIA) Tool (**Appendix A**) needs to be completed with a supporting risk assessment process. This identifies the critical activities which would have the greatest impact in the shortest time should an incident occur. In addition, there needs to be a clear indication in this process as to the time point when these loss of activities occur.

8.2 Stage Two: Determining a BCM Strategy

The business continuity management strategy enables staff to consider what alternatives can be put in place to manage business continuity. This can be done by teams assessing their services either by brainstorming ideas or reviewing ideas using a SWOT Analysis. They need to consider whether people, premises, technology, supplies or other partners can provide their alternative options.

8.3 Stage Three: Developing and Implementing a BCM Response

This stage involves the development and implementation of appropriate plans to ensure critical functions can be maintained. The CCG will utilise its normal command and control structures to support this stage in the process as described in the Business Continuity Plan.

The plans should identify how the event will be managed and identify the process and key ac tivities to be followed with clearly understood aims and objectives which prioritise each critical activity which needs to be recovered. This will include the process of recovery. It will identify the key personnel to deliver the response and key decision maker to ensure implementation. The recovery time objectives should be included in the BIA to support this process and include maximum tolerable period of disruption.

The plan should be short and simple to use but actions detailed need to be realistic, with key tasks assigned to specific roles. These roles need to ensure that the aims and objectives of the plan are achieved. All plans should have a version number and be reviewed on an annual basis. All plans where possible should include alternative working locations, up to date contacts both internally and externally that will be required to support the response. Where additional resources may be required they should be documented in the plan. All lines of communication need to be detailed so that staff are clear who needs to be informed of the incident. All plans should be stored on the CCG shared drive/business continuity plan/relevant department and a hard copy is retained by the Emergency Planning Lead.

8.4 Stage Four: Exercising, Maintaining and Reviewing

All plans should be exercised on an annual basis to ensure that they are maintained and reviewed. The Emergency Planning Lead has a responsibility to ensure this occurs.

9. Activation of the Business Continuity Plans

Business Continuity Plans will be activated in response to either a local or multi-agency major incident. Sometimes Business Continuity Plans are activated informally ie. to manage a short term staff shortage but all activations will be instigated by the Accountable Officer or the deputising 'Head of'. They will advise their staff to activate their plans.

When Business Continuity Plans are activated it is important that all staff receive effective communication about the incident and the response being taken. Communications will be via the following means:-

- Email to all staff if internet access is still available
- Telephone communication to all staff
- Information on the website if available
- Team meetings

10. Exercising

10.1 All Business Continuity Plans need to be exercised on an annual basis. This may occur either through a table top exercise or through activation of a major incident or a more localised service related incident. The exercising of plans may be part of a wider major incident exercise across the organisation. The exercise programme will ensure all business continuity arrangements are validated and provide assurances that arrangements in place met the requirements of the organisations. The exercise programme has full support from the senior management team.

10.2 All exercises will be recorded on the Business Continuity Management Log.

10.3 All aims and objectives of the exercise will be fully documented and a report completed to the risk management committee which will demonstrate the organisations achievements of those aims and objectives. This report will include any relevant actions that are required and identify lessons learned and good emergency practice and any feedback from observers at an exercise or stakeholders involved in the incident.

11. Reviewing

11.1 All business continuity plans need to be reviewed on an annual basis. This may be via the exercise programme or post incident or as part of the annual review process. The Emergency Planning L ead will manage the Business Continuity review process via the Business Continuity Management Log.

12. Recovery

12.1 Following activation of Business Continuity Plan, a stage of recovery needs to take place to ensure that services return fully to normal business. This may include a stand down process which is documented in the business continuity plan and this will determine how each activity is performed once things are resumed.

12.2 The plan needs to include recovery timescales for each specific level and also the specific resources required which may include services or resources from other providers. This will be achieved by effective relationships with key stakeholders and external parties which should be established prior to any incident.

12.3 The effectiveness of the recovery of clinical activities will be determined by evaluation the recovery against the recovery time objectives in the Business Impact Assessment.

13. Training and Awareness

13.1 The CCG will ensure that all staff who have been assigned responsibilities defined by the Business Continuity Management Policy and Plan are competent to perform the required tasks by:

- determining necessary competencies to enable staff to perform work related to Business Continuity Management
- provide training via a number of platforms e.g. workshops, external courses and inductions
- evaluate the effectiveness of the training provided, via evaluation reports, one to one sessions conducted by management
- training needs analysis to be conducted on staff assigned BCM roles and responsibilities
- provide the Finance and Performance Committee with annual review of training that has taken place and the impact it has had

13.2 In addition, training and education programmes need to highlight the importance of meeting Business Continuity Management objectives and conforming to the CCG policy.

14. Embedding Business Continuity into the CCG Culture

14.1 The CCG will ensure that Business Continuity Management becomes part of its core values and effective management. To provide this the CCG will:

- raise, enhance and maintain awareness by the implementation of an ongoing Business Continuity education and information programme for all staff via the Mandatory training. This awareness can be raised by workshop sessions or via individual Directorate team briefings

- an evaluation process will be established to monitor its effectiveness

15. BCM Documentation and Records

15.1 The CCG will hold the following BCM System documentation:

- Business Continuity Plan template (**Appendix B**)
- Business Continuity Policy Plan v2.10 (March 2017)
- Incident Response Plan
- up-to-date contact and mobilisation details for relevant agencies, organisations and resources which may be required to support the response strategy
- test schedule and results/test actions register
- training programme attendance
- response structure
- any other documents in support of Business Continuity Plan implementation

15.2 Records will be established, maintained and controlled to provide evidence of the effective operation of Business Continuity Plans.

16. Audit

16.1 Business Continuity plans will be reviewed/audited annually or after any incidents that result in the plans being activated. Staff involved in the incident will evaluate the plan that was activated and whether the policy was followed. An audit of review is monitored via the Business Continuity spreadsheet – this is managed by the Emergency Planning Lead on behalf of the organisation. In addition, BCM may become part of the internal audit programme.

16.2 Training will be evaluated to demonstrate effectiveness.

17. Policy Review

This policy will be reviewed after 12 months and subsequently every 2 years or when any significant changes in business continuity occur.

18. References

NHCCG Incident Response Plan
British Standard BS25999 Business Continuity Civil Contingencies Act 2004
NHCCG Governing Body Assurance and Risk Management Framework

Appendix A

Business Impact Assessment Tool

1. Department / Team / Service Information

1.1	**Name and description of service and location:**	
1.2	**Name of author:**	
1.3	**Job title of author:**	
1.4	**Author telephone and e-mail:**	
1.5	**Date:**	
1.6	**Business Continuity Lead:**	

2. Prioritised Activities

Please identify the prioritised activities for your department/team/service. Prioritised activities are those critical to the department that, if lost, would mean that the service would cease to exist and to which priority must be given following an incident in order to mitigate impacts. Under BS 25999 they were referred to as critical or time-critical functions. Activities should be categorised into:

- highest priority activities which must be continued, or
- activities which could be scaled down if necessary, or

- activities which could be suspended if necessary

2.	List the prioritised activities undertaken	Tick as appropriate			Responsible Officer
		Highest priority and must continue	Can scale down	Could suspend	
2.1					
2.2					
2.3					
2.4					
2.5					

It may be that an activity can be suspended initially but later it becomes a priority. For example a task that must be completed at certain intervals rather than on continuous basis. Use the table below to record the impact of the loss of an activity for different lengths of time and identify where this length of disruption would be acceptable to the organisation and its stakeholders.

Prioritised	Impact of disruption to prioritised activities											Tolerable
	Length of disruption	Category of Impact (please tick)								Comment	Score[1]	
	1=Insignificant, 2=Minor, 3=Moderate, 4=Significant, 5=Catastrophic											
Activity		**Financial**	**Service delivery**	**Reputation**	**Health and safety**	**Information security**	**Statutory or regulatory duty**	**Business objective**	**Supplier**			**(Yes or No)**
2.1	Up to ½ day											
	½ day to 1 day											
	1 day to 1wk											
	1wk to 1mth											
	1mth to 3mths											
2.2	Up to ½ day											
	½ day to 1 day											
	1 day to 1wk											
	1wk to 1mth											
	1mth to 3mths											
	Up to ½ day											

2.3	½ day to 1 day												
	1 day to 1wk												
	1wk to 1mth												
	1mth to 3mths												
2.4	Up to ½ day												
	½ day to 1 day												
	1 day to 1wk												
	1wk to 1mth												
	1mth to 3mths												
2.5	Up to ½ day												
	½ day to 1 day												
	1 day to 1wk												
	1wk to 1mth												
	1mth to 3mths												

Some activities will be of greater priority at different points in the year, for example, certain financial processes will be need to be prioritised at financial year end.

Do your prioritised activities vary at different times of the month or year? Please explain

3. Business Continuity Risks

The table below includes a number of scenarios that present a risk to the organisation. Consider these scenarios and decide whether or not they present a risk to the prioritised activities that you provide. For example, if your service is paperless it is unlikely that a loss of paper records will have an impact. Please add any other scenarios that are relevant to your service.

Ref	Hazard of threat	Y or N	Why?
3.1	Fire or flood		
3.2	Loss of electronic records		
3.3	Loss of paper records		
3.4	IT systems/application failure		
3.5	Mobile telephony failure		
3.6	Major IT network outage		
3.7	Denial of premises		
3.8	Terrorist attack or threat affecting the transport network or office locations		
3.9	Theft or criminal damage		
3.10	Chemical contamination		
3.11	Serious injury to, or death of, staff whilst in the offices.		

3.12	Significant staff absence due to severe weather or transport issues		
3.13	Infectious disease outbreak		
3.14	Simultaneous resignation or loss of key staff		
3.15	Industrial action		
3.16	Fraud, sabotage or other malicious acts		
3.17	Violence against staff		
3.18	*Please add any other relevant threats*		

Which of the following hazards and threats are relevant to your department or service?

The Civil Contingencies Act (CCA) regulations and guidance (chapter 6, 6.74) identifies five broad strategy options that could be considered when developing your risk reduction strategy:

- **Do nothing:** if the risk is deemed to be acceptable by senior management they may choose to do nothing. This may be suitable for an event with a very low probability of occurrence, such as an earthquake.
- **Changing, transferring or ending the process:** consideration must be given to fulfilling any statutory duties and any insurance or reputation ramifications as a result of a third party failing to deliver.
- **Insurance:** may provide some financial cover but cannot protect the reputation of the organisation and other associated losses.
- **Loss mitigation:** putting in place procedures to eliminate or reduce the risk, such as installing smoke alarms.
- **Business Continuity Planning:** putting in place arrangements that allow for the recovery and continuity of key business processes within a pre-identified time frame.

The table below is based on the NHS England Risk Register from the *Risk Management Policy and Procedures.* Please complete this table against the risks you have identified above. Please use the reference number from the left hand column of the table above in order to complete the table.

Department/Team/Service Risk Assessment										
Ref Eg 3.1	**Date reviewed**	**Existing controls**	**Impact**	**Likelihood**	**Total Risk Score**	**Senior Responsible Officer**	**Mitigating Actions**	**Risk Owner**	**Date for review**	**Residual risk**

The Total Risk Score is calculated by multiplying the **Impact x Likelihood** using the table below:

		Likelihood of Occurrence				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Certain
Impact	5 Catastrophic	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

Appendix B

Business Continuity Planning Template

The purpose of this section is to identify what is required in order to deliver your prioritised activities and it is this information that will form the basis of the recovery plan. This section must be completed where the risks to the service cannot be removed or reduced to an acceptable level through other mitigating actions.

Prioritised Activity	Recovery time objective (RTO)[2]	PEOPLE required to restore the service	PREMISES required to restore the service	TECHNOLOGY/SUPPLIES required to restore the service	INFORMATION required to restore the service	Recovery Point Objective (RPO)[3]	PROVIDERS required to restore the service	PROFILE & STAKEHOLDERS required to restore the service	Maximum Tolerable Period of Disruption (MTPoD)[4]
2.1									
2.2									
2.3									
2.4									
2.5									

You can refer to the table below.

[2] The RTO is the period of time following an incident within which an activity must be resumed
[3] The RPO is the point to which information used by an activity must be restored to enable the activity to operate on resumption

[4] The MTPoD is is the time frame during which a recovery must be affected before an outage compromises the ability of to achieve the organisation's business objectives and/or survival, also referred to as the Maximum Acceptable Outage.

PEOPLE	PREMISES	TECHNOLOGY/SUPPLIES	PROVIDERS	PROFILE & STAKEHOLDERS
Key Staff : What staff do you require to carry put your key functions? Can staff be contacted out of hours? Could extra capacity be built into your staffing to assist you in coping during an incident?	**Building :** What locations do your department's key functions operate from? (Primary site, alternative premises) Could you operate from more than one premise? Could you relocate operations in the event of a premise being lost or if access was denied?	**IT :** What IT is essential to carry out your key functions? Is data backed-up and are back-ups kept off site? Do you have any disaster recovery arrangements in place?	**Reciprocal Arrangements:** Do you have any reciprocal agreements with other organisations? Do you have agreements with other teams, departments or organisations regarding staffing and the use of facilities in the event of an incident?	**Reputation :** Who are your key stakeholders? How could reputational damage to your team, department or organisation be reduced? How could you provide information to staff and stakeholders in an emergency

Skills / Expertise / Training : What skills / level of expertise is required to undertake key functions? Could staff be trained in other roles? Could other members of staff undertake other non- specialist roles in the event of an incident?	**Facilities :** What facilities are essential to carry out your key functions? Are any of your facilities multi-purpose? Are alternative facilities available in the event of an incident?	**Documentation :** What documentation / records are essential to carry out your key functions, and how are these stored? Is essential documentation stored securely (e.g. fire proof safe, backed-up)? Do you keep copies of essential documentation elsewhere?	**Contractors / External Providers :** Do you tender key services out to another organisation, to whom and for what? Do you know of alternative contractors or are you reliant on a single contractor? Do your contractors have contingency plans in place? Could contractors be contacted in the event of an incident?	**Legal Considerations :** What are your legal, statutory and regulatory requirements? Do you have systems to log decisions, actions and costs in the event of an incident

Minimum Staffing Levels : What is the minimum staffing level with which you could provide some sort of service? What is the minimal staffing level to continue to deliver your key functions at an acceptable level? What measures could be taken to minimise impacts of staff shortfalls?	**Equipment / Resources :** What equipment / resources are required to carry out your key functions? Could alternative equipment / resources be acquired in the event of an incident / disruption? Could key equipment be replicated or do manual procedures exist?	**Systems & Communications :** What systems and means of communication are required to carry out your key functions? Are your systems flexible? Do you have alternative systems in place (manual processes)? What alternative means of communication exist?	**Suppliers :** Who are your priority suppliers and whom do you depend on to undertake your key functions? Do you know of suitable alternative suppliers? Could key suppliers be contacted in an emergency?	**Vulnerable Groups :** Which vulnerable groups might be affected by failing to carry out key functions? How could vulnerable groups be contacted/accommodated in the event of an incident?