Cabinet Office

Section C: Practical Guidance

Guide 1: Guidance on Natural Hazards

Guide 2: Checklist for Infrastructure Owners

Guide 3: Guidance on Information Sharing

Guide 4: Guidance on Assessing Dependencies

Guide 1: Guidance on Natural Hazards

This guidance has been produced with the assistance of the National Risk Assessment Team (situated in the Cabinet Office), the Met Office, Environment Agency and the British Geological Survey.

Purpose

The guidance provides infrastructure owners and operators, and all those with a stake in the delivery of essential services (including regulators, suppliers, and emergency planners), with reasonable worst case scenarios for those natural hazards most likely to significantly disrupt the UK's critical infrastructure. These descriptions should frame their collective efforts to improve the cross sector resilience of critical infrastructure to natural hazards.

Background

As the summer floods of 2007 showed, the scale of the impact of natural hazards on society is influenced by the degree of disruption to critical infrastructure that occurs, and the subsequent effect on the delivery of essential services. For example, the impact of the floods of 2007 on society was exacerbated by the loss of Mythe Water Treatment Works, which left 350,000 people (not all of whom resided within the flooded areas) without drinking water supplies for 17 days.

In the recent past, society has been disrupted by natural hazards on a regular basis. For instance, since the floods of 2007 there has been severe flooding in Cumbria (2009), cold spells with snow (late 2009 and early 2010), and volcanic ash (also in early 2010). All of which exposed weaknesses in the ability of the UK's critical infrastructure to prepare for, respond to and recover from natural hazards, including:

- a lack of knowledge (and a lack of understanding of the cross sector vulnerabilities of elements of critical infrastructure) concerning the type and severity of natural hazards of greatest concern, and the linkage between different natural hazards;

- a lack of understanding of the potential impacts of natural hazards on critical infrastructure;
- different levels of resilience to natural hazards in organisations supplying essential services; and
- poor sight of the resilience of key supply chains to natural hazards, and the impact that any vulnerabilities might subsequently have on critical infrastructure.

This guidance seeks to address these gaps by providing hazard scenarios for the most likely hazard events in the UK.

Scope

The hazard descriptions are drawn from the National Risk Assessment. They set out the hazard events that might have a major impact on all, or significant parts of, the UK, and for which Government, emergency planners and infrastructure owners and operators can reasonably be expected to plan for.

Each scenario is the product of a national assessment of the likelihood and impact of a particular hazard on the UK's critical infrastructure. The scenarios describe reasonable (not absolute) worst case events for the UK as a whole, and as a result, there will be local variations.

It is not a risk assessment, nor a planning document; Infrastructure owners, regulators, suppliers and local emergency planners are best placed to work together to understand the impact of natural hazards on their organisations, supply chains and wider communities, and, therefore, are also best placed to identify priorities and exploit synergies for delivering improvements in resilience.

Next steps for infrastructure owners and operators, emergency planners and regulators

Infrastructure owners and operators should use this guidance as the basis for discussions with resilience partners (including regulators, suppliers, customers and emergency planners) aimed at collectively and sustainably improving the cross sector resilience of critical infrastructure to natural hazards.

It is intended that such analysis becomes embedded into existing corporate and community level risk assessment and mitigation processes. For example, it is entirely possible that, over time, knowledge of a particular hazard and/or the importance of a particular site can increase thus creating new risks that were not previously considered. It is therefore important for infrastructure owners and their resilience partners to regularly reappraise the risks posed by the full range of natural hazards.

Structure

The guidance is divided into two sections:

G1.1 Explores the interconnectivity of natural hazards and provides reasonable worst case scenarios for those hazards listed within the National Risk Register (2010). It also includes an analysis of additional hazards, volcanic ash , severe volcanic activity and severe space weather, because of their potential impact on critical infrastructure.

The type and severity of 'primary' natural hazards are listed with related weather effects, and potential impacts on infrastructure.

G1.2 Lists some geological hazards for infrastructure owners and resilience partners that can also affect critical infrastructure, depending on the specific characteristics of their location.

Infrastructure owners should consider the impact on the delivery of their essential services if an event similar to the scenarios / hazards described in G1.1 and G1.2 occurred. The impact assessment should also consider potential disruption to supply chains and distribution systems, particularly where other assets of critical infrastructure are part of the chain.

G1.1 Hazard Descriptions

The majority of natural hazards within this annex are drawn from the National Risk Assessment, which seeks to capture the range of emergencies that might have a major impact on society including: coastal flooding, inland flooding, storms and gales, low temperatures and heavy snow, heat waves and drought.

Figure G1.1 illustrates the unclassified summary of the risks, as presented in the National Risk Register.[1]

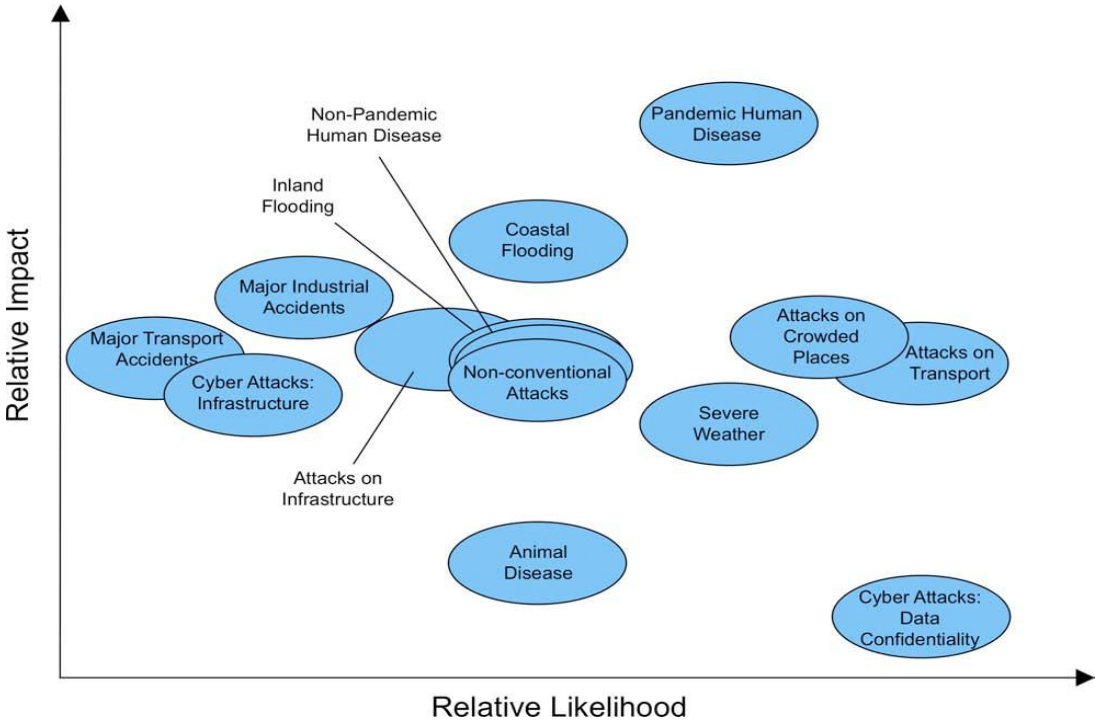

Figure G1.1: An illustration of the high consequence risks facing the United Kingdom

Typically, a single natural hazard can carry a variety of challenges for infrastructure owners and planners. For example, a prolonged period of dry weather also carries the risk of thunderstorms and flash flooding; warmer weather, following a cold spell with snow, causes rapid thawing, which leads to flooding. Table G1.1 shows the relationship between different natural hazards.

[1] National Risk Register: www.cabinetoffice.gov.uk/content/risk-assessment

Table G1.1: The connection between different natural hazards events

Source	Initial Consequences	Knock –on consequences
Storms and Gales	Strong winds (Gales) Tidal surge Snow Lightning Heavy Rainfall Tornadoes Hail	River and coastal flooding Surface water flooding Land instability Wildfire
Prolonged period of hot weather	Heat	Thunderstorms Drought Dust/Smog/haze Land instability Wildfire
Prolonged period of dry weather	Reduced Rainfall	Dust/Smog/Haze/fog Reduced ground water flow Water quality Land instability Drought
Excessive cold with snow	Cold Snow	Ice Ice accretion Wind chill Fog Surface water and river flooding (snow melt)

Table G1.2 sets out the reasonable worst case scenarios for the natural hazards, as determined by the 2010 National Risk Register, with the addition of volcanic ash, severe volcanic activity and severe space weather.

Table G1.2: Reasonable worst case scenarios for natural hazards in the UK

Scenario	Reasonable worst case scenario	Other related effects	Potential impacts on infrastructure
Inland flooding	A single massive inland event or multiple concurrent regional events following a sustained period of heavy rainfall extending over two weeks (perhaps combined with snow melt or intense summer rainfall leading to widespread surface water flooding). The event would include major fluvial flooding affecting a large, single urban area. This is broadly regarded as a 0.5% annual probability flood event.	Storms and gales Snow Land Instability (including offshore and submarine) Heavy rainfall	• Loss of primary transport routes • Lack of staff availability • Impaired site access • Loss of power supplies • Loss or contamination of water supplies • Closure of local businesses • Increased demand for emergency power and water supplies • Increased demand for health and emergency services • Loss of emergency services assets
Coastal Flooding	Major sea surge, tides, gale force winds and potentially heavy rainfall. Many coastal regions and tidal reaches of rivers affected. Excessive tide levels and many coastal and/or estuary defences overtopped or failing (breaches). Drains 'back-up'. Inundation from breaches in defence systems would be rapid and dynamic with minimal warning and no time to evacuate. Inundation from over-topping of defences would allow as little as 1 hour to evacuate.	Storms and gales Snow Land Instability (including offshore and submarine) Heavy rainfall.	• Loss of primary transport routes • Lack of staff availability • Impaired site access • Loss of power supplies • Loss of water supplies • Closure of local businesses • Increased demand for emergency power and water supplies • Increased demand for health and emergency services

Scenario	Reasonable worst case scenario	Other related effects	Potential impacts on infrastructure
Windstorm: storms and gales	Storm force winds affecting most of a region for at least 6 hours. Mean speeds in excess of 70mph with gusts in excess of 85mph. Short term disruption to infrastructure including power, transport networks, homes and businesses.	Flooding Land instability Heavy rainfall Wildfire	• Loss of power • Loss of telecoms • Blocked road and train routes and flight disruption
Excessive Cold with Snow and ice	Snow falling and lying over most of the area for at least one week and after an initial fall of snow there is further snow fall on and off for at least 7 days. Most lowland areas experience some falls in excess of 10cm, a depth of snow in excess of 30cm and a period of at least 7 consecutive days with daily mean temperature below -3ºC.	Storms and gales Flooding Land instability Ice Ice accretion	• Loss of primary transport routes • Lack of staff availability • Impaired site access • Loss of power supplies • Loss of water supplies • Closure of local businesses • Increased demand for emergency power and water supplies • Increased demand for health and emergency services

Scenario	Reasonable worst case scenario	Other related effects	Potential impacts on infrastructure
Prolonged Period of Hot / Dry Weather	<u>Hot</u> Daily maximum temperatures in excess of 32ºC and minimum temperatures in excess of 15ºC over most of the region for at least 5 consecutive days. <u>Dry</u> Periodic water supply interruptions for up to 10 months. Emergency Drought Orders in place authorising rota cuts in supply according to needs of priority users as directed by the Secretary of State.	Thunderstorms. Heavy rainfall. Flash Flooding. Drought. Dust. Haze. Smog. Land instability Wildfire	• Loss or significant reduction of water supplies • Slowed rate of sewage flow through the system leading to public health concerns • Reduction in water quality • Temporary loss of primary transport routes • Loss of power supplies • Closure of local businesses • Increased demand for water supplies from all infrastructure sectors including health, agriculture, energy sectors and emergency services • Increased demand for emergency power • Increased demand for health and emergency services
Volcanic ash	Volcanic ash incursions for up to 25 days. The entire UK mainland and potentially other parts of Europe could be affected for up to 10 of these days. A single period of closure within the 3 month eruptive episode may last up to 12 consecutive days, depending on meteorological conditions.	None	• Sporadic and temporary closures of significant parts of UK airspace
Severe volcanic Activity	Severe volcanic eruption, generating large amounts of gas and ash over a five month period affecting UK and northern Europe.	None	• Increased demand for healthcare systems • Closure of UK airspace • Reduced yield from harvests

Scenario	Reasonable worst case scenario	Other related effects	Potential impacts on infrastructure
Severe Space Weather	Resulting from solar eruptions causing rapidly varying geomagnetic fields on earth.	None.	• Disruption to satellite services for several days • Loss of power supplies • Loss of satellite communications and computer based control systems • Disruption to monetary systems • Interruptions to Global Positioning System (GPS) • Disruption to broadcast services • Disruption to aviation sector

G1.2 Other Hazards

Geological Hazards

In general, the UK is a geologically stable region. Large scale incidents, such as earthquakes, no longer significantly affect our country and therefore very few geological hazards feature within the National Risk Register. However, at the local level, risk is determined by the geological characteristics of the specific location under consideration. As a consequence, the impact of geological hazards still carries a significant cost for UK society. For example, the British Geological Survey has estimated that cost of damage to property caused by the swelling and shrinking of clay was in excess of £3 billion for the last decade.

It is therefore important that geological risks are considered as part of a site specific risk assessment.

This section provides an overview of the range of geological hazards affecting the UK and their potential disruption to critical infrastructure.

The following geological hazards can cause damage to buildings, transport networks and power and water supplies through ground movement and / or land instability.

Landslides. The downward movement of ground under gravity. Movement may be relatively slow (slides) or fast (rockfalls) and may also affect flat ground above and below the moving slope. A slope remains stable while its strength is greater than the stress imposed by gravity. Other factors that determine the risk of landslides include the type of geological material; fractures and joints, the angle of the slope, and the position of the water table. Landslide potential is most significant in areas of Scotland, Wales, middle, south west, east and south coast England. Offshore landslides are poorly known, however nearshore occurrences are known in sea lochs where slopes are steeper than the general seabed.

Swelling and shrinking clay. Some rocks that contain clays can increase or decrease in volume as they absorb or lose water. These volume changes can cause either swelling (heave) or shrinking (subsidence) and cause damage to foundations of infrastructure. The potential of swelling and shrinking clay is moderate across the UK but areas of southern and eastern England are particularly at risk.

Soluble rocks. These include salt, gypsum, limestone and chalk and underlie about one fifth of England, parts of South and North Wales and small parts of Scotland. All these rocks can dissolve some very quickly, forming caves and underground cavities that can collapse or allow covering materials to funnel in causing sinkholes and subsidence. Houses and roads can collapse and the problem can be aggravated by flooding and extreme rainfall events.

Compressible and Collapsible materials. Some types of soil and rocks may contain layers of very soft materials like peat or some clays. These may compress if unevenly loaded by overlying structures, or if the groundwater level changes.

Running sand. Occurs when loosely packed sand becomes fluidised by water flowing through the spaces between the grains. The pressure of the flowing water reduces the contact between the grains and they are swept along in the flow. Running sand is most prevalent in the middle and south of England.

Earthquakes. The UK has a rather low level of seismic risk, expressed in terms of the likelihood of damage at any particular location. For example, estimates of the expected strength of earthquake shaking likely to occur in Britain show that there is only a 10% chance of experiencing shaking equivalent to intensity 6 or higher in a 50 year period, even in areas of relatively high exposure. (Intensity is a measure of earthquake shaking. An intensity value of 6 corresponds to a slightly damaging earthquake). Far field earthquakes can trigger tsunamis that could impact the UK coasts. Historical evidence and models suggest greatest risk is from the area west of Gibraltar impacting on south west England.

Offshore and coastal geological hazards. The UK Continental Shelf Designated Area is approximately 3.5 times larger than the UK land area. Geological hazards exist on the coast and offshore. For example, large areas of the coastline of the UK are prone to erosion, and offshore, gas deposits present a hazard.

The rate of coastal erosion (exceeding 15 metres per year in places) is of real concern to coastal buildings and transport networks and supply cables particularly in southern and eastern England. Offshore gas deposits affect activities involved in the development of renewable and non-renewable energy resources and waste disposal.

When inland flooding moves into the sea it can trigger submarine landslides where the slope is steep, eg fjordic settings such as Scottish sea lochs. This movement, although unseen, can impact on infrastructure on the sea bed and along nearby coasts.

Offshore severe storms can change the geometries of sand banks that would have consequence to renewable sighted on them, such as wind farms. Longer term increased storminess, and ocean changes could affect scour on infrastructure (pipelines, cables, foundations) or alter coastal erosion patterns.

Offshore shallow gas is a hazard eg by drilling rather than allowing it to naturally seep to the surface. This can impact infrastructure on the sea bed eg oil filed installations, pipelines and cables.

Guide 2: Checklist for Infrastructure Owners and Operators

The following set of questions is designed to assist infrastructure owners and operators to develop an Organisational Resilience Strategy that takes full account of the risk to their critical infrastructure from natural hazards, and sets out an approach to embed the strategy into corporate governance mechanisms.

Resilience Checklist for Infrastructure Owners and Operators

Identify Risks

Understand your criticality

STEP 1: Determine the elements of infrastructure critical to the provision of essential services provided by your organisation.

STEP 2: For your critical infrastructure, identify linkages with other elements of critical infrastructure within your supply chain.

Understand Hazards

STEP 3: Using the scenarios in the Natural Hazards Guidance (Guide 1), identify which hazards are of greatest concern to your critical infrastructure and supply chains.

Self Assessment Questions

1) Have you worked with external agencies to assess the natural hazards risks to your organisation's critical infrastructure? For example:
    a) Met Office;
    b) Local Authorities;
    c) Environment Agency;
    d) British Geological Survey
    e) Ordnance Survey
2) Does the location of your critical infrastructure make it more vulnerable to disruption from natural hazards?
3) Have you identified your key / critical suppliers / customers? Do some of those deliver an essential service for your community?

Assess Risk Understand your vulnerability

STEP 4: Understand what level of resilience you have to those hazards through design and service standards.

STEP 5: Using the findings from your investigations into (3) and (4) determine your level of residual risks.

Self Assessment Questions

4) What standards (design, protection, network design, service, performance, recovery time) offer resilience to your critical infrastructure? Where are the gaps?

5) Could there be a surge in demand for your services as a consequence of disruption from natural hazards? Will you be able to manage this?

6) Have you worked with key / critical supply chain partners to understand their vulnerability to disruption by natural hazards? How could their disruption affect the delivery of your essential services?

7) Have you worked with emergency responders, and others that your organisation would rely on during a period of disruption to improve your understanding of:

   a) Their vulnerability to disruption from natural hazards;

   b) The assistance that your organisation could expect to receive from them during a period of disruption from natural hazards?

Build Resilience

STEP 6: What is the risk appetite within your organisation? How is resilience of critical infrastructure considered and weighted by the corporate Board in decision making? Does this need to change?

STEP 7: Based on the conclusions of (6) and the principles set out in Section A of this Guide, decide what level of resilience is required and what resilience strategy will be adopted to provide the required level of resilience. Consider if the design of your infrastructure needs to evolve to provide greater resilience to future climates.

STEP 8: Embed organisational resilience at the core of your strategic decision making processes.

STEP 9: Engage with emergency responders for the area over which your organisation supplies essential services.

Self Assessment Questions

8) For disruption as a result of natural hazards, are you willing to:

   a) Accept the risk, do nothing (tolerate); or
   b) Mitigate the risk through emergency and business continuity plans (treat); or
   c) Outsource your product / service to another supplier or purchase insurance (transfer); or
   d) Cease the activity, move to another location or invest in greater resilience (terminate)?

9) Is the Board aware of the risk of disruption from natural hazards?

10) Has your organisation's risk appetite to disruption from natural hazards been agreed at Board level?

11) Is the Organisational Resilience Strategy championed at Board level?

12) Has the Board committed resources to improving the resilience of your critical infrastructure to disruption from natural hazards?

13) Has the Board overseen the production of contingency plans to manage disruption from natural hazards?

14) Do you have plans in place to manage (a combination of)?

   a) Loss of primary transport routes;
   b) Reduced staff availability;
   c) Impaired site access;
   d) Loss of power supplies; and lack of availability of alternative power supply;
   e) Loss of water supplies; and lack of availability of alternative water supplies;
   f) Closure of local businesses;
   g) Increased demand for health; emergency services, your products / services and those within your supply chain;
   h) Supply chain disruption

15) Have these plans been shared with emergency responders and supply chain partners (up and down stream)?
16) Does the Board seek assurances on the resilience of critical infrastructure to disruption from natural hazards at least annually?
17) Do you have a resilience based education and awareness programme in place within your organisation? If not, do you have board / senior management level support to put in place a resilience based education and awareness programme?
18) Have key staff been trained to implement emergency and business continuity plans?
19) Is there evidence that resilience, and particularly the risk from natural hazards, has been factored into the organisation's strategic decision making including medium to longer term investment plans?
20) Have your business continuity plans been tested against the British Standard, BS25999?
21) Does your organisation aim to achieve BS25999 alignment / certification?

22) Are your critical suppliers aligned or certified to BS25999? Do you make this a requirement?

Evaluate Resilience

STEP 10: Challenge, test and exercise your organisational resilience strategy. Report to your Board, Regulator or Lead Government Department residual vulnerability of any CNI within your remit.

Self Assessment Questions

23) Have you reviewed your Organisational Resilience Strategy?

24) Have you identified and tested any assumptions that underpin the delivery of your strategy?

25) Do you have an exercise programme in place that addresses the risk from natural hazards? Has it been approved by the Board? Do Board members take part in exercises?

26) Have you exercised more than one type of disruption at any one time ie loss of primary transport routes, coupled with loss of power and water supplies?

27) Are plans tested at least annually? Have findings been recorded and lessons learned?

28) Were supply chain partners and emergency responders included in these tests / exercises?

29) Were findings shared with the Board, supply chain partners, emergency responders, regulators and / or government?

30) Have you taken part in your supply chains' and / or emergency responder's tests / exercises?

Guide 3: Guidance on Information Sharing

Purpose

The purpose of this Guidance is to enable information on critical infrastructure to be shared at an appropriate time to those who need it to improve the resilience of infrastructure and essential services, and deliver an effective emergency response to civil emergencies. To achieve this, there is a 'need to know' information on critical infrastructure prior to an event and ensure appropriate plans are in place to respond and recover.

For civil emergency planning it is necessary to understand:

(a) what infrastructure provides essential services in an area, and its dependencies;

(b) the risks (likelihood and impact) of disruption to that infrastructure from natural hazards and threats; and

(c) the assumptions being made about assistance from emergency services e.g. pumping of flood waters by the Fire and Rescue Service (FRS).

This guidance has been provided in response to concerns by both Category 1 and 2 responders that information on critical infrastructure is not being shared with the right people at the right time for civil emergency planning, especially information on Critical National Infrastructure (CNI). This is due to protective markings, commercial sensitivities and lack of knowledge of infrastructure.

The limitations on sharing information on critical infrastructure have been shown to limit the accuracy of risk assessment and the effectiveness of event planning, emergency response and incident recovery. It also limits the ability to factor in vulnerabilities of existing infrastructure within operators' investment decisions.

Scope

This guidance focuses on information sharing regarding critical infrastructure. Critical infrastructure is a broad term used to describe Critical National Infrastructure (CNI) and other infrastructure of *national significance* as well as infrastructure and assets

of local significance. Disruption to critical infrastructure would lead to the loss or disruption of essential services, or present a hazard to the community, or reduce the effectiveness of an emergency response, and/or could lead to loss of life. Hence, critical infrastructure may require specific arrangements for emergency planning and response by the emergency responder community.

Sites and elements of the national infrastructure that have been identified by the Government as being of strategic national importance are known as Critical National Infrastructure. The loss or compromise of these assets would have severe, widespread effect impacting on a national scale.

This guidance outlines a process for Category 1 and 2 responders under the Civil Contingencies Act (CCA) 2004 that is intended to support and enhance information sharing under the Regulations and to enable Category 1 and 2 Responders to receive the necessary information on infrastructure to carry out their duties to best effect. It is intended to assist Local Resilience Fora (LRFs) in England and Wales, Strategic Co-ordination Groups (SCGs) in Scotland, and resilience discussions in Northern Ireland. (Note: any references in this guidance to LRFs also include SCGs in Scotland).

Principles

The guidance builds upon examples of current practice developed by local resilience forums often in multiple local resilience forum groups. It also respects the concept of the 'need to know' information for emergency planning and uses the principle of 'right issue, right time, right level' (as outlined in Table G3.1) in line with the Civil Contingencies Act's statutory guidance, Emergency Preparedness. It enables emergency responders to adopt a risk-based and proportionate approach to inclusion of the loss of essential services within emergency plans.

Table 1: "Right issue, right time, right level" Assessment [2]

Issue	Time	Level
Information on critical infrastructure (includes CNI)	Before emergency for civil emergency planning	Held by appropriate Police and Fire & Rescue personnel who must be Security Cleared (SC) and have appropriate storage facilities
Planning assumptions for critical infrastructure	Before emergency for civil emergency planning	LRF members Must satisfy the Baseline Personnel Security Standard (BPSS).
Information on critical infrastructure networks and systems	Before emergency, for assessment of interdependencies	Utility Group (led by Category 2 responders) Must satisfy the Baseline Personnel Security Standard (BPSS).
Relevant information on critical infrastructure	During an emergency, for prioritisation and response	SCG Must satisfy the Baseline Personnel Security Standard (BPSS).

In applying this guidance, all government departments and agencies must adhere to the Government's Security Policy Framework.[3]

Any information on critical infrastructure obtained for civil emergency planning should not be shared further or wider within organisations beyond the immediate 'need to know' for civil emergency planning, and must not be used for political or commercial gain. Information originating outside of government of a commercial or sensitive nature should be protectively marked as "commercially confidential" and handled accordingly.

Organisations need to take responsibility for managing their risks from natural hazards or other threats. These risks should not be devolved or transferred to the emergency services.

[2] HMG Personnel Security Controls: www.cabinetoffice.gov.uk/resource-library/hmg-personnel-security-controls

[3] HMG Security Policy Framework: www.cabinetoffice.gov.uk/resource-library/security-policy-framework

CTSAs should continue to provide regular oral briefings to LRFs on the CNI within their area, and continue to disclose information on CNI on a "need to know" basis at the Strategic Co-ordination Group (SCG) during civil emergencies for the purpose of enabling an effective emergency response. All members of a SCG should satisfy the Baseline Standard (BPSS) – see Table G3.1 - which is an appropriate standard for information on CNI for use during an incident.[4]

The CCA 2004 (Contingency Planning) Regulations 2005 set out the obligations for information sharing and co-operation that underpin the normal day to day exchange of information between those involved in resilience planning. Formal requests can be made by Category 1 and 2 Responders for information from other Category 1 and 2 Responders where it is necessary for the requesting responder to obtain that information. These Regulations provide that responders are under a duty to comply with the request unless the information is sensitive and falls within a specified exception.

Guidance

This document sets out an **iterative process** that supports the framework provided by the CCA (and associated guidance) and the duty on Category 1 and 2 responders to share information for the purposes of improved emergency planning, see the outline process chart in Table G3.2. It requires a proportionate approach to consideration of critical infrastructure in civil emergency planning.

The success of this approach is dependent upon establishing effective relationships between responders and infrastructure owners and operators. Many local resilience forums are already working together to encourage and support this through Utility Groups or Category 2 Forums. In Scotland some Strategic Co-ordination Groups have established CNI sub-groups, and in Wales there is one Utility Group reporting to the Wales Resilience Forum. Other providers of essential services (who are not Category 1 or 2 responders under the CCA) should be engaged with information sharing as appropriate. It is recognised that infrastructure owners have widely

[4] If the meetings of the SCG are occasional then BPSS is sufficient and there is no requirement for National Security Vetting to be undertaken.

varying roles and responsibilities, and geographical areas of responsibility. The LRFs therefore need to discuss with infrastructure owners the optimum approach for their area, although many national infrastructure owners are unable to directly support every LRF. It is therefore recommended that Utility Groups or Category 2 Forums operate in the first instance across several LRF areas (see also the paragraph on information sharing protocols at the end of this section).

Suggested Process

1. LRFs to produce the Community Risk Register (CRR)[5] based on the Local Risk Assessment Guidance, National Risk Register, Planning Assumptions and new Guidance on Natural Hazards. This process should identify the hazards and threats that could affect the area and the potential consequences of these (including the impact on the provision of essential services in the LRF area).

2. Providers of essential services undertake business continuity management (BCM) to ensure plans are in place for disruptive incidents. This is a requirement under the CCA for Category 1 responders. It is recognised that Category 2 responders have various systems in place for business continuity planning. BS25999 is encouraged, although it is recognised that some sectors have their own specific requirements and regulations for business continuity and emergency plans. BCM should:

    - Include consideration of operational activities to ensure security of supply and the continued provision of essential services in the event of natural hazards

    - Identify any 'critical' elements of networks or assets that provide essential services for which they are responsible - that which, if lost or disrupted would significantly impact on an LRF area and and/or more widely, even if critical parts of the network are located outside of that community

    - Include an assessment and understanding of dependencies and interconnectivity with other sectors.

[5] Requirement under the Civil Contingencies Act 2004

It is recognised that Category 1 and 2 responders will seek information from their utility providers to gain greater understanding of the resilience of their own utility supplies for business continuity management purposes. These requests are expected to be directed to their business contract / account managers. They will relate to supplies to specific sites or parts of the network, and will be more limited than that necessary to carry out wider emergency preparedness duties. Utility companies will need to ensure their business models facilitate provision of such information to Category 1 responders and other customers seeking such information for their Business Continuity Plans. Where feasible and practical, sector regulators may wish to propose standards of resilience that their sectors will meet (subject to derogation where necessary). Individual companies would then only need to ask if there was a derogation in force for the part of the network that they are supplied from.

An agreed lead Category 1 Responder for the LRF (normally the Chair of the LRF) to request information on critical infrastructure within the LRF Area from Category 2 responders (and other owners of critical infrastructure who are prepared to provide information under these arrangements). Using the information from their BCM process, owners of infrastructure should provide information on any critical infrastructure that provides essential services within the LRF area, whether the infrastructure is located within or outside of the LRF area. This should include sites where a response or support may be needed from emergency responders to manage the consequences of civil emergencies, and any critical local assets or infrastructure as determined by infrastructure owners in discussion with other local responders.

The information (to be used for emergency planning purposes only) should include:

a) Name of infrastructure network / system;

b) Critical installations or sites in the network;

c) Location of critical installations / sites, and their function;

d) Network / site owners;

e) 24 / 7 Emergency contact name and numbers for emergencies;

f) Specific safety / hazards information for the network and sites (e.g. COMAH) and access / egress restrictions that the emergency services need to know;

g) Outline of the consequences of loss or disruption of the critical infrastructure in terms of loss of service to x number of people in the LRF area, and which other LRF areas could also be affected;

h) A general assessment of the service's vulnerability to natural hazards and accidents, and any mitigation measures taken to reduce the risks;

i) What action the network / site owner would take in case of an emergency;

j) Support the infrastructure owner anticipates receiving or may need from emergency services and other emergency responders during an incident.

Any references to sites/assets being critical infrastructure indicates that the asset is important / critical and could provide useful targeting information for those with a malicious intent. Such information may require a protective marking (e.g. 'RESTRICTED'). An example of the type of information that would be restricted is: "Skiptown water works is critical because if the site was destroyed approximately two million people would lose their water supply for over a month, and all the water treatments works in the north of the country would also stop functioning".

Information containing multiple references to critical infrastructure and details of potential consequences of disruption to those assets may require a higher protective marking, for example, confidential. References to (a) a site labelled as CNI, (b) a CNI criticality scale score, and (c) details of wider consequences beyond the LRF area, should be removed to limit the need for higher protective markings.

3. <u>The senior Police lead for emergency planning to collate information on critical infrastructure and work with the appropriately trained and qualified Fire and Rescue Service (FRS) officer for contingency planning to oversee the use of this information on critical infrastructure within the LRF for civil emergency planning.</u>

The Police and FRS officers must be security vetted to SC level and ensure they have measures in place to transmit, store and handle information at RESTRICTED and CONFIDENTIAL level. They should jointly review the information on critical infrastructure and:

(a) **Check** that all CNI in the area has been identified within the wider critical infrastructure for use in emergency planning. This may involve a cross check with the CNI catalogue held by the local CTSA. If as a result of this cross check, a CTSA is aware of a CNI asset in the LRF area that has not been identified by the Police and FRS officers, the CTSA will contact the National Counter Terrorism Security Office (NaCTSO) who will co-ordinate these queries and liaise with CPNI for a resolution.

(b) **Check** that the existing FRS and Police emergency response plans for the LRF area adequately cover all critical infrastructure and the loss of essential services, particularly where a response from the emergency services is required in an emergency for critical infrastructure. Where necessary, further develop the Police and FRS emergency response plans as necessary - can be separate plans or restricted/confidential annexes to existing emergency plans. Also consider the extent of the loss of essential services in adjacent LRF areas and liaise with those areas to ensure appropriate prioritisation of CNI in emergency response plans and arrangements for mutual aid.

(c) **Check** that the existing local risk assessment guidance and resilience planning assumptions adequately reflect the potential impacts arising from the failure of critical infrastructure and loss of essential services in the LRF area. Discuss with other Category 1 responders to ensure their plans adequately consider and address those planning assumptions and the potential loss of essential services arising from disruption of infrastructure. The Police and FRS officers holding the information on critical infrastructure may provide supervised access to the information on a ‘need to know’ basis, to allow other Category 1 responders to review their emergency response plans - providing the individual(s)

within those organisations are security cleared to a minimum of Baseline Personnel Security Standard (BPSS). [6]

Where the impacts of loss of critical infrastructure may require a response involving other emergency responders within the LRF, provide those members with:

i. emergency contact details for the Category 2s that provide essential services in the LRF area;
ii. local planning assumptions, aggregated from individual consequence of loss information providing a wider picture of the full impact of a potential emergency; and
iii. information on the hazards that are likely to cause these impacts.

Information on critical infrastructure within emergency plans should be kept to a level appropriate and necessary for the purposes of the plan. Restricted or confidential information should be within separate annexes (if necessary to include within the plans) and handled accordingly. Labelling infrastructure as CNI within emergency plans is not permitted.

4. Category 2 responders should get together to share information on their roles and responsibilities, arrangements for emergency response, and information on their critical infrastructure. The purpose is for infrastructure owners to gain a better understanding of the dependencies of their infrastructure on others' systems and networks, and knowledge of roles, responsibilities and capabilities across all sectors of infrastructure. The group should share information on critical infrastructure, consider the potential for cascade failures across networks and systems, and hence identify additional assets in the network that are critical for continuity of essential services to the risks identified in the Community Risk Register.

[6] BPSS is sufficient for access Restricted and Confidential material and in some cases occasional Secret material.

It is recommended that these groups cover multiple LRF areas. Membership could be based on previous regional geographical boundaries or on a thematic or shared risk basis. Utility Groups (Category 2 Forums) already exist in some parts of the UK that fulfil this role. The term 'Utility Group' will be used in this guidance. Utility Groups may wish to combine with Telecom Sub-Groups where desirable and practical.

LRFs should be invited to send an appropriate representative(s) to the Utility Groups. These groups will support the building of better relationships between providers of essential services. They will also enable Category 1 responders to understand how category 2 responders plan to deal with service interruptions, and agree trigger points when the Category 1 will be notified of an emergency by the Category 2 responder. Other providers of essential services (not currently covered by the CCA) should be invited to participate as appropriate.

Whilst sharing information enables improved emergency planning, it does not reduce the need for direct communication during an incident to obtain an understanding of the actual problems being faced. The Utility Groups will enable effective relationships to be established between responders before an event occurs, which then assist the emergency response to and recovery from civil emergencies. Members of existing groups commented that the Utility Group creates trust between infrastructure owners which supports open communication, facilitates sharing of information and encourages co-operation during emergencies.

Owners and operators of critical infrastructure should use the information on dependencies and on emergency responder capabilities to update their business continuity plans and to inform future investment in the infrastructure to improve resilience.

5. LRFs to use the planning assumptions provided by the Police and FRS alongside the improved information and understanding of infrastructure networks and systems gained through the Utility Group to update and improve the CRR and emergency plans. Improved understanding of potential failures and key weaknesses and dependencies should provide a more accurate understanding of

local risks, particularly where these may differ in severity or detail from those listed at a national level. Each LRF will be responsible for deciding which risks to include in their emergency plans to ensure an effective response to emergencies.

Infrastructure owners and operators may wish to contribute to specific LRF meetings relating to the preparation of emergency plans for their sites. This will enable them to ensure that their sites are appropriately prioritised and prepared for the response they may receive in an emergency. It will also enable them to further improve their business continuity plans and inform their investment planning to improve resilience of the essential services. Active engagement in the Utility Group by infrastructure owners could reduce the need to regularly attend LRF meetings. The multiple LRF Utility Group in the North West of England has established effective relationships between utility companies such that they are able to share attendance and represent others' interests at occasional LRF meetings across the region when emergency plans are being discussed.

Plans should be shared with relevant Lead Government Departments so they can be assured their key sites have been prioritised appropriately.

6. Category 2 responders use improved understanding of risk in preparing / revising their business continuity management arrangements, ensuring appropriate co-ordination between the plans.

Additional notes and recommendations

7. The Utility Groups may wish to consider whether visits to the most critical sites for the Police and Fire & Rescue Service (and other Category 1 responders as appropriate) would be of value in terms of familiarisation of access to the site, location of critical components / equipment, site operators and their actions in a crisis, back-up arrangements, and to understand the recovery process and timetables. This follows similar good practice for COMAH sites. Visits should be co-ordinated with existing visits where possible to maximise the benefit to the infrastructure owners. For those sites that are part of the CNI and have NOT previously had engagement with Police and FRS planners, any proposed initial contact and visit must only be conducted after consultation with the local CTSA.

8. Understanding of dependencies should feed into strategic planning and capital investment decisions to improve the long term resilience of the networks to natural hazards and other threats. The right investment in the development and improvement of infrastructure networks will prevent severe disruption and loss of service from natural hazards and man-made threats. Understanding dependencies will ensure investment within sectors takes account of the need of other sectors. Investment decisions should consider the potential impacts of climate change so infrastructure is resilient to today's weather and that likely to be experienced during the lifetime of the development.

9. The Civil contingencies Act permits the use of protocols to formalise information sharing arrangements. They can reduce the burden on responders and create efficiencies by ensuring that efforts are properly focussed and that duplication is minimised. They can be particularly relevant where Category 1 responders working at local level are dealing with responders whose operational footprint may be national or multi LRF level. The process set out in this document could be used as a basis for a formal protocol if required.

Table G3.2: Critical infrastructure information sharing for emergency planning – outline process chart

STEPS	WHO	COMMENTS AND LINKS
1. Produce Community Risk Register to identify local risks and essential services	LRF	Current CRR process to be used to identify essential services in LRF area. Use Section C: Guide 1- Guidance on Natural Hazards.
2. Providers of essential services use the CRR to inform their business continuity management (BCM)	All organisations providing essential services in LRF area	BCM to cover essential services, critical infrastructure and supply chains. Refer to BS25999 or equivalent.
3. Request information on critical infrastructure in LRF Area (from trusted partners in the LRF)	Lead Cat 1 responder (e.g. Chair of LRF)	Information to be protectively marked. Information must not be used for wider use or for commercial or political gain.
4. Use information on critical infrastructure to review emergency response plans and local planning assumptions	Led by Police and Fire & Rescue Service	Collate and review information. Check that all CNI included in information on critical infrastructure. Check emergency plans and local planning assumptions adequately cover response for critical infrastructure and potential disruption of essential services
5. Utility Group considers interdependencies of critical infrastructure (networks and systems)	Organisations providing essential services	See Section C: Guide 4 – Guidance on Assessing Dependencies. See Annex 3: Example Terms of Reference for Utility Groups.
6. Use planning assumptions and information from the Utility Group to update CRR and emergency plans	LRF	Only unrestricted information to be used in publicly available version of the Community Risk Register.
7. Information used to improve emergency and business continuity plans, and investment decisions	Category 1 and 2 Responders	Resilience of critical infrastructure to be taken into consideration for wider emergency response plans, and to inform investment decisions

Guide 4: Guidance on Assessing Dependencies

This Guidance sets out a practical approach that can be used to assess dependencies. It is currently being tested by the responder community in parts of England and Scotland.

Understanding Dependencies

There are two principal types of dependencies to be considered for infrastructure. These are *geographical* and *physical*.

Geographical dependencies are where key infrastructure sites or installations are co-located in one close geographical area and hence are both dependent upon local infrastructure e.g. local roads, energy supplies and emergency services. The installations are also likely to be affected by an incident due to their close proximity. The Buncefield explosion in December 2005 illustrated how the explosion and fire disrupted the operation of other infrastructure, including energy distribution, transportation, information infrastructure, finance, and health. The nearby M1 motorway was closed for two days and an adjacent business park with 92 companies was destroyed (damages over £70m). A nearby IT company data centre suffered significant damage. Their servers hosted the patient administration system for two hospitals, which were unavailable for the hospitals to use for a week. The servers also hosted a North London payroll of approximately £1.4 billion, and systems/data for several local authorities.

Physical dependencies are those resulting from a connection between installations, sites and with other networks. For example, the physical dependency on electricity supply for the operation of water treatment works, or the dependency upon communications for the control of remote plant and equipment. The physical dependencies are typically not obvious and as such represents a significant and hidden risk to networks and systems. Without a sufficient understanding of physical dependencies, a loss of a key element of the infrastructure network (such as a major installation) could lead to cascade failures where further disruption is caused beyond the point of failure.

Where infrastructure sites or installations are dependent upon other services, such as electricity supplies, water or telecommunications, then these services are known as the upstream dependencies. These infrastructure sites/installations will often also supply services to other infrastructure (e.g. electricity supply provided to water treatment works) – these are known as its downstream dependencies. Where dependencies between two assets exist in both directions, this is known as an interdependency.

It is reasonably straightforward to assess *geographical* dependencies. Information is available to the responder community to identify major infrastructure assets that are located in the same geographical areas and hence could be affected by a single incident. For example, the area surrounding an industrial plant can be analysed for other critical infrastructure that could be affected by an explosion, or critical infrastructure can be assessed within each river or coastal floodplain.

Physical dependencies are more difficult to understand and map, however effective progress can be made by adopting a pragmatic approach building upon the requirements within the Civil Contingencies Act 2004 to co-operate and share information:

(1) Establish or use an existing group of utility providers and emergency responders covering multiple LRF areas. (This may be an existing Utility Group, Category 2 Forum or a CNI sub-group). Members may include:

   a. Providers of essential services relevant to area covered (water, energy, communications, transport, health, emergency services, government, food and finance);

   b. Other significant asset owners in the area;

   c. Police, fire and rescue service;

   d. Local authorities;

   e. Environment Agency;

   f. Counter Terrorism Security Advisors.

(2) Determine relevant tools available within the group, for example Ordnance Survey maps, geographical information systems (GIS) for mapping, National Resilience Extranet access for sharing information.

(3) Apply one or more of the following dependency mapping approaches:

a. **Start with a Site / Asset**. Identify the critical infrastructure that provides essential services in the Area, or is essential during civil emergencies, and map downstream dependencies.

b. **Start with Communities**. Identify the major communities (centres of population) in an area and determine the networks and critical infrastructure that provides the essential services to those communities. Map physical upstream dependencies.

c. **Start with Hazards**. Identify where specific hazards could occur and determine which infrastructure could be disrupted, then assess the downstream dependencies and impacts of loss of the infrastructure.

(4) Map dependencies, either simply as key installations and networks on a large plot Ordnance Survey map, or as a GIS mapping system.

(5) Produce a dependency map for the area to be used as an information and challenge document during risk assessment, pre event planning and exercising, ensuring visibility of key dependencies during an emergency.

Supporting Information Sharing to Understand Dependencies

Since the 2007 floods, several organisations, especially the emergency responders, have expressed concerns about the difficulties in sharing information on critical infrastructure, especially on Critical National Infrastructure (CNI). There is clear need to sharing the right information with the right people at the right time to facilitate an effective emergency response to civil emergencies.

The Guidance on assessing dependencies is intended to enable local emergency responders and infrastructure owners to work together to ensure a sufficient understanding of infrastructure networks and dependencies across sectors. The approach involves using the Community Risk Register and business continuity management best practice (as outlined in BS25999 or industry equivalents). Many

businesses and organisations that have business continuity management are accustomed to assessing their dependencies and preparing for loss of infrastructure, which is essential for delivery of core functions.

The assessment of dependencies is a fundamental aspect of good business continuity management. However, the 2010 Business Continuity Management Survey, *Disruption and Resilience,* still recognises that only 49% of businesses have undertaken BCM, rising to 65% for larger businesses. In addition, respondents to the 2010 Survey recognised loss of IT (69%) and telecommunications (62%) as the two greatest threats facing their businesses.

It is good business practice for owners/operators of critical infrastructure to, as a minimum, identify their immediate upstream dependencies (known as first tier) as part of their business continuity management (many infrastructure owners have mapped their network on a geographical information system for asset monitoring and planning e.g. gas network, electricity transmission network). However, it is recognised that each part of a network or system will have its own upstream and downstream dependencies and so to move beyond the first tier quickly becomes a time consuming and complex exercise. As the networks get closer to the point of supply to customers it becomes increasingly hard to use network maps to understand dependencies, redundancy and critical routes. This is particularly the case in the communication, information and energy networks where advanced networks are able to switch or re-route supplies and components are often not critical until failures have occurred elsewhere within the network.

The understanding of dependencies should enable operators to inform their strategic planning and capital investment decisions to improve the long-term resilience of the networks to natural hazards and other threats. Understanding dependencies will ensure investment within sectors takes account of the needs of other sectors.