

FOR CONSULTATION



CabinetOffice

Keeping the Country Running:

Natural Hazards and Infrastructure

For Consultation:

**A Guide to improving the resilience of critical
infrastructure and essential services**

FOR CONSULTATION

Produced by:

Cabinet Office
22 Whitehall
London
SW1A 2WH

Contact:

Civil Contingencies Secretariat, Cabinet Office

naturalhazards@cabinet-office.x.gsi.gov.uk

Web address: www.cabinetoffice.gov.uk

Publication date: March 2011

© Crown copyright 2011

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to it not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when reproduced as part of another publication or service.

Consultation Details

Purpose

The purpose of this consultation is to seek views of government departments, regulators, industry groups, infrastructure owners and emergency responders on the draft Guide on Natural Hazards and Infrastructure. We would particularly like to hear view on the practicality of the guidance contained within the Guide and any opportunities and barriers to implementation.

There is no impact assessment associated with the Guide as the Guide is not mandatory. The Guide has been developed to respond to needs identified by organisations that have interests in the resilience of infrastructure, and to fill gaps in advice that were highlighted during the 2007 floods. The guidance is intended to help organisations reduce the likelihood and costs of damage and disruptions to infrastructure from natural hazards, and in doing so improve their resilience to hazards and threats.

Timetable

The consultation will run for a period of 8 weeks. We will consider responses received by noon on **Friday 6 May 2011**.

How to respond

Consultation questions are included throughout the document to seek view on particular aspects of the Guide. We invite responses to these questions, supporting evidence and any issues that should be considered by the Programme.

Please submit responses to the questions and other evidence to: naturalhazards@cabinet-office.x.gsi.gov.uk marking your response with 'Consultation on Critical Infrastructure Resilience' in the subject field of your email.

Alternatively, you can submit your response via the **National Resilience Extranet** using one of the following methods:

NRE Method 1: Complete the consultation questionnaire and upload it into the document store of the NRE in the following folder: <https://www.resilience-extranet.gse.gov.uk/AtlasApps/Pages/Collaborate/DocumentStore/DocumentStore.aspx?folderid=110548>

NRE Method 2: Complete the consultation questionnaire and provide your response directly onto the NRE: <https://www.resilience-extranet.gse.gov.uk/AtlasApps/Pages/Common/Event/Event.aspx?EventID=276>

FOR CONSULTATION

You can also submit responses by post to the following address:

Natural Hazards Team
Cabinet Office
22 Whitehall
2nd Floor
London
SW1A 2WH

Should you require this document or the consultation response template in a different format, please advise us of your specific requirements:

- email: naturalhazards@cabinet-office.x.gsi.gov.uk
- telephone: 0207 276 5088

Contact for comments or complaints about the consultation process

If you have comments or complaints about the consultation process itself, please contact:

Vanessa Barron
Cabinet Office
Planning and Performance
Kirkland House
22 Whitehall
London SW1A 2WH

Email: vanessa.barron@cabinet-office.x.gsi.gov.uk

Handling of Information from Individuals

The information you send may need to be passed to colleagues within Cabinet Office or other Government departments, and may be published in full or in a summary of responses.

All information in responses, including personal information, may be subject to publication or disclosure in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004). If you want your response to remain confidential, you should explain why confidentiality is necessary and your request will be acceded to only if it is appropriate in the circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department. Contributions to the consultation will be anonymised if they are quoted.

Individual contributions will not be acknowledged unless specifically requested.

Acknowledgments

The Cabinet Office is grateful to the organisations that have supported the Critical Infrastructure Resilience Programme and the development of this Guide.

The organisations include:

Arqiva
Association of Chief Police Officers
Association of Electricity Producers
Chief Fire Officers Association
Department for Business, Innovation and Skills
Department for Communities and Local Government
Department of Energy and Climate Change
Department for Environment, Food and Rural Affairs
Department of Health
Department for Transport
Energy Networks Association
Environment Agency
Her Majesty's Treasury
Highways Agency
Home Office
Local Government Association
Met Office
Ministry of Defence
National Grid
Network Rail
Northern Ireland Executive
Office of Communications (Ofcom)
Office of the Gas and Electricity Markets (Ofgem)
Scottish Executive
Scottish Resilience
The Centre for the Protection of National Infrastructure
The Water Services Regulation Authority (Ofwat)
Transport for London
Water UK
Welsh Assembly Government

Contents

Executive Summary	7
Section A: Introduction and Definitions	8
1 Introduction	9
2 Definitions	12
Section B: Building Resilience	18
3 Identify Risks and Assess Resilience: Natural Hazards.....	21
4 Address Resilience: Standards	26
5 Review Resilience: Sector Resilience Plans	32
6 Governance and Organisational Resilience	35
7 Guidance for Regulated Sectors	38
8 Sharing Information and Assessing Dependencies	43
Section C: Practical Guidance	51
Guide 1: Guidance on Natural Hazards.....	52
Guide 2: Checklist for Infrastructure Owners and Operators	65
Guide 3: Guidance on Information Sharing	69
Guide 4: Guidance on Assessing Dependencies.....	82
Section D: Annex	88
Annex 1: Pitt Recommendations on Critical Infrastructure.....	89
Annex 2: Related Legislation.....	90
Annex 3: Example Terms of Reference for Utility Groups	95

Executive Summary

The National Security Strategy (NSS) sets out that one of our key tasks is to improve resilience of the infrastructure¹ most critical to keeping the country running against attack, damage or destruction. The top risks identified in the NSS include those from natural hazards.

The floods of summer 2007 and more recent events such as the Cumbria Floods, the 'Big Freeze' in January 2010, the eruption of the Eyjafjallajokull volcano in Iceland and the prolonged period of extreme cold weather in December 2010 have all highlighted the vulnerability of the UK's national infrastructure and essential services to disruption from natural hazards.

Building resilience in our infrastructure is important to reduce our vulnerability to natural hazards. This can be achieved by improving (where necessary) protection, encouraging an ability in organisations and their infrastructure networks and systems to absorb shocks and recover, and enabling an effective local and national response to emergencies.

This Guide has been developed to support infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services.

The Guide provides advice on risk assessment for natural hazards, standards of resilience, business continuity and corporate governance, guidance for economic regulators and information sharing on infrastructure.

¹ See Annex A for definitions of Infrastructure and resilience

Section A: Introduction and Definitions

This section introduces infrastructure resilience, sets out the background and provides definitions.

1 Introduction

Purpose

1.1 In its National Security Strategy and Strategic Defence and Security Review, the Government set out the need to improve the security and resilience of the **infrastructure most critical to keeping the country running** against attack, damage or destruction. International terrorism, cyber attacks, major accidents and natural hazards are identified as among the most serious risks to the UK's national security interests.

1.2 The purpose of this Guide is to focus on the last of these – natural hazards – and to encourage infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services. The Guide has been developed in partnership with representatives of these organisations under the Critical Infrastructure Resilience Programme.

1.3 The Guide supplements existing guidance and fills gaps identified during the consultation on the Strategic Framework and Policy Statement (March 2010).

1.4 The Guide is divided into sections as follows:

- a) Section A (this section) explains the purpose and background of the Guide, introduces infrastructure resilience and provides definitions;
- b) Section B outlines an approach for improving and maintaining the resilience of infrastructure; and
- c) Section C provides practical guidance for Government, regulators, owners and operators of infrastructure, and emergency responders.

FOR CONSULTATION

Background

1.5 The floods of summer 2007 and more recent events such as the Cumbria Floods, the 'Big Freeze' and the eruption of the Eyjafjallajokull volcano in Iceland have all highlighted the vulnerability of the UK's national infrastructure and essential services to disruption from natural hazards.

1.6 Damages caused by natural hazards can be significant – the 2007 floods alone cost the UK economy over £4 billion, and the damage specifically to critical infrastructure was valued at about £674 million². The costs from lost revenues, reputational damage, contractual penalties and the potential for litigation, provide a strong driver for organisations to manage risks and build resilience into their operations.

1.7 Many of the more detailed lessons from the summer 2007 floods were identified by Sir Michael Pitt in his review, the key recommendations of which are at Annex 1. He highlighted the need for:

- improved understanding of the level of vulnerability or risk to which infrastructure and hence wider society is exposed;
- More consistent emergency planning for failures;
- Improved sharing of information at a local level for emergency response planning; and
- Improved involvement of 'Category 2' responders³ in multi-agency response exercises in crisis management.

1.8 The Review called for a more systematic approach to building resilience in critical infrastructure, and called for a cross sector campaign – involving owners/operators, regulators, and government - to improve the resilience of critical infrastructure and essential services, especially to disruption from natural hazards.

1.9 In response to these recommendations, the Government in March 2010 published:

² The costs of the summer 2007 floods in England. Environment Agency January 2010.

³ Category 2 responder: A person or body listed in Part 3 of Schedule 1 to the Civil Contingencies Act. These are co-operating responders who are less likely to be involved in the heart of multi-agency planning work, but will be heavily involved in preparing for incidents affecting their sectors. The Act requires them to co-operate and share information with other Category 1 and 2 responders.

FOR CONSULTATION

- a) a Strategic Framework and Policy Statement setting out the process, timescale and expectations for a critical infrastructure resilience programme;
- b) a Summary of the Sector Resilience Plans 2010; and
- c) Interim Guidance to the Economic Regulated Sectors.

Infrastructure Resilience

1.10 The Government's approach is that the main responsibility for resilience of critical infrastructure lies with the owners and operators. However, government, regulators and industry need to work together to ensure investment in infrastructure considers the needs for security and resilience. Investment to improve the security and resilience of critical infrastructure should be:

- proportionate to the risks
- enabled by improved sharing of information between those who need to know
- delivered at the lowest practicable level.

1.11 The lead Government Departments for each infrastructure sector are supported by the Home Office and the Centre for the Protection of National Infrastructure (CPNI) on matters of security, HM Treasury on financing and investment in infrastructure, the Cabinet Office on resilience and cyber security and the Department for the Environment, Food and Rural Affairs on climate change adaptation.

1.12 Owners and operators of national infrastructure do not all face the same risks or need to tackle issues in the same way. The differences across sectors and geographical locations means there is no "one size fits all" approach to improving resilience. A tri-partite arrangement is necessary within each sector between infrastructure owner, regulators and government to explore the optimum mechanisms and strategy to provide security for the infrastructure in the sector.

2 Definitions

2.1 The **national infrastructure** is a complex mix of networks, systems, sites, facilities and businesses that deliver goods and services to citizens, and supports our economy, environment and social well-being.

2.2 Within the national infrastructure, nine sectors have been identified as providing **essential services** that are the fundamental services upon which daily life in the UK depends. The 9 sectors are: food, energy, water, communications, transport, health, emergency services, government, and finance.

2.3 Within these nine sectors, the Government has identified certain assets as being of strategic national importance to essential service delivery. These are collectively known as the **Critical National Infrastructure** (CNI). The loss or compromise of these assets would have a severe, widespread impact on a national scale.

2.4 The wider infrastructure does more than just deliver these essential services. Other particularly high risk or significant infrastructure may also warrant special consideration and arrangements for security and/or resilience. On this basis, Government maintains a priority interest not only in Critical National Infrastructure, but in other critical infrastructure that is of national significance including:

- Civil nuclear facilities
- Hazardous sites (such as top tier COMAH sites)
- Iconic sites
- Companies / research organisations which hold information that is of particular economic or strategic value to the UK.

2.5 For the purposes of civil emergency planning, the emergency responders may decide to make special provisions for other infrastructure of primarily local significance (**critical local infrastructure or assets**) in their emergency response plans. These might include arrangements for infrastructure whose loss would impact on delivery of essential services, have other significant impacts within the local area, or be needed to support an emergency response.

FOR CONSULTATION

2.6 **Critical infrastructure** is therefore a broad term used to describe CNI and other infrastructure of *national significance* as well as infrastructure and assets of local significance.

Risk

2.7 **Risk** is defined as the likelihood that a hazard will actually cause its adverse effects, together with a measure of the potential impact.⁴ The Government monitors the most significant **risks of terrorism and other malicious acts, major accidents and natural hazards – collectively known as civil emergencies** - that the United Kingdom and its citizens could face over the next five years through the National Risk Assessment (NRA). This assessment is conducted annually and draws on expertise from a wide range of departments and agencies of government. The National Risk Assessment takes into account the impacts of emergencies on human welfare, including the social disruption that is caused by civil emergencies, and on economic output.

2.8 The **National Risk Register 2010 (NRR)**⁵ is the published ‘unclassified’ version of the NRA. It identifies the range of civil emergencies and indicates the relative likelihood and impact (see Figure 1).

⁴ HSE, “reasonably practicable” guidance (www.hse.gov.uk/risk/expert.htm)

⁵ www.cabinetoffice.gov.uk/intelligence-security-resilience/national_risk_register

FOR CONSULTATION

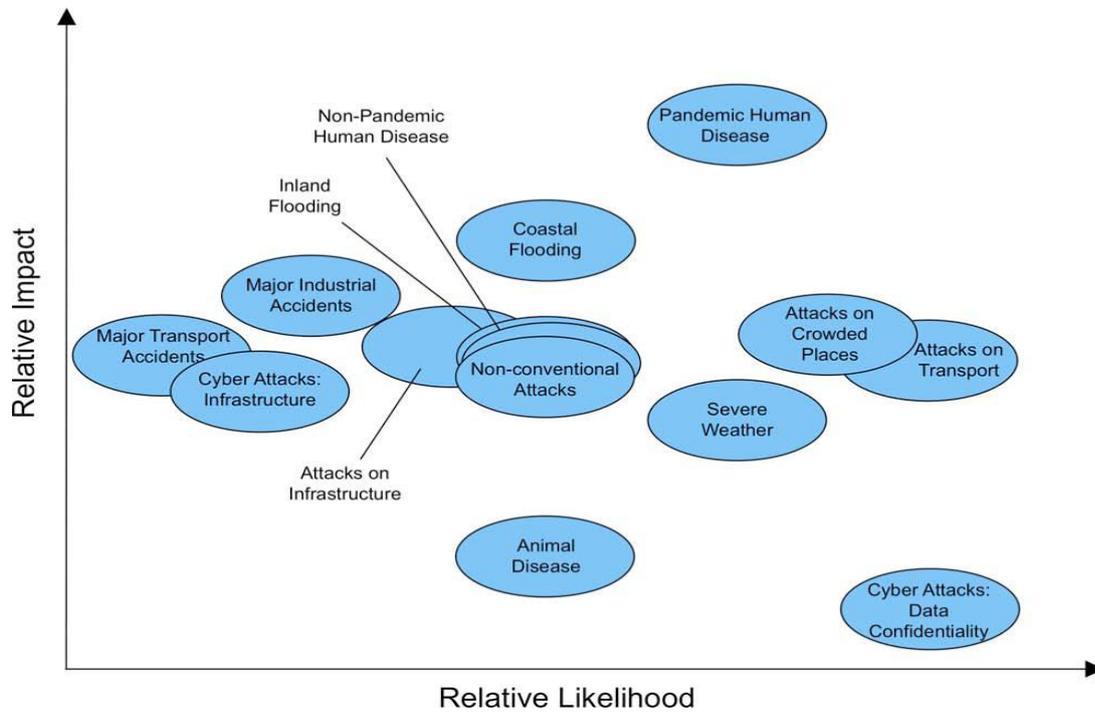


Figure 1: An illustration of the high consequence risks facing the United Kingdom.

2.9 **Local Resilience Assessment** is carried out by emergency responders listed under the Civil Contingencies Act, and including the 'blue light' services, local authorities and other front-line responders. Through Local Resilience Fora (LRF) they may collectively publish **Community Risk Registers** (CRRs). Government ministers may provide guidance on risks and on planning assumptions for emergency response derived from the National Risk Assessment.

2.10 **Risk management** is a process of identifying, understanding, managing, controlling, monitoring and communicating risk. This ensures investments are considered across the range of options and choices, and are proportionate to the risks. Effective risk management is the key to facilitating and building resilience, particularly when driven at the corporate level to create a culture where resilience and business continuity management is embedded in operations. This creates '**organisational resilience**' – the ability of an organisation to anticipate, plan and respond to uncertainties and disruptions to business operations.

Resilience

2.11 **Resilience** is the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover from a disruptive event⁶. Resilience is secured through a combination of activities or components; the four principle strategic components are shown in Figure 2. The appropriateness and cost-effectiveness of each component varies across the nine sectors of national infrastructure owing to the different types of infrastructure and technical opportunities. Each of these components can be utilised or adopted to different levels. Given the range of risks, organisations should select combinations of responses from all four of these components to develop a strategy that will deliver the most cost effective and proportionate risk management response to the hazards and threats.



Figure 2: The components of infrastructure resilience: In building resilience, the contribution made by each of these four components needs to be considered

2.12 The **Resistance** element of resilience is focused on providing protection. The objective is to prevent damage or disruption by providing the strength or protection to resist the hazard or its primary impact. Resistance strategies have significant weaknesses as protection is often developed against the kind of events that have

⁶ In its broader sense, it is more than an ability to bounce back and recover from adversity and extends to the broader adaptive capacity gained from an understanding of the risks and uncertainties in our environment. But for the purpose of this guidance, a narrower definition has been adopted.

FOR CONSULTATION

been previously experienced, or those predicted to occur based on historic records. Protective security measures aimed at reducing the impact of malicious threats may or may not help to reduce the impact of natural hazards. Disruptive events can exceed the standards provided for protection thus resulting in loss or damage and significant impacts, particularly where the resistance strategy is the only component of a resilience strategy.

2.13 The **Reliability** component is concerned with ensuring that the infrastructure components are inherently designed to operate under a range of conditions and hence mitigate damage or loss from an event. The tendency of a reliability strategy is to focus only on the events within the specified range, and not events that exceed the range. This can lead to insufficient awareness or preparation for events outside of the range, and hence significant wider and prolonged impacts can occur. Reliability cannot therefore be guaranteed, but deterioration can sometimes be managed at a tolerable level until full services can be restored after the event.

2.14 The **Redundancy** element is concerned with the design and capacity of the network or system. The availability of backup installations or spare capacity will enable operations to be switched or diverted to alternative parts of the network in the event of disruptions to ensure continuity of services. In some of the sectors of national infrastructure, redundancy strategies would lead to an initial loss of performance until the alternative infrastructure can be brought into operation. The telecommunications sector employs a redundancy strategy to provide the capacity and flexibility to meet peak demand for services and enable re-routing of communications 'traffic' in the event of failure or loss of components. In this sector, the switch over to maintain services is instantaneous. The resilience of networks reduces when running at or near capacity, although in some sectors or organisations it is recognised that it may not always be feasible to operate with significant spare capacity within the network.

2.15 The **Response and Recovery** element aims to enable a fast and effective response to and recovery from disruptive events. The effectiveness of this element is determined by the corporate culture, its capabilities, and the thoroughness of efforts to plan, prepare and exercise in advance of events. The strategy may differentiate between the response and the recovery. Some owners of critical infrastructure understand the weaknesses in their networks and systems and have arrangements in place to respond quickly to restore services. Recovery is considered in pre-event

FOR CONSULTATION

planning to explore opportunities to reduce future risks and/or build resilience in infrastructure during the recovery stage.

2.16 Hence resilience of infrastructure is provided through (a) good design of the network and systems to ensure it has the necessary resistance, reliability and redundancy (spare capacity), and (b) by establishing good organisational resilience to provide the ability, capacity and capability to respond and recover from disruptive events. The latter is gained through business operations and appropriate support for business continuity management.

Box 1: BT Plc

BT is committed to building resilience within the communications infrastructure and to providing continuity and integrity of services to its domestic clients and commercial customers. However, with such a complex and interconnected network it is difficult to accurately map and understand critical links that could lead to disruption of service. Therefore, BT builds its preparedness and capability to respond to events by providing national, regional and local resilience liaison and management, and actively engaging in exercises. BT has developed over 5500 site recovery plans and has over 100 mobile exchange recovery units in their fleet ready to respond and recover from events. The Emergency Operations Management Centres themselves all have mirror sites located across the country to ensure seamless management of disruptive events.

Consultation Questions:

1. Are these definitions for infrastructure clear and appropriate?
2. Does the use of the four components of resilience (figure 2) help to convey the need to think in broader terms than 'protection' when building resilience?

Section B: Building Resilience

B1. This section is intended to introduce an approach to building resilience based on the definitions set out in Section A. This approach is supported by the practical guidance provided in Section C for organisations that manage and operate infrastructure networks and systems, as well as emergency responders.

B2. The chapters in this Guide provide information and guidance for each of the segments of the infrastructure resilience model – see figure 3. This Guide is designed to fill the gaps in guidance and hence supplements existing business processes and industry guidance used by organisations to build resilience to natural hazards.

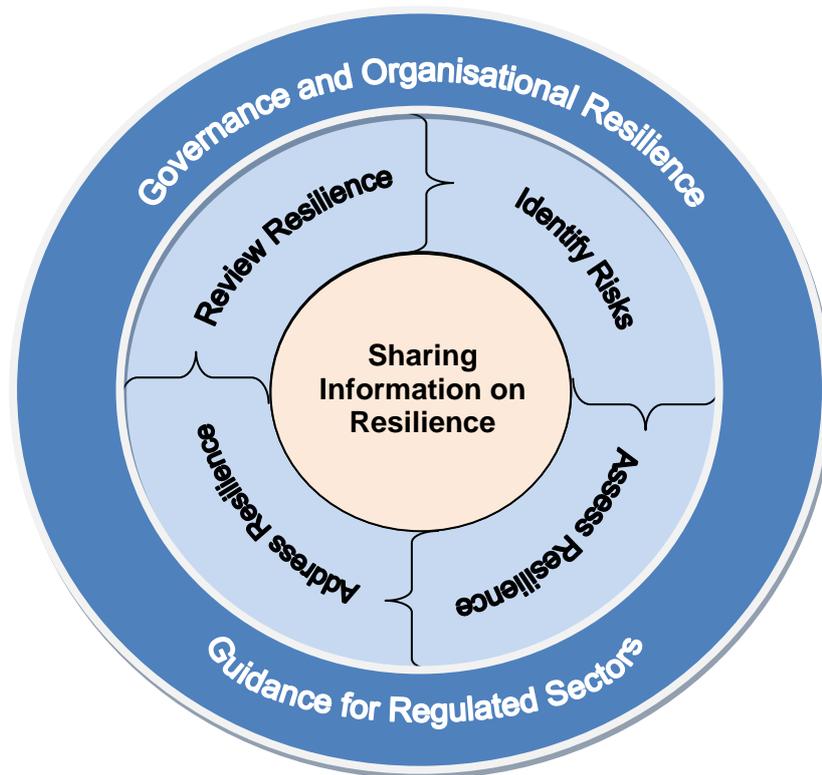


Figure 3: Infrastructure Resilience Model

FOR CONSULTATION

B3. The effectiveness of the four components of resilience (Resistance; Reliability, Redundancy; Response/Recovery) can be assessed using the resilience model shown in figure 3. This Resilience Model is based upon the risk model used within the public sector for management of risk⁷. The four basic steps of resilience building are described in the middle circle: identify risk, assess resilience, address resilience and review resilience. These four steps are supported by the outer circle representing the context and environment where resilience can be secured. Key to building resilience is the governance and attitudes to risk and resilience within an organisation. The regulatory environment for infrastructure in the UK is also part of the governance framework, and included in this guide is specific guidance for regulators (based on the interim guidance published in March 2010). Information sharing is at the heart of the resilience model. Sharing information on the risk of disruption to critical infrastructure is a vital element to ensuring the continuity of essential services during a civil emergency – this is considered in chapter 8.

B4. This Guide provides:

- Guidance on **natural hazards** to enable organisations to identify risks and assess resilience of their business operations (Chapter 3);
- Information to assist with a common understanding of resilience, the components for building resilience, and **standards of resilience** (Chapter 4);
- Information on the Lead Government Departments (LGDs) work to produce **Sector Resilience Plans** (SRPs) that assess the vulnerability and report the level of resilience of the most critical infrastructure to Ministers (Chapter 5);
- Guidance on how **Business Continuity Management** can be used to ensure continuity of essential services and embed resilience within an organisation to create 'organisational resilience' in the face of all kinds of risks of disruption (Chapter 6);

⁷ The Orange Book, *Management of Risk – Principles and Concepts*, produced by HM Treasury, establishes the concept of risk management and provides a basic introduction to its concepts, development and implementation of risk management processes in government organisations (http://hm-treasury.gov.uk/orange_book.htm).

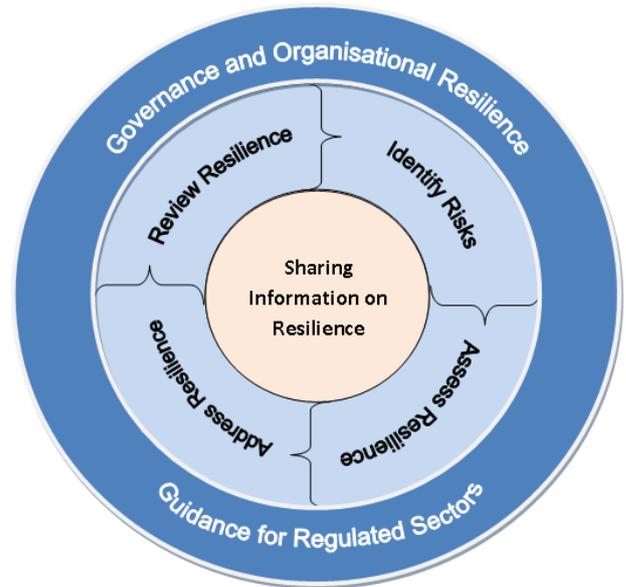
FOR CONSULTATION

- Guidance for the economic **regulated sectors** to consider in terms of how they may be able to support building resilience in their infrastructure networks and systems (Chapter 7); and
- Guidance to encourage and support **sharing of information on critical infrastructure**, to help organisations understand the dependencies between networks and systems, and to plan for the consequences of disruption of essential services within emergency response plans (Chapter 8).

Consultation Questions:

3. Is the structure and content of the Guide helpful and clear? Please suggest how either can be improved.
4. Does the Infrastructure Resilience Model clarify the process of building infrastructure resilience?
5. Should this Guide be published electronically on the UK Resilience website and National Resilience Extranet in parts to enable different audiences to access the relevant guidance / chapters?

3 Identify Risks and Assess Resilience: Natural Hazards



Risks from Natural Hazards

3.1 To improve resilience to natural hazards, organisations need the following information about the risks:

- knowledge of the likelihood, and frequency, of natural hazards of greatest concern and the linkage between different natural hazards;
- Knowledge of the likely primary impacts of different kinds of natural hazards on infrastructure operations and operators;
- Knowledge of the secondary impacts of hazards to other infrastructure operations and key supply chains; and understanding of the dependencies between infrastructures and essential services.

3.2 This chapter and the accompanying Guidance (see Section C: Guide 1) sets out the natural hazards most likely to affect infrastructure in the UK and provide guidance on how these hazards can affect infrastructure resilience.

Using the Guidance on Natural Hazards

3.3 The Government maintains a National Risk Assessment (NRA) process and, since 2008, a public National Risk Register, to indicate the most common types of emergency for which organisations and communities can prepare. The hazard descriptions within the guidance (Table A2) are drawn from the National Risk

FOR CONSULTATION

Assessment, and are based on a **reasonable worst case scenario for each type of hazard**. These reasonable worst case scenarios represent an upper limit on the risks for which the Government plans and against which infrastructure owners **and operators** can reasonably be expected to build resilience.

3.4 The natural hazards that can disrupt infrastructure include hydrological hazards (e.g. drought, floods), geological hazards (e.g. earthquakes, landslides and volcanoes) and climatic and atmospheric hazards (e.g. extremes of heat and cold, windstorm). They also include other risks not covered in this edition of the guide, but outlined in the National Risk Register, including: risks of disruption to operations from major industrial accidents, infectious disease of humans and animals, and malicious attacks by criminals or terrorist on infrastructure operations, including through cyber attacks.

3.5 Public sector emergency planners use guidance derived from the NRA to inform their own assessment of the likelihood and impact of disruption caused by the risks described in this guidance, in their local area. Similarly, infrastructure owners and operators can use the guidance along with their local knowledge to assess the risks to infrastructure operations and the impact of natural hazards on their organisations, supply chains and wider communities. This will enable organisations to set priorities and exploit opportunities and synergies within the business to deliver improvements in infrastructure resilience.

3.6 For some organisations or individual assets / networks these scenarios may already be met. Infrastructure owners and operators may chose to adopt higher standards of resilience implied by higher magnitude scenarios that could result in significant disruption or even destruction of service for the most critical assets (see Box 5 in Chapter 4 for an example of this activity in the energy sector). For less critical assets, infrastructure owners and operators may decide that a lower standard of resilience is justified on cost grounds.

3.7 Owners and operators of critical national infrastructure should be aware of the point at which their own organisation's viability will be irrevocably threatened and at which normal service delivery may not be able to be resumed with existing infrastructure and assets. A comparison between the natural hazard worse case scenarios and the industry design and service standards (see Chapter 4) will assist infrastructure owners and operators to identify gaps in resilience.

FOR CONSULTATION

Initial and secondary impacts of natural hazards

3.8 The natural hazards within the guidance are mainly drawn from the National Risk Register (2010), and include coastal flooding, inland flooding, storms and gales, low temperatures and heavy snow, heat waves, drought and volcanic ash.⁸ A scenario for severe space weather is also under development. The scenarios have been developed with Met Office, Environment Agency, the British Geological Survey and relevant Government Departments. But other hazards, with a low likelihood of national disruption such as landslips, are also included within the guidance because of their potential to impact on critical infrastructure at a local level.

3.9 Typically, a single natural hazard can carry a variety of challenges, beyond the initial event, for infrastructure owners and planners. For example, a prolonged period of hot 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 1 shows the relationship between different natural hazards (captured in the National Risk Register) and these knock-on effects.

Table 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 (at least five consecutive days)	Heat	Thunderstorms Drought Dust/Smog/haze Land instability Wildfire
Prolonged period of dry weather (developing over 3 years)	Reduced Rainfall	Dust/Smog/Haze/fog Reduced ground water flow Water quality Land instability Drought Wildfire
Excessive cold with snow	Cold Snow	Ice Ice accretion Wind chill Fog

⁸ www.cabinetoffice.gov.uk/intelligence-security-resilience/civil-contingencies-uk-resilience/national_risk_register.aspx

FOR CONSULTATION

		Surface water and river flooding (snow melt)
--	--	--

3.10 Where the risks of disruption by natural hazards cannot either be predicted, or mitigated, public sector emergency planners use national resilience planning assumptions. These are based on the NRA and set out a number of common consequences that should be planned for, setting an upper limit on the level of capability required in each instance. So, for example, the planning assumptions set out a range of numbers of casualties likely to be caused by the main kinds of emergency, and also an estimate of the type, extent and duration of disruption of essential services. These take account of the direct impacts of emergencies, and of second order effects. So the planning assumption for disruption of public telecommunications (that services might be lost at a regional level for up to three days) takes into account not only the main risks of human error, bad weather, or flooding but also the effects of a major loss of electricity supply on which telecommunications are dependent. Business continuity planning assumptions can also be derived from the analysis of risks in the National Risk Assessment, under the headings in Table 2.

Table 2: Categories of business continuity planning assumptions based on the National Risk Assessment.

Large-scale temporary absence of staff
Permanent or long-term loss of staff
Denial of site or geographical area
Loss of mains electricity
Disruption to transport
Loss of mains water and sewerage
Loss of availability of oil and fuel
Loss of telephone/mobile telephone communications

Longer-Term Risks of Disruption Caused by Changes in the Climate in the UK.

3.11 In testing resilience to natural hazards, and particularly when considering assets with a long life-span, future climates should also be considered. The UK Climate Projections (UKCIP) have been produced to help organisations understand the range

FOR CONSULTATION

of possibilities for the UK's future climate over the rest of the century against three different emission scenarios – low, medium and high.⁹

3.12 The projections describe how the climate of the UK might change throughout this century and attaches probabilities to different levels of future climate change. The projections allow users to consider the implications of uncertainties and risks in the design of infrastructure and investment decisions. This is important to build resilience of infrastructure to current and future natural hazards.

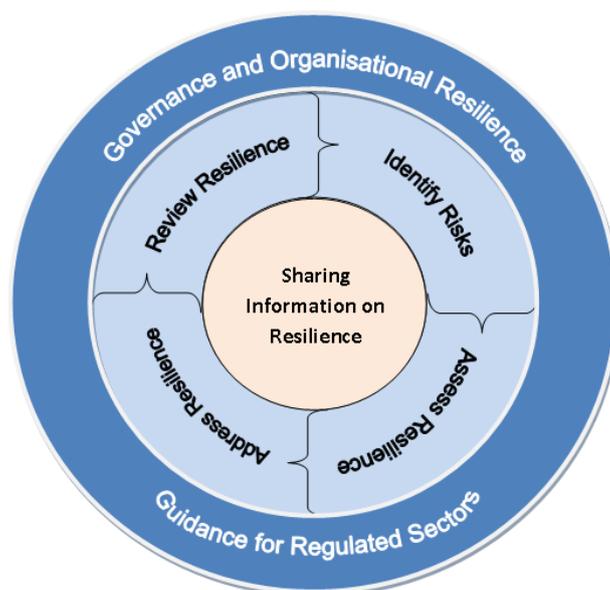
Consultation Questions:

6. Does the 'unrestricted' information on the hazards from the National Risk Assessment provide a reasonable basis for civil emergency planning for infrastructure?
7. Should this information on hazards be linked to the National Risk Assessment to ensure new risks are included in future updates of this guidance?
8. Is information required on any other risks not included in this current version of the Guide? If yes, please state which natural hazards?

⁹ <http://ukclimateprojections.defra.gov.uk/>

4 Address Resilience: Standards

4.1 There is no national standard for the resilience of infrastructure in the UK. The Pitt Review raised concerns about the existing level of resilience of critical infrastructure to disruption from the greatest natural hazard risk to the UK, flooding. The Review proposed “that the Government set out explicit standards against which investments could be planned and appraised”¹⁰ and suggested that a 1 in 200 (0.5%) annual probability event was a reasonable starting point to protect Critical National Infrastructure from flooding.¹¹



4.2 The Pitt Review proposed the standard be used to drive improvements in resilience using the range of responses, including network design, operational management (including supply chains) and business continuity. Taken together these actions drive up the organisation’s ability to resist and respond to multi-hazards and threats i.e. ‘all risks’.

4.3 The Pitt Review has acted as a catalyst for action across all nine sectors of the national infrastructure to improve resilience. Those organisations most severely affected by the floods in 2007 have invested or committed significant resources to improve the resilience against future floods.

4.4 The flood resilience standard, as suggested in the Pitt Review, provides a useful aspiration and guide to longer term planning and investment beyond regulatory price reviews and investment cycles. However, it should be viewed in terms of the broader approach to resilience consisting of the components of resistance, redundancy, reliability, response and recovery. Thus a more useful benchmark is that “**essential**

¹⁰ <http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html> (Page 264)

¹¹ <http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html> (Page 257-258)

FOR CONSULTATION

services provided by Critical National Infrastructure (CNI) in the UK should not be disrupted by a flood event with an annual likelihood of 1 in 200 (0.5%)”. Both regulators, where relevant, and utility companies should consider the cost/benefits of individual projects when determining which projects to fund and whether they can achieve this resilience standard for flooding. Actual levels of resilience for CNI should be monitored through the Sector Resilience Plans.

4.5 Specifying a flood resilience standard in terms of probability will ensure that the standard stays relevant in a changing climate, although it creates an evolving target. Building resilience will need to consider the impacts of climate change over the lifetime of the infrastructure and make allowances for the magnitude of future hazards in investment decisions to and secure the necessary adaptation over time.

4.6 The most likely reasonable worst case scenarios for natural hazards are introduced in Chapter 3 and presented in Section C: Guide 1. These scenarios should be used to challenge the level of resilience afforded by design and service standards, and identify gaps in resilience.

4.7 The Government has worked with regulators and industry to review the current levels of resilience of critical infrastructure and the need for standards for resilience to be established in the UK. Various approaches to defining standards were considered in relation to the four main components of resilience, including design standards, service standards, performance standards, event standards and maximum recovery time standards.

4.8 It is unnecessary to set ambitions for standards for every hazard for all assets, all sectors, and all durations. Such an approach would risk duplication of existing International and British Standards, be lengthy, disproportionate, and involve unjustifiable financial costs. Moreover, natural hazards do not necessarily occur in isolation but tend to be either simultaneous or consecutive; therefore an ‘all-risks’ approach to resilience building is more appropriate.

4.9 Existing standards establish industry requirements for the four components of resilience. For example, design standards for operating temperatures ensure that equipment has the **resistance** to damage from heat waves in the UK.

Overview of Infrastructure Standards

4.10 The UK's infrastructure is designed and built using a wide range of international and British engineering and design standards. **Design standards** are developed by industry and used to ensure infrastructure is fit for purpose and designed to operate in the range of conditions likely to be experienced in the UK (or worldwide for standard components - see Box 2 and 3). However, such standards are intended to protect the physical integrity of the asset, not necessarily the service. For example, an asset may not be destroyed by a flood event because of a good design standard, but it is nonetheless flooded and the service it provides may be lost for the duration of the event. Therefore, whilst design standards contribute to ensuring resistance and reliability of infrastructure, they alone are not necessarily sufficient to provide resilience to essential services.

Box 2: Communications Infrastructure

Mobile Communications towers are exposed on higher ground to wind storms and debris which could cause a tower to collapse. Additionally, exposed structures have increased ice formation which in turn increases the towers' vulnerability to high winds.

BS8100 provides a design standard for the design of communications towers within the mobile and broadcast industry. Factors taken into account are the life-time of the structure, the geographic location i.e. vulnerability to hazards, and consideration of other infrastructure in the area. Hence, mobile communication towers are designed to withstand wind, debris and other natural hazards and as a result are rarely disrupted by the weather in the UK.

Box 3: Design Standards in the Energy Sector

Electrical equipment such as transformers and circuit breakers are vulnerable to temperature extremes, which can lead to power outages. The design standard IEC 61936-1:2010 provides common rules for the design and the erection of electrical power installations so as to provide safety and proper functioning for the use intended.

IEC 61936-1 specifies a temperature range within which component parts of the electricity network should be designed to operate, for example outdoor

FOR CONSULTATION

components should function at ambient air temperatures of between -25°C and 40°C as calculated over a 24 hour period. Recorded extreme UK temperatures remain within this range, thus components designed to this standard would be expected to continue to operate during periods of extreme weather in the UK. In addition, critical circuits will have 2 levels of redundancy so that in the event of any minor faults the service will remain operational.

4.11 **Network design standards** consider the capacity of the network and the ability to re-route services in the event of failure. The spare capacity and ability to re-route significantly increase the resilience of essential services. The electricity transmission and distribution networks in the UK are very effective in the ability to control and manage the supply of services to prevent disruption as a result of the design of the network. However other sectors, such as water or transport, have less opportunity for re-routing owing to operating at near full capacity and the costs of providing redundancy within the networks.

4.12 **Service standards** are used in some sectors to provide customers with a level of expectation for the service provided. These vary from the time to answer calls received by customer services to the volume of water provided per day per customer in the event of disruption to piped services. Within the economically regulated sectors, specific secondary legislation sets obligatory service standards to which any company operating in water, energy and transport must comply. Examples of these service standards include service expectations, safety requirements, fault toleration levels, response / reconnection objectives and penalties for service disruption. For instance, the principal service standard for the water industry is the Security and Emergency Measures Direction (SEMD) (see Box 4). Regardless of the hazard, the SEMD includes a service level with penalties if companies fail to meet their service obligations. This is based upon each water undertaker's worst operational case scenario. Companies' compliance with SEMD is assessed annually and audited by external appointed certification teams.¹²

¹² www.cabinetoffice.gov.uk/media/349089/interim-guidance-ers.pdf

Box 4: Resilience through mutual aid: the Water Industry

Under the Security and Emergency Measures Direction (1998) water companies are required to provide plans to ensure provision of the water supply.

In 2004, the Water UK Council established a mutual aid protocol for all members to ensure delivery of water by companies during an emergency. The protocol includes agreements to share emergency equipment and support affected member company(s) during incidents. This enhances the resilience and contingency options available to the industry as a whole.

This protocol was amended following the lessons the industry learned from the 2007 floods. Issues addressed include number and readiness of assets, technical compatibility of assets, means of managing and deploying staff and the resilience of the scheme to cater for simultaneous events.

4.13 Service standards are useful to encourage building resilience within networks and systems, yet they often include 'exception' clauses in the event of severe weather or 'unexpected' operating conditions. In addition, penalties payable to customers for loss of supply do not reflect the actual cost and/or inconvenience to the consumer.

4.14 A maximum allowable **recovery time standard** could be specified for some industries and sectors. This would set clear expectations but the severity and scale of an event will vary considerably making the recovery time standard difficult to plan for and deliver. It will not be proportionate to the risks, and difficult to measure.

4.15 **Event standards** can be established to set a level of resilience against an extreme event that the network or system should be able to continue to operate without widespread loss or disruption to the essential services. Describing reasonable worst case scenarios for hazards will enable infrastructure owners and operators to identify and assess their resilience, and consider any gaps in resilience of an asset or network between the event and the actual or current design and service standards. An organisation's ability and capability to manage and respond to events greater than these reasonable worst-case scenarios is dependent upon their generic organisational resilience. Alongside this, infrastructure owners should consider in their business

FOR CONSULTATION

continuity plans the speed with which they expect to be able to restore services in the event of supply being disrupted for whatever reason, including events which are not specifically itemised or which are more serious or extreme than those covered in the reasonable worst case scenarios.

4.16 The standards described above each have a role in contributing to one or several of the four components of resilience (see Figure 2). By understanding existing standards, and how they are fulfilled, Government, regulators and infrastructure owners and operators can develop a cost-effective resilience strategy for critical infrastructure within their sector.

Box 5: Energy Sector Resilience

The UK energy sector under the direction of the Energy Networks Association (ENA) produced an *Engineering Technical Report on Resilience of Flooding of Grid and Primary Substations (ETR 138)*. The report outlined a risk-based approach to flooding as well as methods to improve resilience of services where technically feasible and economically viable.

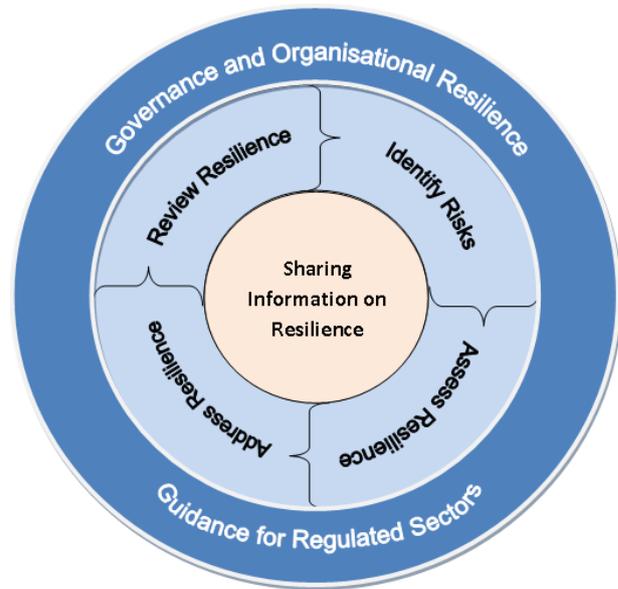
The electricity transmission and distribution industry has set out target levels (standards) of resilience for different assets within their sector, which includes a risk-based target of the 1 in 1000 (0.1%) annual probability flood for the highest priority assets within their Critical National Infrastructure. Other measures to improve resilience include the capacity to reconnect or provide an alternative energy supply to consumers.

This model of co-operation in the development of standards is being rolled out further to evaluate other hazards in the energy sector.

Consultation Questions:

9. Do you agree that a blanket standard for all hazards and all sectors would be disproportionate and unachievable?
10. Is this flexible approach that builds upon existing industry standards workable in practice?

5 Review Resilience: Sector Resilience Plans



5.1 Recommendation 51 of the Pitt

Review proposed that relevant

Government Departments and the Environment Agency should work with infrastructure operators to identify the vulnerability and risk of assets to flooding and a summary of the analysis should be published in Sector Resilience Plans.

5.2 This recommendation has been implemented and Sector Resilience Plans are now a key driver within Government to support and enable the continuous improvement in the resilience of critical infrastructure. The first Plans were produced in December 2009.

5.3 Sector Resilience Plans will be updated regularly (currently annually) by each lead government department, working with regulators and industry, as part of an ongoing assessment to increase government's understanding of the level of resilience of the UK's most critical infrastructure to natural hazards. Plans are developed for the nine infrastructure sectors: Water, Energy, Transport, Communications, Health, Emergency Services, Finance, Food and Government.

5.4 The Sector Resilience Plans will set out:

- a picture of risk and vulnerability for the entire sector developed by bottom up aggregation of risk and vulnerability analysis on a periodic basis;
- the levels of ambition for resilience across the critical infrastructure (based on standards of resilience and protection, economic incentives and business continuity planning for all risks);

FOR CONSULTATION

- a programme of measures (actions) for achieving the appropriate level of ambition for resilience, along with the timescales for delivery; and
- a mechanism for reporting progress on the implementation of the programme of measures and updating the plan on an annual basis.

5.5 The Plans will enable the lead Government Department to have a concise report on the current level of vulnerability and resilience in their sector, and a programme of measures to improve resilience where necessary.

5.6 The first iteration of the Sector Resilience Plans, completed in January 2010, reported on the resilience of Critical National Infrastructure (CNI) assets in each sector to coastal and fluvial flooding. Some departments also reported on the generic resilience in their sector, exercise programmes, business continuity planning and on-going work with industry and regulators to build resilience to flooding. An example of good practice is the approach being taken for the Government sector, see box 6.

5.7 Sector Resilience Plans are classified due to the sensitive nature of the contents, but, to encourage and support improvements in the collective resilience of the UK's critical infrastructure to natural hazards, the Cabinet Office will publish a summary of the Plans.¹³

5.8 The Lead Government Departments will continue to work with infrastructure owners and regulators to produce the Sector Resilience Plans to summarise the level of resilience in their sector to all risks (hazards and threats) and report to their Secretary of State. A summary of these reports will be produced for the National Security Minister and Advisory Council, and published.

¹³ The *Sector Resilience Plan for Critical Infrastructure 2010* can be found at www.cabinetoffice.gov.uk/ukresilience/infrastructure/resilience.aspx.

Box 6 Example of good practice: Business Continuity Management and Independent Internal Reviews

A requirement for Government Departments to undertake business continuity management is set out in the Security Policy Framework.¹⁴ Departments are supported in their business continuity planning through a Cabinet-Office led cross-departmental forum. To ensure a level of consistency and an objective review of the quality of planning by departments, the Government uses a system of Independent Internal Review.

The Independent Internal Review is a process jointly owned between the Cabinet Office and the staff of the Emergency Planning College. This process combines the expertise of central government and private sector security-cleared staff with in-depth knowledge of the public sector.

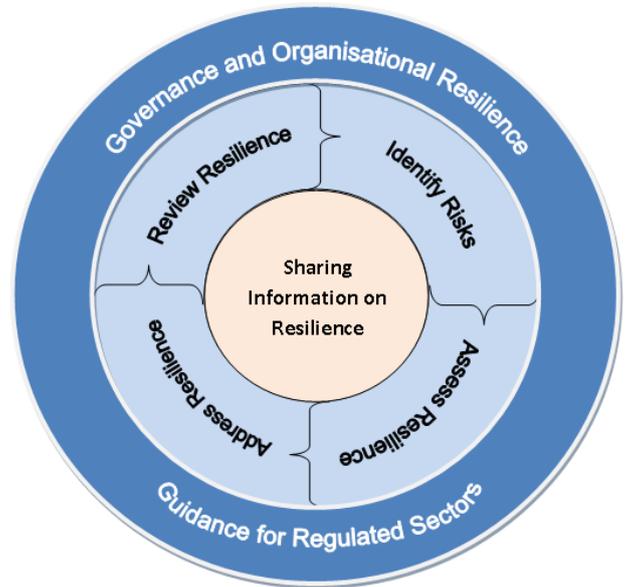
The Government will utilise the Internal Review process to assess the business continuity plans and management systems of Ministries and departments against the British Business Continuity Standard BS25999. If a department can demonstrate alignment to BS25999 then the Emergency Planning College will award a certificate, valid for one year. If a certificate is not awarded, then any significant changes needed to the department's processes and management are outlined. This forms the basis of an action plan to meet the standard to drive departmental activity.

Consultation Question:

11. Are Sector Resilience Plans a helpful method to gain a regular high-level assessment of the overall resilience of infrastructure in each Sector? Please explain your answer, and suggest any further or alternative methods of assessing infrastructure resilience and/or monitoring progress.

¹⁴ HMG Security Policy Framework, version 4, Cabinet Office May 2010.
http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

6 Governance and Organisational Resilience



6.1 The Pitt Review stated that “the driver for business continuity and wider organisational resilience should be in the long-term interests of stakeholders and all those who depend on the organisation in some way.”

6.2 The dynamic and changing nature of risks means that to achieve resilience, a longer term commitment is necessary as part of a continuous improvement cycle. An ‘organisational resilience strategy’ that sets out how an organisation will identify, assess and manage the changing risks will support delivery of resilience. Such a strategy would ideally:

- outline the organisation’s aspirations for delivering improvements in resilience;
- determine what success, in terms of resilience, looks like for the organisation;
- identify specific resilience priorities over the short, medium and long term;
- match the organisation’s risk appetite (see Chapters 3 and 4 for more information on the risk from natural hazards and how to measure the vulnerability of an organisation’s critical infrastructure to risks);
- be influenced by discussions with supply chain partners and emergency responders;
- produce an action plan for achieving desired improvements in resilience;
- be reviewed at Board level at regular intervals; and

FOR CONSULTATION

- be positioned at the core of the organisation's corporate governance processes.

6.3 Governance is defined as “the combination of processes and structures implemented by the Board (senior management) to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.”¹⁵

6.4 Embedding organisational resilience into governance mechanisms should ensure that the vulnerability of critical infrastructure to disruption from natural hazards is considered by the Board alongside other organisational priorities. Thereby, informing strategic investment and procurement decisions, risk management and discussions with supply chain partners. It would enable infrastructure owners and operators to improve their understanding of the resilience of their infrastructure, measure the success of the strategy at regular intervals, and make necessary amendments to secure delivery or to match changing organisational priorities.

6.5 As part of the organisational resilience strategy, infrastructure owners and operators may aim, where proportionate, to maintain business continuity plans that meet the requirements of the British Standard, BS 25999, for Business Continuity Management. This is a benchmark standard for corporate resilience and enables organisations to challenge business processes and decisions to improve their ability to manage disruption from natural hazards.

6.6 Meeting the requirements of BS25999 certification may be disproportionate. For example, infrastructure owners may already be legally obligated to maintain high quality business continuity plans or, for smaller firms in particular, the cost may be too high. However, organisations may find it valuable to review BS 25999 to assess whether following the principles and process within the British standard would strengthen their current business continuity arrangements.

6.7 The Government's Corporate Resilience Strategy is being developed to support the thousands of small businesses where it may not be appropriate or cost-effective to comply fully with BS25999. This Strategy is taking a holistic approach to encourage organisations to adopt and embed business continuity management within their operations. The Strategy advocates a standardised approach to guide business to best practice in business continuity management and provide a 'gateway for the standard' for those businesses unfamiliar with the discipline.

¹⁵ HM Treasury. Internal Audit Standards. April 2009. Page 35.

FOR CONSULTATION

6.8 In summary, to derive resilience, infrastructure owners and operators may wish to produce an organisational resilience strategy that:

- fully integrates the resilience of critical infrastructure to natural hazards and other threats and hazards;
- is risk based incorporating, where appropriate, the components of resistance, redundancy, reliability, response and recovery;
- is developed / reviewed with stakeholders (including supply chain partners, customers and emergency responders) to strengthen the collective resilience of the supply chain;
- encapsulates Business Continuity Plans that aim to either meet the requirements of, or incorporate elements of the British Business Continuity Standard, BS 25999; and
- is designed, implemented and reviewed at Board Level and embedded in corporate governance processes.

6.9 **Section C: Guide 2** provides a checklist of questions intended 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.

Consultation Question:

12. Do you agree with the need to ensure resilience is incorporated into corporate governance? Please explain your answer, and suggest any further action that would help to achieve this.

The Cabinet Office would like to receive examples of good practice of embedding resilience into corporate governance and/or approaches to creating organisational resilience that can be shared within the resilience community.

7 Guidance for Regulated Sectors

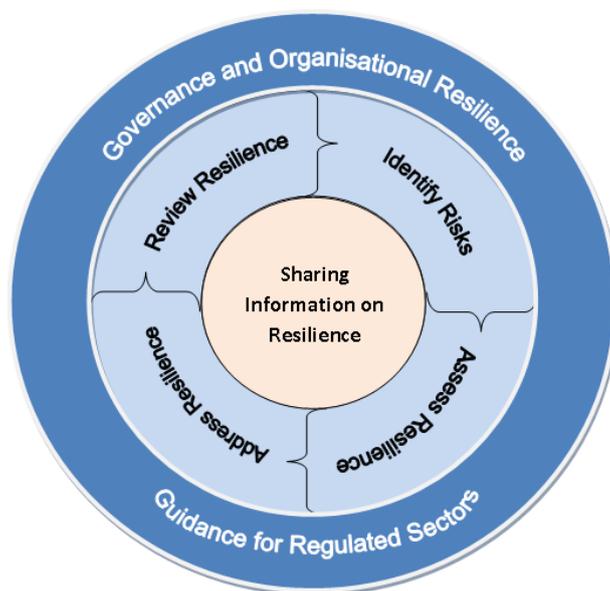
Regulators' Role in Building Resilience

7.1 Of the nine national infrastructure sectors, sub sectors of the energy (electricity and gas), transport (rail and aviation), communications (telecoms, broadcasting and postal services) and water sectors are regulated by economic regulators.

7.2 Regulators have a key role in supporting the resilience agenda, and the Pitt Review recommended that this was recognised by 'placing a duty on economic regulators to build resilience'. Since 2007, regulators have acted within existing structures and legal frameworks to achieve significant results in building both physical resilience in critical infrastructure and general response capability. Clearly, continued and sustained co-operation and action by regulators will negate the need for the Government to place a specific duty on regulators to build and/or maintain resilience.

7.3 The relationships between Government, Regulators and industry in the economically regulated sectors are important to support the building of resilience. By working together the legislation and regulations can be used to secure the right attention and level of investment for resilience measures.

7.4 In March 2010, the Government published 'Interim Guidance to the Economic Regulated Sectors' to assess whether new resilience duties should be assigned to the regulators. The objective was to encourage discussion within sectors and provide evidence on how, or whether, the regulatory framework of the UK needed to be changed to facilitate higher levels of resilience, or if changes were necessary to sustain their positive action to improve resilience in the long-term. Eight considerations for action were suggested to regulated sectors. Co-ordinated responses from each



FOR CONSULTATION

sector were encouraged as a means to demonstrate capacity and willingness to discuss challenging issues and co-operate to build resilience. The responses and ongoing discussions have provided the evidence for the guidance set out throughout this Guide, although specific issues for the regulators are discussed below.

7.5 The eight considerations were based upon best practice across the main utility sectors of water, energy, transport and communications. The eight considerations have been updated (see box 7) based upon the responses from regulators, but remain worthy of further discussion between the Government, regulators and industry as regulatory duties evolve.

Box 7: Eight Considerations for Regulated Sectors

1. Reporting on resilience. As society increasingly becomes risk averse and prioritises security of supply and resilience, consideration should be given to the incorporation of a specific resilience section in infrastructure owners' annual reports.

2. Vulnerable site monitoring schemes. Consideration should be given to establishing a monitoring and reporting system for the most vulnerable critical infrastructure in each sector.

3. Business Continuity Management (BS25999). Consideration should be given on the best means to drive up adoption of BS25999, or equivalent standards, and the benefits of external auditing or review.

4. Inconsistent standards. Consideration should be given to assessing and monitoring actual standards of infrastructure resilience and how to share such information within and across sectors.

5. Formalising innovative funding initiatives. Consideration should be given to co-ordination of research initiatives on resilience across sectors.

6. Improving resilience business cases. Consideration should be given to the evaluation and weighting of corporate reputational, social and environmental benefits of building resilience within infrastructure cost benefit analyses and investment decisions.

7. Exemption clauses in service standards. Consideration should be given to the appropriateness and role of exemption clauses or limitations of liability in service and performance standards as an incentive to build resilience.

8. Data impact on financing redundancy. Consideration should be given to: (a) how high probability low impact event data is used in assessing the probability of low likelihood, high impact events, and the need to build resilience for such events, and (b) the greater value of building redundancy within the network rather than protection of sites for a single hazard.

A duty to build resilience

7.6 The existing regulatory framework should be exploited to its full potential before any new or additional duties for regulators to build resilience are considered. Legal duties already exist within the regulations which could be used support the building of resilience within the sectors. Regulators have varying remits and duties; nevertheless, these duties are not static. The government has the right to notify the regulators of new environmental, social or economic considerations. Natural hazards are essentially 'environmental and social' considerations, hence a basis exists which can be used to direct the activities of the regulators. As regulations are formally reviewed and updated, the Government will consider whether amendments to the regulations are required to support improvements in security and resilience of the critical infrastructure.

7.7 There are varied levels of engagement and comprehension of resilience within the sectors. Regulators, infrastructure owners and operators, and Government all have a key role in ensuring that there is a good understanding of the level of resilience within their sector and opportunities are taken to improve resilience where necessary.

7.8 The Digital Economy Act 2010 has provided Ofcom with a specific duty to report to Government on resilience in the communications sector. This is welcomed and other Lead Government Departments should consider whether similar requirements on their regulators would support understanding of resilience within the sector, and reporting of that resilience in the Sector Resilience Plans. Additionally, the revised European Electronic Communications Framework Directive contains new requirements to enhance the security and resilience of communications networks and services and minimise disruption to them. Legislation will be in place by May 2011 and will include new enforcement powers for Ofcom and an obligation on network providers to report events that have a significant impact on their networks.

7.9 More informally, several sectors have established forums to discuss resilience matters and promote this understanding, for example, the Electronic Communications – Resilience and Response Group. This understanding should be shared with Government, again, to inform the Sector Resilience Plans.

Financing Resilience

7.10 Traditionally, there has been huge variance in the business cases made for resilience in the economically regulated sectors. A particular issue is that historic data, based on small scale low level outages and service disruptions, has been used to inform business cases. This limits support for initiatives to improve resilience to natural hazards, which are often low likelihood, high impact events, for which there is limited historical data.

7.11 Better knowledge of the risks of natural hazards will support full application of risk based decision making and improved mechanisms for managing uncertainty in these decisions. The reasonable worst case scenarios provided in Guide 1, and the UK Climate Projections,¹⁶ should be used to test current levels of resilience and used in future investment decisions to improve the infrastructure network and its long-term resilience. Ofwat has already published a guide to good practice in this area for the water sector.

7.12 Improvements in innovation investment could also lead to improved financing for resilience projects. In recent years, there has been decreasing investment in innovation within some economically regulated sectors. Ofgem has responded to this by establishing an Innovative Funding Initiative, allowing 0.5% of annual regulated revenue to be spent on research and development. In future, awards could be used to highlight successful innovation across all sectors.

Engagement of Unregulated Sectors in Civil Emergencies

7.13 The unregulated sub-sectors (such as oil, energy generation, satellite communications, providers of ICT) operate in free, open markets with no monopoly; there is no scope for extending existing regulations to improve resilience.

7.14 Establishing communication and co-operation between government and key national organisations in advance of civil emergencies will aid co-operation and support during national emergencies. A voluntary approach gives foresight of obligations to partners without requiring a complex and disproportionate arrangement.

¹⁶ <http://ukclimateprojections.defra.gov.uk/>

FOR CONSULTATION

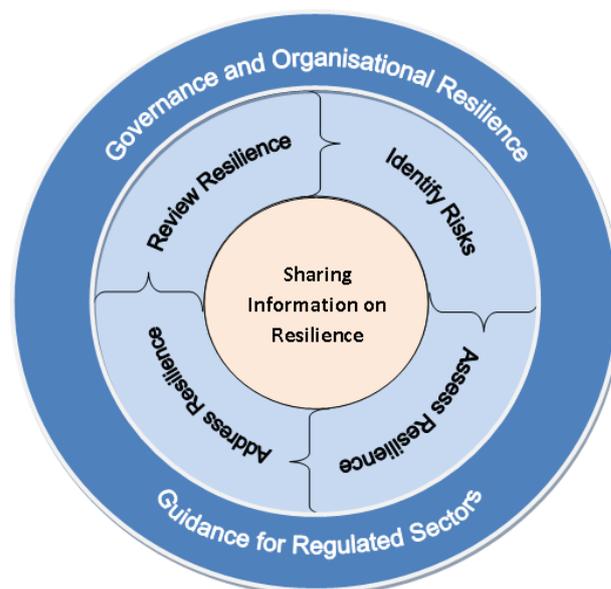
7.15 There are examples of active co-operation between key regulated, lightly regulated and unregulated industries based on a 'memorandum of understanding'. For example, the Electronic Communications - Resilience and Response Group operate under a voluntary memorandum of understanding. This provides a regular opportunity for the UK telecommunication industries to discuss resilience innovation and challenges without a mandatory structure based upon secondary legislation or intrusive regulation.

7.16 The use of a memorandum of understanding approach with lightly or unregulated industry should be considered to encourage and predefine collaboration during national emergencies.

Consultation Questions:

13. Is this guidance helpful for organisations in the economically regulated sectors?
14. Is there any further support needed from Government to enable regulated sectors to build resilience in infrastructure?

8 Sharing Information and Assessing Dependencies



The Need to Share Information

8.1 Since the 2007 floods, concerns have been raised by both Category 1 and 2 responders (as defined under the Civil Contingencies Act 2004) that information on critical infrastructure, especially Critical National Infrastructure (CNI), is not being shared with the right people at the right time for civil emergency planning.¹⁷

8.2 Sir Michael Pitt's evidence indicated that the response to the 2007 floods was compromised by the lack of awareness of the consequences of loss of critical infrastructure. He said there was a need to shift the thinking from the "need to know" to the "need to share".

8.3 To develop and enable an effective emergency response to civil emergencies there is a 'need to know' information on critical infrastructure and the consequences of loss or disruption prior to an event and put the necessary plans in place. For the purposes of civil emergency planning, it is necessary to understand:

- a) what infrastructure provides essential services in an area and/or at a national level, and its dependencies;
- b) the risks (likelihood and impact) of disruption to that infrastructure from natural hazards and threats; and

¹⁷ The legal obligations and general principles for sharing information under the Civil Contingencies Act (2004) can be found at: www.cabinetoffice.gov.uk/ukresilience/preparedness/informationsharing.aspx

FOR CONSULTATION

- c) the assumptions being made about assistance from emergency services e.g. pumping of flood waters by fire and rescue service.

8.4 There are several reasons why information is not shared on critical infrastructure including the classified nature of some information, commercial sensitivities and knowing what information is needed and what it will be used for. This chapter introduces a process in the form of guidance that emergency responders may wish to use to enable information on infrastructure to be shared more freely.

Guidance on Information Sharing

8.5 The information sharing guidance provided in Section C: Guide 3 uses the principle of 'right issue, right time, right level' in line with the statutory guidance for the Civil Contingencies Act (2004) (CCA).

8.6 The guidance has been developed to establish an approach for Category 1 and 2 responders to receive the necessary information on infrastructure to carry out their duties to best effect. It sets out an iterative process that supports the framework established by the CCA, and draws upon the duties on Category 1 and 2 responders, to ensure that the right information can be shared for the purposes of emergency planning and business continuity management (BCM).

8.7 The success of this approach is dependent upon establishing **effective relationships** between responders and infrastructure owners and operators. Many Regional Resilience Fora are actively encouraging and supporting this through a sub-group called a Utility Group / Forum, or Cat 2 Forum, or CNI sub-group. The forum is a mechanism for Infrastructure Owners / Operators to come together to discuss roles, responsibilities, critical infrastructure and dependencies. Key category 1 responders and other providers of essential services (who are not Category 1 or 2 responders under the CCA) should also be included and engaged as appropriate.

8.8 The process for information sharing is based upon the need for emergency responders to understand what infrastructure in its geographical area is critical to the delivery of essential services. The information is needed for two reasons: (a) to include loss of essential services in its Community Risk Register, (b) to include any responses that may be required for critical infrastructure to be included in the Category 1 responder's emergency response plans.

FOR CONSULTATION

8.9 The iterative process is set out in Figure 4 and is based upon all emergency responders working through a systematic approach: (Note: the process refers to LRFs, although it is intended to equally apply in Scotland, Wales and Northern Ireland).

(a) Understand the risks that could affect your community and

infrastructure. The members of the Local Resilience Forum should produce the community risk register using the Regional and Local Risk Assessment guidance and information on natural hazards.

(b) Ensure the resilience of your own assets. All emergency responders need to understand the resilience of their critical infrastructure (including police and fire stations etc) through business continuity management (BCM). The Community Risk Register should provide information on local risks.

(c) Share your resilience. Emergency responders should share information on their resilience with other relevant parties, particularly those within their resilience forum(s). Information shared should include generic standards for their sector, alongside specific information on the resilience of their critical infrastructure.

(d) Improve Knowledge of Critical Infrastructure. The Local Resilience Forum(s) should understand what infrastructure is critical in the local communities. This can include any elements that are determined by the LRF to be critical infrastructure (or critical local assets), such as a community centre or school, as well as the Critical National Infrastructure¹⁸ that provides essential services in the area. The process should also ensure a common understanding of which hazards may have a significant primary or secondary impact on the delivery of essential services in the community and dependencies between critical infrastructure.

(e) Develop specific local planning assumptions for the hazards that could affect your community. The knowledge of critical infrastructure and potential risks to disruption of services should be used to develop specific local planning assumptions for the Local Resilience Forum.

¹⁸ LRF members need to be aware of critical infrastructure, but only key members of the LRF will need to know if it is labelled as CNI. Information on CNI needs to be protected in accordance with government guidance.

FOR CONSULTATION

(f) Update Emergency Plans. Improved knowledge on critical infrastructure and local hazards should be used to update the Community Risk Register and inform emergency response plans and investment decisions.

8.10 The process has been developed based on existing good practice. Many infrastructure owners and operators recognise the need and benefits of occasional meetings to share knowledge and information on their assets and emergency response arrangements. In several regions across England, formal Regional Utility Groups (Category 2 Forums) have already been established. The London Regional Utility Forum includes senior representatives of utility companies and other responders, who meet three or four times a year to share information and plan for civil emergencies. The NW Regional Utility Group has been operating for several years and has developed excellent relationships between infrastructure owners and operators. Members are now able to attend LRF meetings and raise issues on behalf of other organisations in the Utility Group, and feedback to the other members.

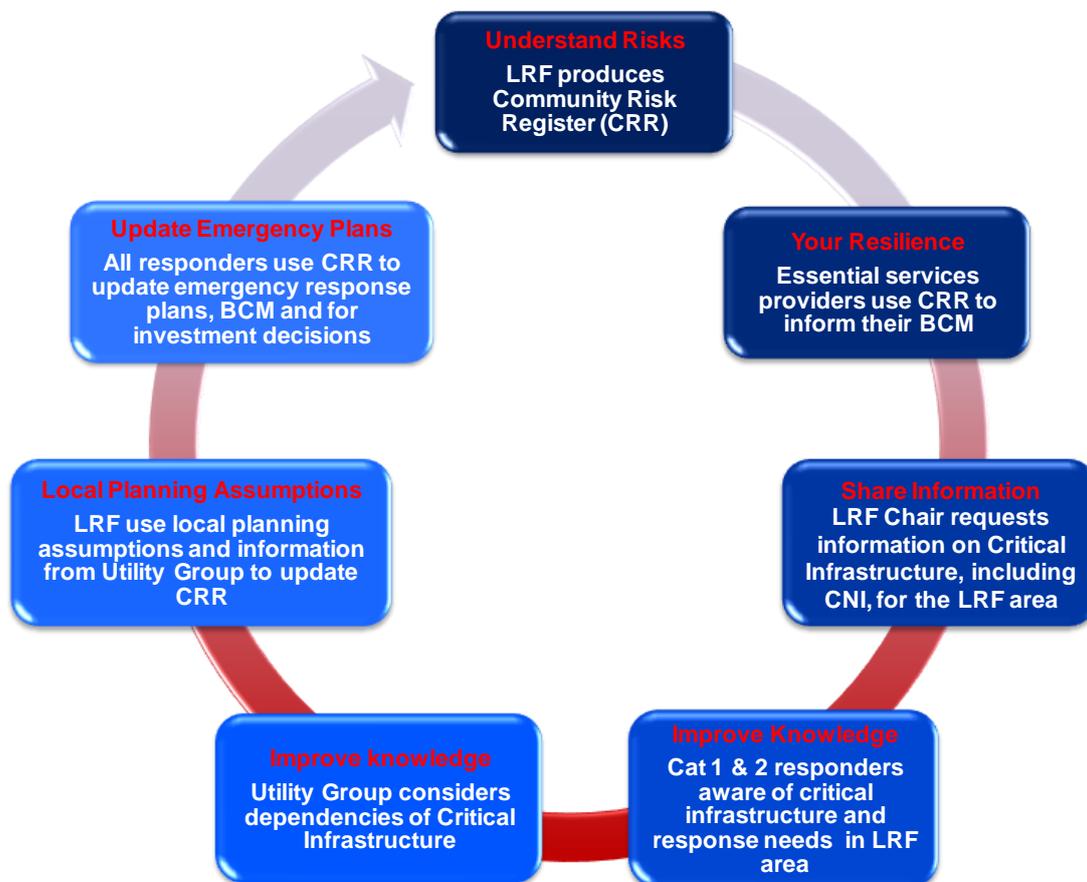


Figure 4: Iterative process to support information sharing for civil emergency planning (LRF = Local Resilience Forum, FRS = Fire and Rescue Service, BCM = Business Continuity Management)

FOR CONSULTATION

8.11 In other parts of the UK, the emergency responders have come together to undertake specific activities to improve emergency plans. The Lincolnshire approach to mapping critical assets is illustrated in box 8.

Box 8: Lincolnshire Mapping of Critical Assets Case Study

During 2010, Lincolnshire's Critical Infrastructure and Essential Services Group held a series of workshops looking at Critical Infrastructure along its coastal strip. These workshops were attended by local representatives and asset owners, including Anglian Water, CE Electric, British Telecom and five of the local drainage boards. The results will feed into the local Multi-Agency Flood Plan's community impact assessments.

During the workshops, organisations were asked to look at four issues: identifying assets; assessing their ability to continue to provide services during a flood; highlighting interdependencies between asset owners; and service restoration time frames.

The workshops were an opportunity to review and update Lincolnshire's GIS system, which already contains sites including telephone exchanges, electricity sub stations, water and waste assets, together with vulnerable community assets such as blue light services, rest centres and schools. Key locations were highlighted in which the impact of community flooding would be significantly worsened by infrastructure failure.

The Group noted that *"The workshop sessions have been an excellent way of gaining greater knowledge of infrastructure assets in Lincolnshire's coastal region, and the implications of a flooding event on the communities they serve...Local knowledge proved invaluable in providing the right kind of detail for the plan. Members of central emergency planning teams are less likely to have the full background knowledge on historical events or asset performance than the manager responsible for that area."*

8.12 The information sharing guidance recommends utilising the existing regional groups or forums of responders to share information on critical infrastructure and also discuss the dependencies between networks and systems. These Groups should provide co-ordinated advice to several Local Resilience Forums to ensure critical infrastructure and the loss of essential services can adequately be reflected in

FOR CONSULTATION

emergency response arrangements. The term Utility Group has been used throughout the Guide, although other terms can be used. These Groups are for emergency planning prior to events, and do not replace the need for infrastructure owners and operators to support Strategic Co-ordination Groups (SCGs) during a civil emergency. The benefits of partnership working in a Utility Group before an event will improve the provision of support to SCGs.

Understanding Dependencies

8.13 The floods of 2007 vividly demonstrated how a single event can have far-reaching implications as a result of knock-on consequences passed through the dependencies chain of critical infrastructure (see Figure 5). These relationships between infrastructure networks need to be understood to establish reasonable local planning assumptions for civil emergency planning.

8.14 Infrastructure dependencies are defined as the reliance by one piece of infrastructure on a service provided by another. There are two types of dependencies; **physical** and **geographical**. 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. 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. In addition, infrastructure can have interdependencies where assets are dependent upon each other. For example, electricity needs telemetry to run its operations whilst communications needs electricity to run its networks. Unknown dependencies and interdependencies often lead to emergencies escalating in unexpected directions through cascading failures. An example of geographical dependencies from the 2007 floods is shown in Figure 5.

FOR CONSULTATION

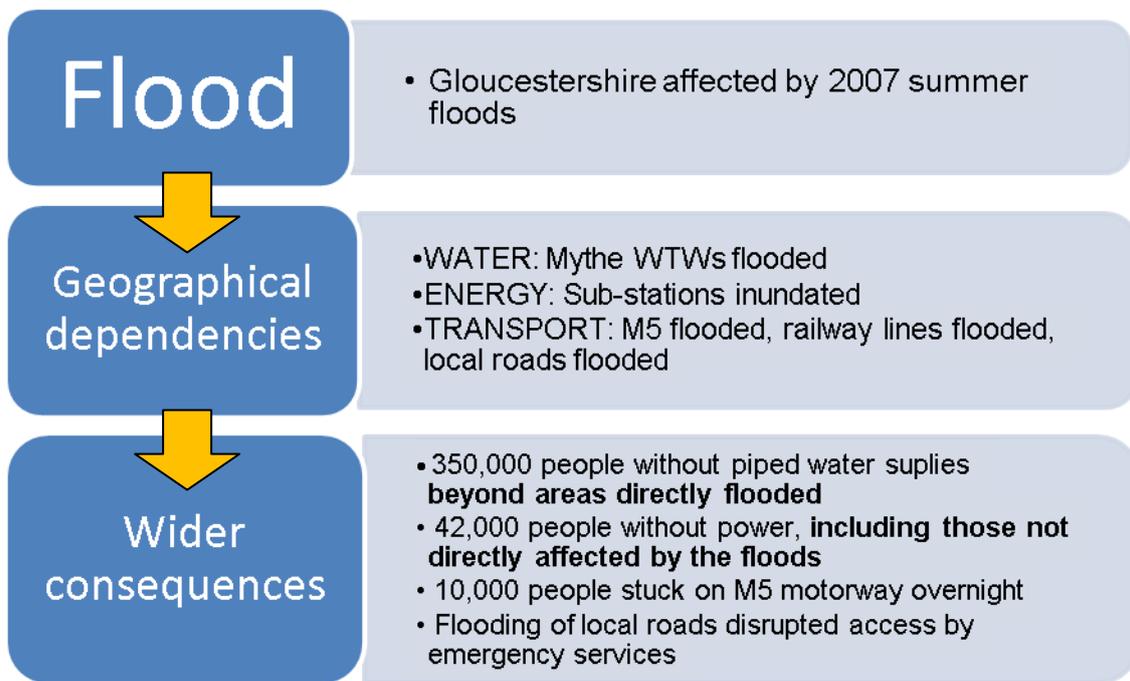


Figure 5: Geographical dependencies highlighted during the summer 2007 floods

8.15 There are examples within each of the nine sectors of national infrastructure of organisations having considered immediate dependencies as part of their business continuity management. However, this is not consistently and rigorously undertaken with sufficient knowledge of physical and geographical dependencies across networks.

8.16 The size and complexity of the infrastructure networks and systems across the UK mean that a complete understanding of the dependencies and interdependencies is not realistically achievable. However, bringing organisations together will enable discussion about the major installations and infrastructure networks that supply essential services to communities within a region.

8.17 To assist with this process, practical guidance is provided in this Guide to enable emergency responders and infrastructure owners and operators to work together and develop a sufficient understanding of infrastructure networks and dependencies across sectors.

8.18 Different approaches to assessing dependencies are set out in the guidance, again, based on existing good practice and are being piloted by resilience forums in England and Scotland.

FOR CONSULTATION

Consultation Questions:

15. Do you consider that this approach is suitable for Cat 1 and Cat 2 responders who do not already have arrangements in place to share information on critical infrastructure? Please explain your answer, and suggest any further clarification that is necessary.

16. The process for information sharing includes a step to determine planning assumptions for the loss of essential services in an LRF area. Would it be helpful for the Cabinet Office to produce national planning assumptions for loss of essential services?

17. Please provide any other comments you have on the consultation document.

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;
- 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 based on the National Risk Register 2010. 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 regional and 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 three sections:

A2.1 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 two additional hazards, volcanic ash 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.

A2.2 Lists some geological hazards for infrastructure owners and resilience partners that can also have an affect on critical infrastructure dependent on the specific characteristics of their location.

A2.3 Provides advice for infrastructure owners on next steps.

A2.1 Hazard Descriptions

The majority of natural hazards within this annex are drawn from the National Risk Register (2010), which seeks to capture the range of emergencies that might have a major impact on society (Figure A1) including: coastal flooding, inland flooding, storms and gales, low temperatures and heavy snow, heat waves and drought.

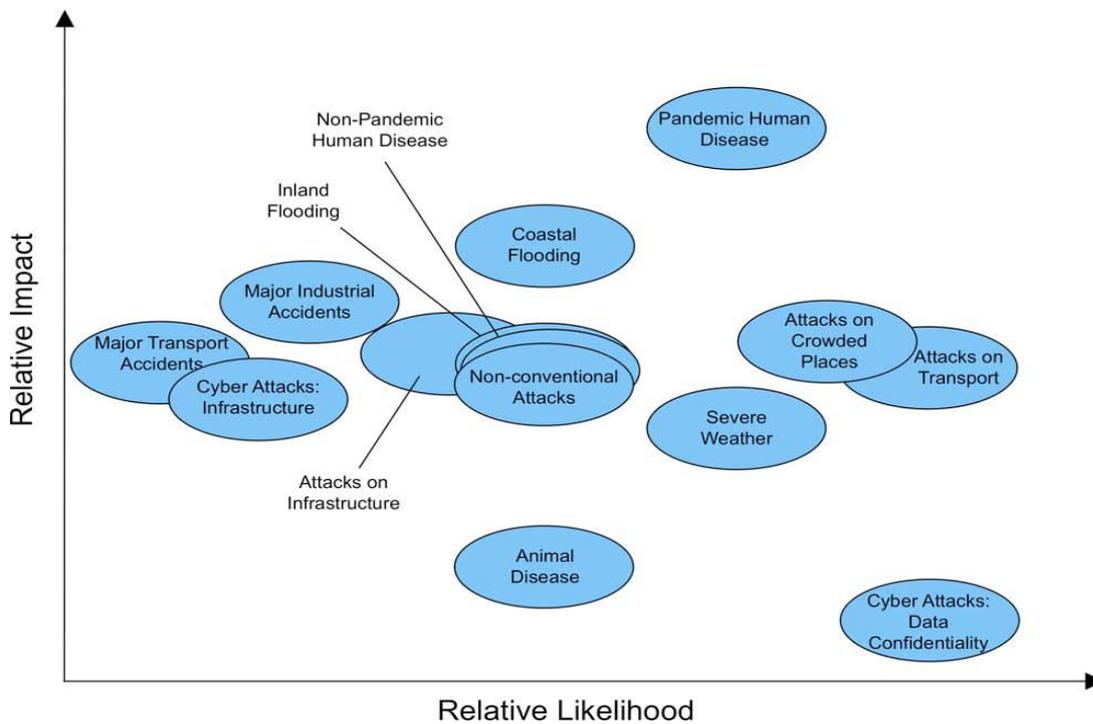


Figure A1: An illustration of the high consequence risks facing the United Kingdom¹⁹

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 A1 shows the relationship between different natural hazards, and these knock on effects and subsequent impacts on infrastructure are included within the hazard descriptions provided within the annex.

¹⁹ National Risk Register 2010

Table A1: The connection between different natural hazards events captured in the National Risk Register 2010

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 A2 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 and severe space weather.

Table A2: 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.	<ul style="list-style-type: none"> • 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;

FOR CONSULTATION

<p>Coastal Flooding</p>	<p>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.</p>	<p>Storms and gales Snow Land Instability (including offshore and submarine) Heavy rainfall.</p>	<ul style="list-style-type: none"> • 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;
<p>Windstorm: storms and gales</p>	<p>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.</p>	<p>Flooding Land instability Heavy rainfall Wildfire</p>	<ul style="list-style-type: none"> • Loss of power; • Loss of telecoms; • Blocked road and train routes and flight disruption;
<p>Excessive Cold</p>	<p>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</p>	<p>Storms and gales Flooding Land instability Ice</p>	<ul style="list-style-type: none"> • Loss of primary transport routes;

FOR CONSULTATION

<p>with Snow</p>	<p>of snow in excess of 30cm and a period of at least 7 consecutive days with daily mean temperature below -3°C.</p>	<p>Ice accretion</p>	<ul style="list-style-type: none"> • 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
<p>Prolonged Period of Hot / Dry Weather</p>	<p><u>Hot</u> Daily maximum temperatures in excess of 32°C and minimum temperatures in excess of 15°C over most of the region for at least 5 consecutive days.</p> <p><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.</p>	<p>Thunderstorms. Heavy rainfall. Flash Flooding. Drought. Dust. Haze. Smog. Land instability Wildfire.</p>	<ul style="list-style-type: none"> • 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;

FOR CONSULTATION

			<ul style="list-style-type: none"> • 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 Space Weather	Resulting from solar eruptions causing rapidly varying geomagnetic fields on earth. <i>Scenario under development.</i>	None.	<ul style="list-style-type: none"> • Loss of power supplies; • Loss of satellite communications and computer based control

FOR CONSULTATION

			<p>systems;</p> <ul style="list-style-type: none">• Disruption to monetary systems;• Loss of Global Positioning System (GPS)• Disruption to broadcast services.
--	--	--	---

A2.2 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.

FOR CONSULTATION

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 filled 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.

Checklist for Infrastructure Owners and Operators on Resilience

Identify Resilience

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 Resilience

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?

Address 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?

Review 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 regional and local resilience fora. 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 1) in line with the Civil Contingencies Act's statutory guidance. It enables emergency responders to adopt a risk-based and proportional approach to inclusion of the loss of essential services within emergency plans.

Table 1: “Right issue, right time, right level” Assessment²⁰

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.²¹

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.

²⁰ Further information on BPSS and National Security Vetting is available at: <http://www.cabinetoffice.gov.uk/media/420689/hmg-personnel-security-controls.pdf>

²¹ HMG Security Policy Framework, version 4, Cabinet Office May 2010. http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

CTSA's 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 1 - which is an appropriate standard for information on CNI for use during an incident.²²

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 figure 1. 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 Regional Resilience Fora are already actively encouraging and supporting this through Utility Groups or Cat 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 varying roles and

²² If the meetings of the SCG are occasional then BPSS is sufficient and there is no requirement for National Security Vetting to be undertaken.

responsibilities, and geographical areas of responsibility. The Resilience Fora 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 Cat 2 Forums operate in the first instance across several LRF areas.

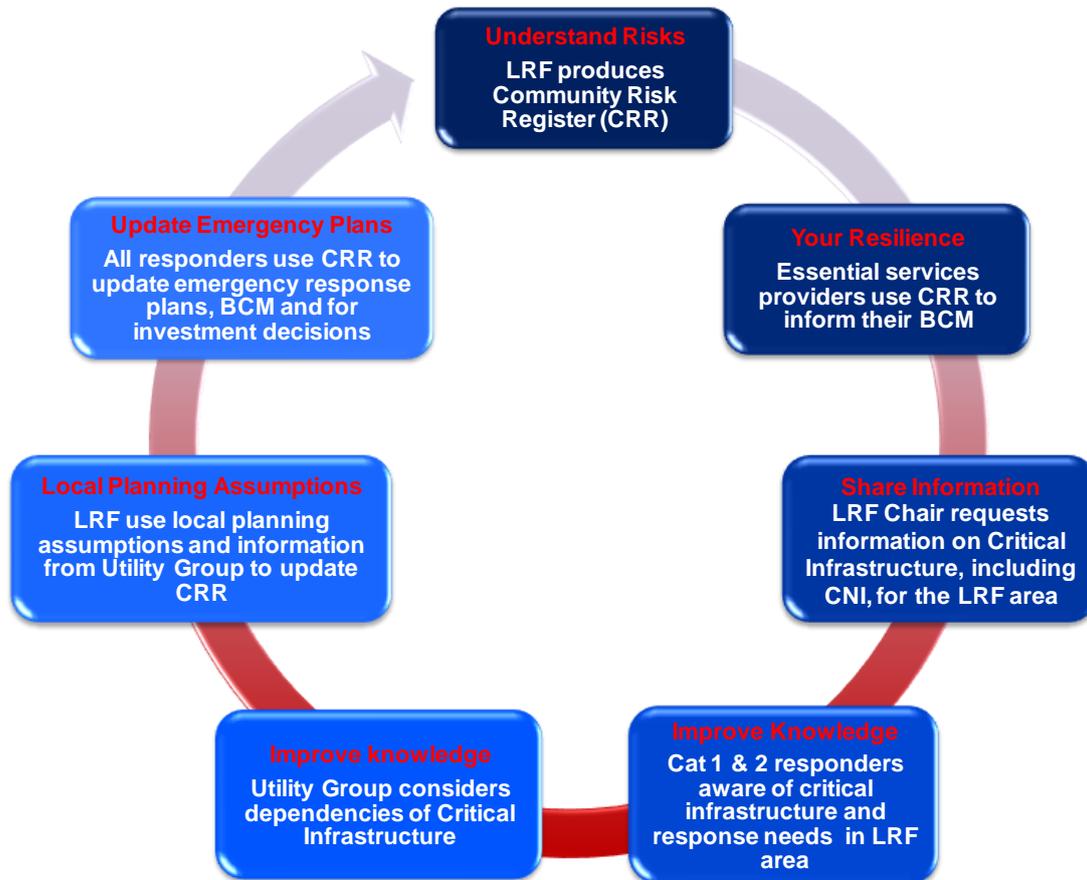


Figure 1: Outline of the approach to information sharing on critical infrastructure
(LRF = Local Resilience Forum, FRS = Fire and Rescue Service, BCM = Business Continuity Management)

Suggested Process

1. Category 1 Responders through LRFs to produce the Community Risk Register (CRR)²³ based on the Local Risk Assessment Guidance, National Risk Register, Planning Assumptions and new Guidance on Natural Hazards. This process

²³ Requirement under the CCA 2004

FOR CONSULTATION

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.

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. 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.

FOR CONSULTATION

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.

FOR CONSULTATION

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 2 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 (e.g. 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. 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.

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 for other Category 1 responders on a 'need to know' basis for the purposes of review their emergency response plans providing the individual(s) within those organisations are security cleared to a Baseline Personnel Security Standard (BPSS)²⁴ or above.

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.

²⁴ BPSS is sufficient for access Restricted and Confidential material and in some cases occasional Secret material.

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.

It is recommended that these groups cover a region or several LRF areas. 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. The Regional Resilience Forum (RRF) may wish to combine the Utility Group with a Regional Telecom Sub-Group (where it exists).

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 and recovery to 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.

FOR CONSULTATION

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. Category 1 responders and 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 and responder 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 prepared and prioritised 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 Regional Utility Group by infrastructure owners could reduce the need to regularly attend LRF meetings. The NW Regional Utility Group has established effective relationship between utility companies such that they are able to share attendance and represent other's 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.

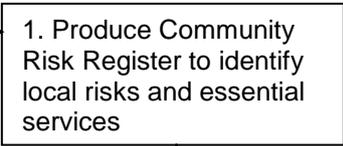
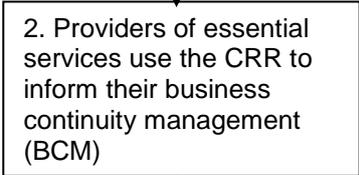
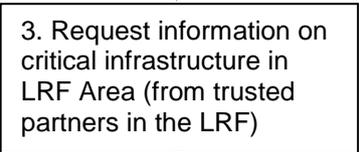
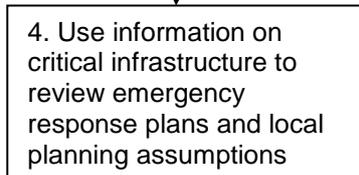
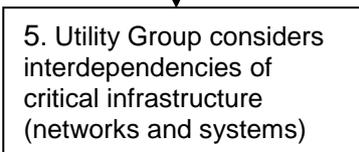
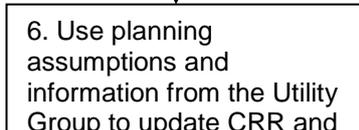
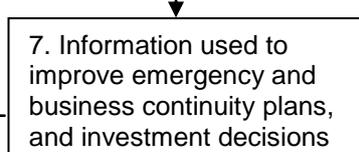
6. Category 2 responders use improved understanding of risk in preparing / revising their business continuity management arrangements, ensuring appropriate co-ordination between the plans.

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 Cat1 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.

CRITICAL INFRASTRUCTURE: INFORMATION SHARING FOR EMERGENCY PLANNING – OUTLINE PROCESS CHART

STEPS	WHO	COMMENTS AND LINKS
 <p>1. Produce Community Risk Register to identify local risks and essential services</p>	<p>Cat 1 Responders through the LRF</p>	<p>Current CRR process to be used to identify essential services in LRF area. Use Guidance on assessing vulnerability of infrastructure to natural hazards.</p>
 <p>2. Providers of essential services use the CRR to inform their business continuity management (BCM)</p>	<p>All organisations providing essential services in LRF area</p>	<p>BCM to cover essential services, critical infrastructure and supply chains. Refer to BS25999 or equivalent – see Guidance on Business Continuity Management for infrastructure.</p>
 <p>3. Request information on critical infrastructure in LRF Area (from trusted partners in the LRF)</p>	<p>Lead Cat 1 responder (e.g. Chair of LRF)</p>	<p>See guidance for list of information needed. Information to be protectively marked. Information must <u>not</u> be used for wider use or for commercial or political gain.</p>
 <p>4. Use information on critical infrastructure to review emergency response plans and local planning assumptions</p>	<p>Led by Police and Fire & Rescue Service</p>	<p>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</p>
 <p>5. Utility Group considers interdependencies of critical infrastructure (networks and systems)</p>	<p>Organisations providing essential services</p>	<p>See Guidance on assessment of vulnerability and dependencies provided by Cabinet Office. See example of Terms of Reference for Utility Groups provided by the Cabinet Office (based on good practice from existing RRF groups)</p>
 <p>6. Use planning assumptions and information from the Utility Group to update CRR and emergency plans</p>	<p>Category 1 Responders</p>	<p>Only unrestricted information to be used in publicly available version of CRR</p>
 <p>7. Information used to improve emergency and business continuity plans, and investment decisions</p>	<p>Category 1 and 2 Responders</p>	<p>Resilience of critical infrastructure to be taken into consideration for wider emergency response plans, and to inform investment decisions</p>

Guide 4: Guidance on Assessing Dependencies

This Guidance sets out a practical approach that could 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 point assets (sites) 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 Regional Utility Group, or a Cat 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 - either the National Resilience Extranet GIS capability (which is limited) or a full GIS package (as used by the local authority emergency planners). All information should ultimately be stored on a GIS system so other relevant information can be used with the critical infrastructure dependencies map.
- (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.

FOR CONSULTATION

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.

Strategic (National) dependencies mapping

In order to build resilience in critical infrastructure, it is essential that the ‘bottom up’ approach is tested now. However, a systemic approach can theoretically be used to map and then model the behaviour of networks and systems if there is sufficient data available. Both the USA and Australia have undertaken extensive work in this area, and the UK is now considering investment in such approaches.

The Technical Strategy Board (TSB) Project SATURN²⁵ is currently seeking to develop software which will be able to fuse data from multiple streams (and across business areas) which will enable the study of interdependencies. Similarly, the Centre for the Protection of National Infrastructure (CPNI) is developing the St. Pancras project, which is jointly funded by a number of Government departments and industry. This project aims to capture and analyse the multiplicity of dependencies centred on St. Pancras station in London, and model the impact of a disruptive incident. Although this project will certainly produce a wealth of useful information, it would almost certainly not be feasible in terms of cost and complexity to extend this type of in-depth study beyond a small sub-set of the critical national infrastructure sites.

Research commissioned by the Chief Scientific Adviser to DfT and BIS will also look at interactions between certain elements of the UK Infrastructure (Water, Waste, Energy, ICT, Transport).

Infrastructure UK’s Strategy for National Infrastructure²⁶ noted that increasing dependencies and interdependencies across sectors “need to be taken into account in investment decisions in order to reduce the risk that a failure in one network has unplanned consequences elsewhere”. The Strategy goes on to commit Infrastructure UK to lead a review to identify critical interdependencies that impact on infrastructure investment needs and to publish an action plan setting out the response to them by Spring 2011.

The aspiration in Scotland is to try to develop a methodology that is simple and easy to implement, using current process mapping software that is effective and commonly used (e.g. Visio).

²⁵ Self-organising Adaptive Technology Underlying Resilient Networks

²⁶ HM Treasury and Infrastructure UK. March 2010. Available at:

http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_186451.pdf

References

1. Infrastructure interdependency analysis: Requirements, capabilities and strategy. Produced for CPNI, TSB and EPSRC, under contract NSIP/001/0001 - Feasibility Study on Interdependency Analysis. Adelard LLP, 2009.
2. A National Infrastructure for the 21st Century. Council for Science and Technology June 2009.

Section D: Annex

Annex 1: Pitt Recommendations

Annex 2: Related Legislation

Annex 3: Example Terms of Reference for Utility Groups

Annex 1: Pitt Recommendations on Critical Infrastructure

RECOMMENDATIONS FROM “LEARNING LESSONS FROM THE 2007 FLOODS” AN INDEPENDENT REVIEW BY SIR MICHAEL PITT

(Allocated to Critical Infrastructure Resilience Programme).

Recommendation 50: The Government should urgently begin its systematic programme to reduce the disruption of essential services resulting from natural hazards by publishing a national framework and policy statement setting out the process, timescales and expectations.

Recommendation 51: Relevant government departments and the Environment Agency should work with infrastructure operators to identify the vulnerability and risk of assets to flooding and a summary of the analysis should be published in Sector Resilience Plans.

Recommendation 52: In the short-term, the Government and infrastructure operators should work together to build a level of resilience into critical infrastructure assets that ensures continuity during a worst case flood event.

Recommendation 53: A specific duty should be placed on economic regulators to build resilience in the critical infrastructure.

Recommendation 54: The Government should extend the duty to undertake business continuity planning to infrastructure operating Category 2 responders to a standard equivalent to BS 25999, and that accountability is ensured through an annual benchmarking exercise within each sector.

Annex 2: Related Legislation

Duties and obligations under which the economic regulators operate are not static. In this respect, new and existing actions need to be taken into account before additional obligations and duties are considered. The Government response to Pitt Recommendation 53 stated this position was to be taken. Therefore the overarching legislative framework and its ongoing evolution need to be placed in context before the need, scope and appetite for additional duties are considered.

There are three main areas currently in development which extend resilience duties to the economic regulators in the utility sectors. The main areas are *the Civil Contingencies Act (2004)*, the *Adapting to Climate Change Act (2008)*, and the *Planning Act (2008)*.

Civil Contingencies Act 2004

The *Civil Contingencies Act (2004)* provides a structure for co-operation and information sharing for emergency planning between Category 1 responders (emergency services, local authorities, Health Protection Agency and Environment Agency) and the Category 2 responders within the four regulated utility sectors. Under the Act, Category 1 responders have four core duties: risk assessment, business continuity management, emergency planning, and warning and informing the public. Category 2 responders have a duty to co-operate and share information to support Category 1 responders in fulfilling their duties. The principal mechanism for multi-agency co-operation under the CCA is the Local Resilience Forum²⁷ (LRF), established to ensure effective delivery of the above duties in a multi-agency environment. LRF activities include, among others, supporting the preparation of multi-agency plans, protocols and agreements and co-ordination of exercises and other training events.

At present, the *Civil Contingencies Act* is mid-way through an enhancement programme in which three relevant areas are being reviewed: increasing utilities'

²⁷ Civil Contingencies Act 2004 (Contingency Planning Regulations 2005 4 (2) (b) and 4 (3))

representation and information sharing, encouraging adoption of business continuity, and reviewing the current categorisation of responders.

Utilities are often represented on an LRF. The Act requires Category 1 responders to meet through the LRF at least every six months²⁸. Category 2 utility responders may be invited to attend and, in this case, need to make arrangements to be effectively represented. There are examples of LRFs and utilities providers working closely together²⁹ but there is inconsistency in representation and involvement which may undermine the systematic objectives of the Act. Options to address this issue are being considered in the Civil Contingencies Act Enhancement Programme.

Under the Act, business continuity is a key duty³⁰ of Category 1 responders. There is no matching obligation on Category 2 utility providers³¹. A duty for Category 2 responders to have emergency plans in place was supported in *Pitt Review* Recommendation 54 and is again being considered.

Pitt specifically mentioned BS 25999 or an “equivalent standard”. While BS 25999 is taken as a reference standard and is acknowledged and accepted as best practice in industry, some sectors have developed more specific industry standards. These would equate to Pitt’s “equivalent standard”. Whether BS 25999 based or an equivalent, a common approach based on established standards is an essential element in building parity-of-esteem and confidence between different categories of responders.

Responder categorisation has been static since 2004. Changes to the categorisation within the Act or the extension of the duties and/or the categories will be considered as part of the enhancement programme.

Even if the categorisation has been static, new Category 2 responders have been added to the list since 2004. As part of future-proofing of the Act, the enhancement programme will identify any other essential service providers who either are not currently categorised as responders, or who may need a new categorisation to cover their functions.

²⁸ Civil Contingencies Act 2004, Regulations 2005 4(4)

²⁹ Government Office East Midlands is holding a “Meet the Utilities” workshop on March 8 2010.

³⁰ Chapter 2, Emergency Preparedness

³¹ Civil Contingencies Act 2004 s.2 (1) (c)

Climate Change Act 2008

The *Climate Change Act (2008)* established new responsibilities for the water, energy and transport sectors and some involvement of the telecommunications sector. This grouping maps to the economically regulated utilities. The Act placed legally-binding obligations to report on carbon reduction as well as adaptation to long term climate change and its associated hazards.

The Adapting to Climate Change Programme (ACC) managed by the Department for Environment, Food and Rural Affairs (Defra), is a cross-government programme, associated with the Act and put in place to monitor and evaluate adaptation planning within the sectors over a 50 year timeframe.

The *Climate Change Act* established new powers for the government to ensure that organisations in key sectors are aware of, and prepared for, the impacts of the changing climate and is a key lever for the ACC programme. The adaptation reporting power within the *Climate Change Act 2008* gives the Secretary of State the power to direct public bodies and utilities companies, as “statutory undertakers”, to produce reports. There is no specified end point for the assessment of risk, and factors need to be considered that go beyond individual sector resilience.

Between July and November 2010, Defra will be directing organisations to report on how they intend to adapt to climate change and how this will be monitored and reported. Organisations to be directed cover the water, energy and the transport sectors. Defra will be inviting organisations in the information and communication technologies sector to report.

This adaptation work is broader than the work done by the Cabinet Office on sectoral resilience planning. The adaptation reporting powers provide a broader assessment of how future climates will change the demand and supply of essential services, and the challenges in ensuring service in the long-term.

Resilience information is a part of the information needed under the *Climate Change Act 2004*. The Cabinet Office is working with Defra to join-up information requests on emergency preparedness and sector resilience with the requests under the programme.

Notably, the ACC programme adds a secondary line of reporting directly to Defra on climate change actions, alongside that due to the lead government department on resilience.

Planning Act 2008

The *Planning Act (2008)* has led to a revised methodology for major infrastructure projects in the utilities sectors of energy, transport and water. The act covers “nationally significant” projects. The *Planning Act* provides for safety and resilience assessment in the initial considerations for new infrastructure investment.

In each of the three sectors identified in the Planning Act 2008, a series of National Policy Statements (NPSs) have been, or will be, produced. Together, they form an overarching framework in which the water, energy and transport networks’ long-term development must be viewed.

Currently, there is a suite of six NPSs in the area of energy, covering fossil fuels, renewables, gas and oil infrastructure, electricity networks and nuclear power. Co-ordinated by Department of Energy and Climate Change (DECC), these statements have been published and are part of an ongoing national consultation.

In the short-term, within the transport sector, there are three national policy statements managed by the Department for Transport (DfT). The Ports NPS is already published and the remaining two transport NPSs are to be given a deadline for publication.

In the mid-term, three water NPSs are managed by Defra. Their publication is scheduled for between the end of 2010 and into 2011. The water NPS will be framed by the extensive work already undertaken in response to the Pitt Review.

NPSs state that the entire lifespan of a facility is to be considered in the planning phase. This ensures adequate consideration for an all hazard adaptation programme. The NPSs include an “operational continuity obligation” as part of the initial planning assessment to ensure that essential infrastructure is designed to remain operational during floods.

FOR CONSULTATION

Planning Policy Statement 25: Development and Flood Risk (PPS 25), published in December 2006, introduced a risk assessment and sequential approach to development and flood risk. Wherever possible, construction on flood plains is avoided. If, in exceptional circumstances, it is decided that infrastructure must be built on a flood plain, mitigation actions must be included in the initial planning and cost analysis.

PPS25 is changing how essential services and infrastructure are located and designed. For example, the Tilbury Substation supplies hundreds of thousands of people on the flood plain around the Thames. However, due to the need for proximity of infrastructure to the serviced area, the substation *had* to be built on a flood plain. The mitigation plan required the entire substation to be built on stilts seven metres above ground level at an additional cost of seven million pounds. The cost of compliance was integrated in the operating costs by the asset owner.

Annex 3: Example Terms of Reference for Utility Groups

Aims

- To bring Category 2 and Category 1 Responders together to provide appropriate information to the relevant LRFs for planning, exercising and emergency response purposes.
- To improve Category 2 responders' understanding of their resilience and interdependencies, to support effective business planning.
- To develop the strong relationships, trust and confidence, which is invaluable in providing an effective response to an emergency.

Terms of reference

Initially, Group to agree principles on data protection and sharing of sensitive information.

Following this,

- To work with relevant LRFs to develop work programmes and make business decisions;
- To provide relevant LRFs and emergency planners with an assessment of key infrastructure interdependencies and possible cascade effects of infrastructure loss or service degradation, altering or adding to planning assumptions where appropriate;
- To provide the relevant LRFs and emergency planners with a summary of publically available infrastructure service and performance standards;
- To provide timely responses to requests from Category 1 Responders for further information on infrastructure resilience and to send representatives to LRF committee meetings, where appropriate;
- To improve understanding of infrastructure owners' roles and responsibilities in a civil emergency and their ability to restore services / provide alternative supplies;
- To share information on dependencies (including supply chain dependencies) for business continuity planning purposes; and

FOR CONSULTATION

- To provide Category 2 responders with the necessary information to represent others at task and finish groups and Gold Command, where appropriate / necessary.
- To maintain a Utilities Directory for each LRF area (if useful for sharing contact information and summary of key facts to support emergency response).

Membership

- All Category 2 responders with assets in the LRF area to be invited to attend.
- Key Category 1 responders (emergency services and LAs).
- Others, as agreed by a quorum. This may include other Category 1 responders, other relevant infrastructure providers and / or CTSA's as appropriate.

[Sectors to be provided with the opportunity to designate representatives, by a voting or rotation system, so long as these representatives are provided with sufficient information to meet their responsibilities.]

Frequency

- Meetings should be held as appropriate to progress this agenda. It may be necessary to meet quarterly for new Utility Groups.

End of document