Cabinet Office

## Keeping the Country Running:

# Natural Hazards and Infrastructure

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

Cabinet Office

Produced by:

Cabinet Office
70 Whitehall
London
SW1A 2AS

Contact:
Civil Contingencies Secretariat, Cabinet Office
www.cabinetoffice.gov.uk/ukresilience
naturalhazards@cabinet-office.x.gsi.gov.uk

Publication date: October 2011

## Acknowledgments

The Cabinet Office is grateful to the organisations that have supported the development of this Guide through their participation on the Critical Infrastructure Resilience Programme Board.

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 Government
Scottish Resilience
Centre for the Protection of National Infrastructure
Water Services Regulation Authority (Ofwat)
Transport for London
Water UK
Welsh Government

In addition we would like to thank the numerous organisations that have provided their thoughts and advice throughout the development of this document and, in particular, the fifty-two organisations that took the time to respond to the consultation to develop this final version.
.

# CONTENTS

## Overview

The National Security Strategy (NSS) sets out that one of Government's key tasks is to improve the resilience of the infrastructure 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.

The UK's critical infrastructure is a complex interconnected system. This Guide has therefore 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.

Divided into four sections, the Guide sets out the principles underpinning infrastructure resilience and provides advice and practical guidance on risk assessment for natural hazards, standards of resilience, corporate governance, information sharing and the role for economic regulators.

# Section A: Introduction, Definitions and Principles of Infrastructure Resilience

A1. 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 prioritised 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 shares best practice and advice to enable organisations to continuously improve their infrastructure's resilience to natural hazards. It supplements existing guidance and fills gaps identified during the consultation on the Strategic Framework and Policy Statement (March 2010). [1]

1.4 The Guide does not provide an assessment of the resilience of the UK's Infrastructure to natural hazards since this is addressed by Sector Resilience Plans (see Chapter 6), and the causes of the vulnerability of UK infrastructure to natural hazards, identified by the Pitt Review and the Institution of Civil Engineers' State of the Nation report, will not be restated in this Guide. [2,3,4]

[1] Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards: www.cabinetoffice.gov.uk/resource-library/strategic-framework-and-policy-statement-improving-resilience-critical-infrastructu

[2] Infrastructure Sector Resilience Plans: www.cabinetoffice.gov.uk/resource-library/sector-resilience-plan-critical-infrastructure

1.5 The Guide is divided into sections as follows:

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

## Background

1.6 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.

1.7 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 million.[5] Lost revenues, reputational damage, contractual penalties and the potential for litigation all provide a strong driver for organisations to manage risks and build resilience into their operations.

1.8 Many of the more detailed lessons from the summer 2007 floods were identified by Sir Michael Pitt in his review. The recommendations regarding infrastructure are listed in Annex 1. He highlighted the need for:

[3] The Pitt Review: http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html

[4] State of the Nation: www.ice.org.uk/information-resources/document-library/state-of-the-nation--infrastructure-2010

[5] The costs of the summer 2007 floods in England. Environment Agency January 2010.

- 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' responders in multi-agency response exercises in crisis management. [6]

1.9 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.

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

- a Strategic Framework and Policy Statement setting out the process, timescale and expectations for a Critical Infrastructure Resilience Programme;
- a Summary of the Sector Resilience Plans 2010; and
- Interim Guidance to the Economic Regulated Sectors.

## Infrastructure Resilience

1.11 The Government's approach is that the main responsibility for resilience of critical infrastructure lies with the owners and operators. But 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;

[6] 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.

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

1.12 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 Department for the Environment, Food and Rural Affairs on climate change adaptation.

1.13 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 and Principles of Infrastructure Resilience

## Definitions

2.1 In its definition of an **emergency**, the Civil Contingencies Act 2004 (the Act) includes events that could cause or threaten serious damage to human welfare or the environment in a place in the United Kingdom.

The Act states that:

- "An event or situation threatens damage to human welfare only if it involves, causes or may cause:

  I. loss of human life;
  II. human illness or injury;
  III. homelessness;
  IV. damage to property;
  V. disruption of a supply of money, food, water, energy or fuel;
  VI. disruption of a system of communication;
  VII. disruption of facilities for transport; or
  VIII. disruption of services relating to health."

- "An event or situation threatens damage to the environment only if it involves, causes or may cause:

  I. contamination of land, water or air with biological, chemical or radio-active matter; or
  II. disruption or destruction of plant life or animal life."[7]

This definition recognises that emergencies can arise through the disruption of supplies of goods and services as much as through the direct effects of the event causing the emergency. In relation to infrastructure, mutual reliance among infrastructure owners and operators on services from other suppliers is referred to as **interdependence.**

2.2 The national **infrastructure** comprises networks, systems, sites, facilities and businesses that deliver goods and services to citizens, and support our economy,

[7] The Civil Contingencies Act 2004: www.legislation.gov.uk/ukpga/2004/36/contents

environment and social well-being. Within the national infrastructure, nine sectors have been identified as providing essential 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; and
- companies / research organisations that hold information of particular economic or strategic value to the UK.

2.5 For the purposes of civil emergency planning, the emergency responders may need 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, or have other significant impacts on human welfare or the environment within the local area, or be needed to support an emergency response. The criteria for determining whether local infrastructure is critical is whether its loss would itself cause, or be likely to cause, a local emergency – see the definition of emergency under the Civil Contingencies Act in paragraph 2.1 above.

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.

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.[8] Through the National Risk Assessment (NRA), 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. This assessment is conducted annually and draws on expertise from a wide range of departments and agencies of government. The NRA 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) is the published 'unclassified' version of the NRA.[9] It summarises a range of civil emergencies and indicates the relative likelihood and impact (see Figure 1).

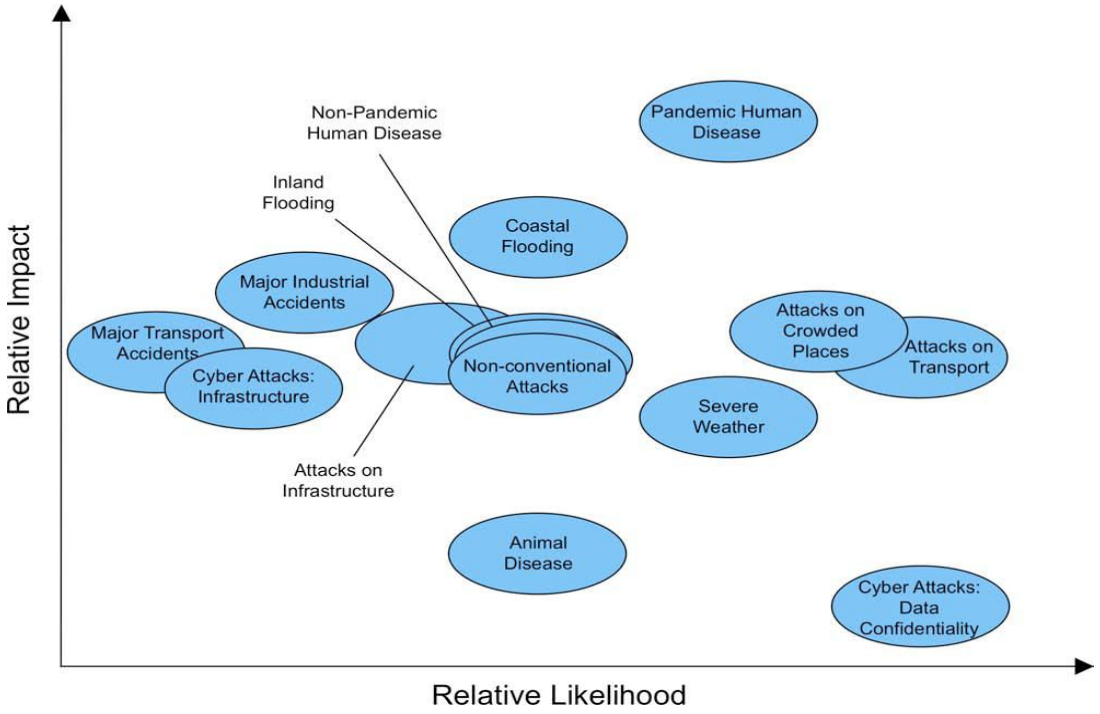



**Figure 1:** An illustration of the high consequence risks facing the United Kingdom.

[8] HSE, "reasonably practicable" guidance: www.hse.gov.uk/risk/expert.htm
[9] National Risk Register: www.cabinetoffice.gov.uk/content/risk-assessment

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

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, (Chapter 5).

2.11 **Resilience** is the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover from a disruptive event.[10] Resilience is secured through a combination of activities or components; the four principal 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.

[10] 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.


**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 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 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 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.

2.17 Chapter 5 encourages organisations to embed the assessment of resilience and subsequent organisational resilience strategies into corporate governance systems. This would allow infrastructure resilience to be considered alongside other

priorities such as customer or service user expectations, procurement strategies and long term climate change adaptation programmes.

### Managing supply and distribution chains, and understanding the risks posed by inter-dependencies

2.18 Infrastructure owners and operators should consider their dependency on supply and distribution chains, and inter-dependence on other infrastructure providers, as contributing to the external risk to their operations; and should manage these risks accordingly using the resilience model in this guide (see Figure 2) which is applicable to all kinds of risks. 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 an area.

2.19 Any assessment of existing levels of resilience should, therefore, include a review of an asset's supply and distribution chains. To do this effectively, infrastructure owners are encouraged to share information with organisations on which the delivery of their essential services depend, particularly other owners of critical infrastructure. These issues are discussed in more detail in Chapter 7, and Guide 3 and 4 provide guidance on information sharing and dependency analysis respectively.

**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 and local resilience liaison and management, and by 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.

## 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, in relation to infrastructure, for each of the segments of the Resilience Cycle (Figure 3).

B3. 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.

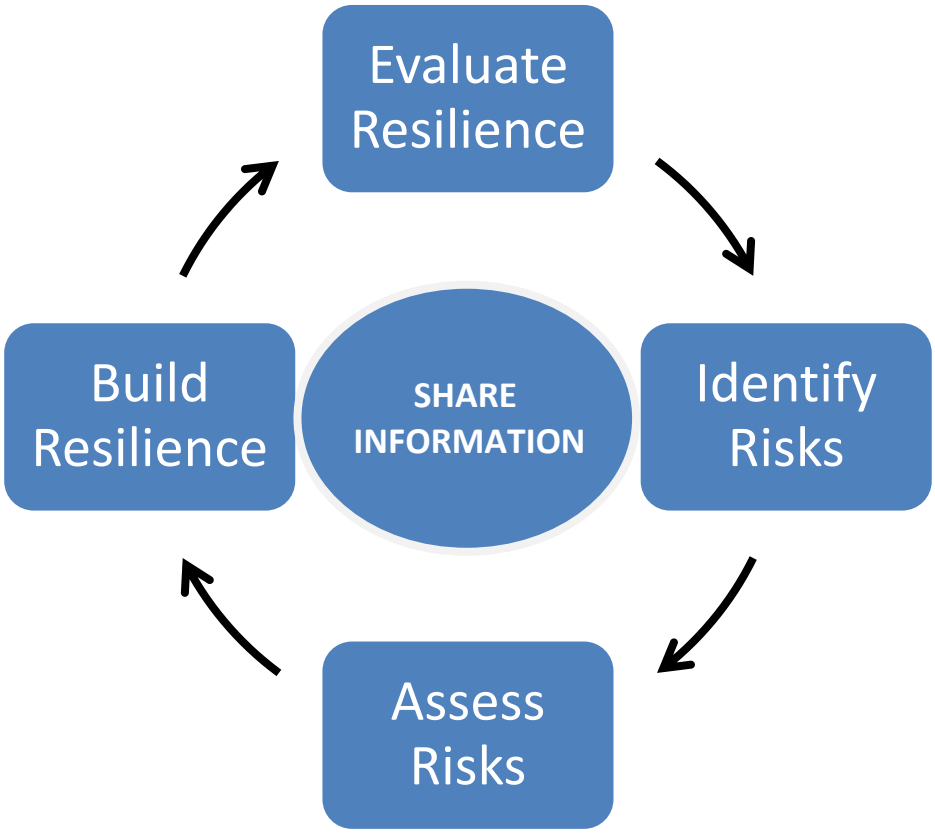



**Figure 3**: Resilience Cycle for Infrastructure Owners

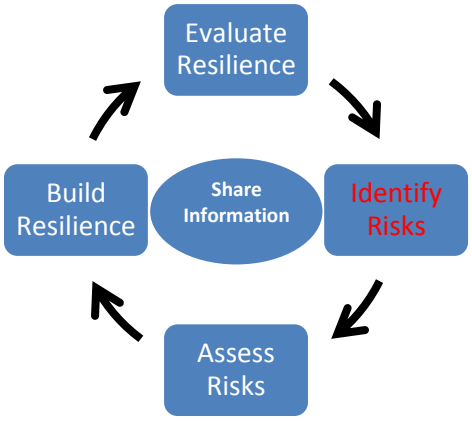
B4. The effectiveness of the four components of resilience (Resistance, Reliability, Redundancy and Response/Recovery) can be assessed using the Resilience Cycle shown in Figure 3. Key to building resilience is the governance of, and attitudes to, risk and resilience within an organisation. Where appropriate, the regulatory environment for infrastructure in the UK should be considered as part of the governance framework, and included in this guide is specific guidance for regulators (based on the interim guidance published in March 2010).[11] Information sharing is at the heart of building infrastructure resilience, and is a vital element to ensuring the continuity of essential services during a civil emergency – this is considered in Chapter 7.

B5. This section provides:

- Guidance on **natural hazards** to enable organisations to identify risks and assess resilience of their business operations (Chapter 3);
- Information to assist understanding of **standards of resilience** (Chapter 4);
- 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 5);
- Information on the work of Lead Government Departments (LGDs) to produce **Sector Resilience Plans** (SRPs) that assess the vulnerability and report the level of resilience of the most critical infrastructure to Ministers (Chapter 6);
- 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 7); and

[11] Interim Guidance for Regulators: www.cabinetoffice.gov.uk/resource-library/infrastructure-resilience-interim-guidance-economic-regulated-sectors

- 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 8).




# 3 Identify Risks: 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 (for example, how heavy snowfall can lead to flooding);
- knowledge of the likely primary impacts of different kinds of natural hazards on infrastructure operations and operators;
- knowledge of the secondary impacts of hazards including those caused by disruption to other infrastructure operations and key supply chains; and
- understanding of the vulnerability of the organisation to these risks, their primary impacts, and to secondary impacts including through dependencies on other infrastructure and essential service providers.

3.2 This chapter and the accompanying Guidance (see Section C: Guide 1) sets out a number of natural hazards judged most likely to affect infrastructure in the UK over the next five years (in the form of reasonable worst case scenarios).[12] It is designed to be a first stage in moving to an 'all-risks' approach to managing the risks of disruption to emergencies of all kinds.

[12] The "reasonable worst case scenario" of a particular risk is based upon historical and scientific data, modelling and trend surveillance and the professional judgments of experts. The justification for the phrase 'worst case scenario' being preceded by the word 'reasonable' in the National Risk Assessment is to prevent scenarios being formulated that are considered so unrealistic or unlikely that they are implausible.

## 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 (NRR), to indicate the most common types of emergency for which organisations and communities can prepare.[13] The hazard descriptions within Guide 1 are drawn from the National Risk 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), climatic and atmospheric hazards (e.g. extremes of heat and cold, windstorm). In the UK, the most prominent of these are set out in paragraph 3.8. Other risks not covered in this edition of the guide, but outlined in the National Risk Register, include: risks of disruption to operations from major industrial accidents, malicious attacks by criminals or terrorist on infrastructure operations, including through cyber attacks; and other naturally occurring events including infectious disease of humans and animals.

3.5 Public sector emergency planners use guidance derived from the NRA to inform their own **local risk assessment**. Similarly, infrastructure owners and operators can use this 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 emergency planners and infrastructure owners and operators to have a shared understanding of risk.

3.6 For some organisations or individual assets / networks, analysis of the four components of resilience (Figure 2) might uncover that existing levels of resilience already meet the challenge posed by these reasonable worst case scenarios. However, infrastructure owners and operators may choose to adopt higher standards of resilience for their most critical assets in order to avoid significant disruption or even destruction of service in a higher magnitude scenario (see Box 5 in Chapter 4

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

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 grounds of value for money

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 reasonable worst case scenarios and the industry design and service standards will assist infrastructure owners and operators to identify gaps in resilience (see Chapter 4).

### Initial and secondary impacts of natural hazards

3.8 The natural hazards set out in Section C: Guide 1 are mainly drawn from the NRR, and include coastal flooding, inland flooding, storms and gales, low temperatures and heavy snow, heat waves, drought and volcanic ash. Scenarios for severe space weather and the effects in the UK or a more serious volcanic effusion in Iceland are also under development but information is provided. The scenarios have been developed with Met Office, Environment Agency, the British Geological Survey and relevant Government Departments. But other common hazards, that are unlikely to cause 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 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)<br>Tidal surge<br>Snow<br>Lightning<br>Heavy Rainfall<br>Tornadoes<br>Hail | River and coastal flooding<br>Surface water flooding<br>Land instability<br>Wildfire |
| Prolonged period of hot weather (at least five consecutive days) | Heat | Thunderstorms<br>Drought<br>Dust/Smog/haze<br>Land instability<br>Wildfire |
| Prolonged period of dry weather (developing over 3 years) | Reduced Rainfall | Dust/Smog/Haze/fog<br>Reduced ground water flow<br>Water quality<br>Land instability<br>Drought<br>Wildfire |
| Excessive cold with snow | Cold<br>Snow | Ice<br>Ice accretion<br>Wind chill<br>Fog<br>Surface water and river flooding (snow melt) |

3.10 Table 1 shows how different natural hazards can have similar consequences. For example, both storms and snow can lead to flooding. This means that the consequences of these separate events on infrastructure could be similar (i.e. both events could lead to restricted site access, damage and reduced supplies). This is the theory of common consequences and the basis for an all-hazards approach to resilience.

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

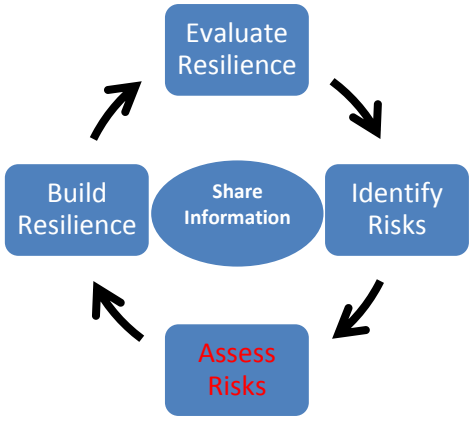
3.11 In assessing the risks of natural hazards, and particularly when considering the resilience of assets with a long life-span, future climates should also be considered. The UK Climate Projections (UKCP) have been produced to help organisations understand the range of possibilities for the UK's future climate over

the rest of the century against three different emission scenarios – low, medium and high. [14]

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.

3.13 The Government undertook to provide a first climate change risk assessment, based on UKCP, in 2012.

[14] UK Climate Change Projections: http://ukclimateprojections.defra.gov.uk/
From September 2011, the Environment Agency, building on the work of the UK Climate Impacts Programme (UKCIP), will take over as Defra's principal partner in delivering the Government's climate change adaptation programme in England. The Environment Agency will provide practical advice to help businesses, organisations and communities prepare for climate change.




# 4 Assess Risks: Standards

## Flood Resilience Standard and Critical National Infrastructure

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" and suggested that a 1 in 200 (0.5%) annual probability event was a reasonable starting point to protect Critical National Infrastructure from flooding. [15, 16]

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 multiple 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

[15] The Pitt Review: (Page 257-258 and 264): http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html

reviews and investment cycles. But the standard 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 "**as a minimum essential 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%)"**. Infrastructure owners and, where relevant, regulators 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 (Chapter 6).

4.5 Specifying a flood resilience standard in terms of likelihood will ensure that the standard stays relevant in a changing climate, although it creates an evolving target. Building resilience will therefore 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 secure the necessary adaptation over time.

4.6 The types of consequences emanating from a flood event are also experienced by infrastructure owners from a wide range of other natural hazards. For example, common consequences from flooding and other natural hazards include the need to prepare for times when the primary site is unavailable, or supply and distribution chains are disrupted or infrastructure is damaged. To that extent, the use of the flood resilience standard to assess and build resilience would enhance the overall resilience of an organisation's infrastructure to other natural hazards.

### Standards for less critical assets and other hazards

4.7 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.

4.8 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.

4.9 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.

4.10 By understanding existing standards, existing contributions to the four components of resilience can be identified. 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

4.11 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 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: Energy Infrastructure**

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 components should function at ambient air temperatures of between -25$^{o}$C and 40$^{o}$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 two levels of redundancy so that in the event of any minor faults the service will remain operational.

4.12 **Network design standards** consider the capacity of the network and the ability to re-route services in the event of failure. Spare capacity and ability to re-route significantly increases 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.

4.13 **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.

**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.

4.14 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.

4.15 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 would not be proportionate to the risks, and difficult to measure.

4.16 **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 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 that are not specifically itemised or which are more serious or extreme than those covered in the reasonable worst case scenarios.

4.17 The standards described above each have a role in contributing to one or more 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.

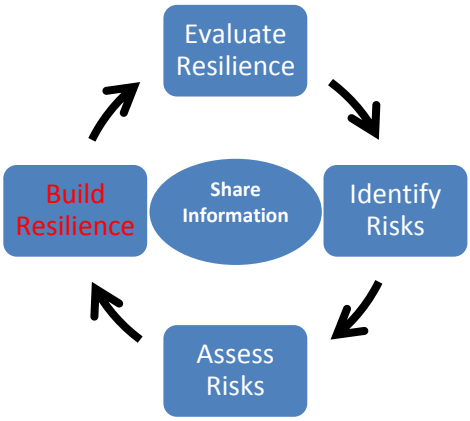
**Box 5: Energy Sector Resilience**

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.

## 5 Build Resilience: Governance




5.1 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."

5.2 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
- be positioned at the core of the organisation's corporate governance processes.

5.3 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.'[17]

5.4 With the appropriate attention of strategic leadership, embedding organisational resilience into governance mechanisms should ensure that the management of the risks to critical infrastructure posed by natural hazards, major accidents and other malicious damage is considered by the Board alongside other organisational priorities. The needs of organisational resilience would thereby inform 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.

5.5 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 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.

5.6 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.

[17] Government Internal Audit Standards: http://hm-treasury.gov.uk/psr_governance_gia_guidance.htm

5.7 The Government is committed to support small and medium sized businesses, which have a potentially significant contribution to make to the resilience of communities, directly and through and the maintenance of essential services. Many small businesses may not find it cost-effective to comply fully with BS25999. But the government will encourage organisations to adopt and embed improved business continuity management within their operations.

5.8 In a related development, Cabinet Office has sponsored the Development of a British Standards Institute Publically Available Specification in Crisis Management (PAS 200). The premise for the PAS is that crisis management is much more than simply the ability to respond to crises when they occur. The PAS establishes that crisis management should be seen as a wider set of capabilities to prepare organisations for crisis, and take steps to prevent and intercept potential crises, as well as being able to act in an informed, effective and decisive manner in mitigating the impacts of crises that do occur. The good practice set out in the PAS is relevant to organisations across all sectors and sizes, and organisations may find it valuable to review the PAS and consider its recommendations.

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

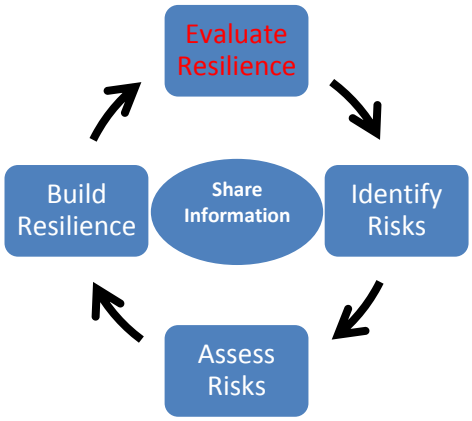
- fully integrates the resilience of critical infrastructure to natural hazards and other threats and hazards;
- is risk based, incorporating, where appropriate, the four components of resilience : resistance, redundancy, reliability and response and recovery;
- is developed / reviewed with stakeholders (including supply chain partners, customers, service users and emergency responders) to strengthen the collective resilience of community supply and distribution systems;
- encapsulates Business Continuity Plans that aim to either meet the requirements of, or incorporate elements of the British Business Continuity Standard, BS 25999;
- considers the recommendations of PAS 200;

- as part of the business continuity process, builds and maintains good working relationships with relevant Category 1 responders, to advise on business continuity planning and have an understanding of response and continuity activities during a disruption; and

- is designed, implemented and reviewed at Board Level and embedded in corporate governance processes.

5.10 **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.

## 6 Evaluate Resilience: Sector Resilience Plans




6.1 Recommendation 51 of the Pitt Review proposed that relevant Government Departments and the Environment Agency should work with infrastructure owners and operators to identify the vulnerability and risk of assets to flooding and a summary of the analysis should be published in Sector Resilience Plans.

6.2 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.

6.3 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.

6.4 The Sector Resilience Plans 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);

- 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.

6.5 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.

6.6 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).

6.7 Sector Resilience Plans are protectively marked owing 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 publishes a summary of the Plans.[18]

[18] Infrastructure Sector Resilience Plans: www.cabinetoffice.gov.uk/resource-library/sector-resilience-plan-critical-infrastructure

**Box 6 Example of good practice: Business Continuity Management and Independent Internal Reviews in the Government Sector**

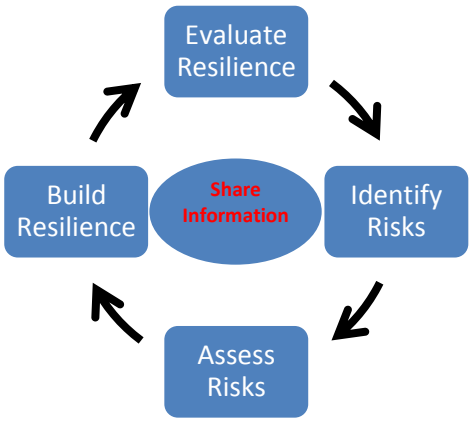
A requirement for Government Departments to undertake business continuity management is set out in the Security Policy Framework.[19] Departments are supported in their business continuity planning through a Cabinet Office-led cross-departmental forum. To ensure a level of consistency and an objective 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 departments and agencies against the British Business Continuity Standard BS25999. If a department can demonstrate alignment to the requirements of BS25999 then the Emergency Planning College will award a certificate, valid for three years. 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.

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

# 7 Sharing Information and Assessing Dependencies




## The Need to Share Information

7.1 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.

7.2 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".

7.3 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:

- what infrastructure provides essential services in an area and/or at a national level, and its dependencies;
- the risks (likelihood and impact) of disruption to that infrastructure from natural hazards and threats; and
- the assumptions being made about assistance from emergency services e.g. pumping of flood waters by fire and rescue service.

7.4 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 Local Resilience Forums may wish to use to enable information on infrastructure to be shared more freely.

**Guidance on Information Sharing**

7.5 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). This Guidance should be read together with Chapter 3 of the CCAs statutory guidance (information Sharing), *Emergency Preparedness*, the non statutory guidance *Emergency Response and Recovery*, *Expectations and Indicators of Good Practice for Category One and Two responders, The Role of Local Resilience Forums: A reference document*. [20, 21, 22]

7.6 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).

7.7 **The success of this approach is dependent upon establishing effective relationships between responders and infrastructure owners and operators.** Many multiple local resilience forum groups 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.

[20] www.cabinetoffice.gov.uk/resource-library/emergency-preparedness
[21] www.cabinetoffice.gov.uk/resource-library/expectations-and-indicators-good-practice-set-category-1-and-2-responders
[22] www.cabinetoffice.gov.uk/resource-library/role-local-resilience-forums-reference-document

7.8 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: (1) to include loss of essential services in its Community Risk Register; (2) to include any responses that may be required for critical infrastructure to be included in the Category 1 responder's emergency response plans.

7.9 Figure 4 sets out a systematic approach for sharing information based on the following steps:

**(1) 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 Local Risk Assessment Guidance and information on natural hazards.

**(2) Ensure the resilience of your own assets.** Local resilience forums 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.

**(3) Share information about your resilience.** Information shared should include generic standards for their sector, alongside specific information on the resilience of their critical infrastructure.

**(4) 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 Infrastructure that provides essential services in the area. [23] 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.

[23] 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.

**(5) 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.

**(6) Update and maintain 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.

7.10 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. Across the UK, several formal Utility Groups (Category 2 Forums) have already been established on previous geographical boundaries or on a thematic or shared risk basis. The London 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. In the North West, a multiple local resilience forum 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.

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

**Figure 4:** Critical infrastructure information sharing for emergency planning – outline process chart

7.11 In other parts of the UK, the emergency responders have come together to undertake specific activities to improve emergency plans. The work of the Lincolnshire and Strathclyde mutli agency critical infrastructure groups are illustrated in Box 8 and Box 9 respectively.

**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."*

**Box 9: Establishing a Local Multi-Agency 'Critical Infrastructure' Group**

In 2010, with the approval of Scottish Government, a local multi-agency 'Critical Infrastructure' Group was established by Strathclyde Police. The group was chaired by the force CONTEST (Counter Terrorism Strategy) Co-ordinator, and the CTSA (Counter Terrorism Security Advisor) Section within the force provided a Secretariat function.

It was decided to run this body as a sub-group of the SECG (Strathclyde Emergencies Co-ordination Group).[24] Membership has been drawn from local authority areas, emergency services, utility companies, the Scottish Environmental Protection Agency, Scottish Government, Strathclyde Police, the Centre for the Protection of National Infrastructure, Ministry of Defence and the SECG itself.

The main purpose of the group was to make better use of local knowledge, particularly CTSA's and local industry/critical site owners, to improve the resilience and protective security of critical sites and CNI in Strathclyde, in consultation with CPNI and Government.

In addition, the group was established to encourage greater partnership working at a local level, in order to develop a better multi-agency approach to address crises or serious incidents occurring within the Strathclyde area.

One of the biggest challenges for the group was the development of an environment where information could be shared safely and appropriately between members. Membership background ranged from security conscious organisations such as the police and CPNI, through to local authorities, where information security measures do not always comply with standards such as the Government Protective Marking Scheme.

Key to the process was the development of an Information Sharing Protocol for members. However, obtaining consensus & agreement in the group regarding this has proved a significant challenge. This process is still on-going and once completed, will provide a methodology and guidance for other police forces or agencies who wish to carry out a similar exercise.

The arrangement has already proved to be extremely useful in a live situation, where certain members of the group were able to exchange information due to the existing relationship and trust that had already been developed. During early 2011, the group participated in a Cabinet Office Pilot Project which looked at information sharing and understanding interdependencies at a Critical Infrastructure asset belonging to Strathclyde Police.

[24] The SECG is the equivalent to a Local Resilience Forum group in England and Wales

Part of the project also involved Strathclyde Police, Scottish Government and key power and utility providers sharing GIS mapping information to identify infrastructure interdependencies at the pilot site. This required a separate non-disclosure document being developed to ensure sensitive commercial information was not distributed or made available inappropriately to competitor organisations involved in the project.

The group is still in its infancy, but advantages can already be seen, in the development of closer working ties between members and the potential for the development of a truly 'Resilient' community.

7.12 The membership of Utility Groups will cut across multiple LRF boundaries. The information sharing guidance encourages infrastructure owners and local responders to agree the membership of Utility Groups based on the most effective and practical approach for their communities / networks. This could be based on geographical boundaries or on a thematic or shared risk basis. In all cases, 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 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. Annex 3 provides example terms of reference for utility groups.

## Understanding Dependencies

7.13 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 (Figure 5). These relationships between infrastructure networks need to be understood to establish reasonable local planning assumptions for civil emergency planning.

7.14 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.

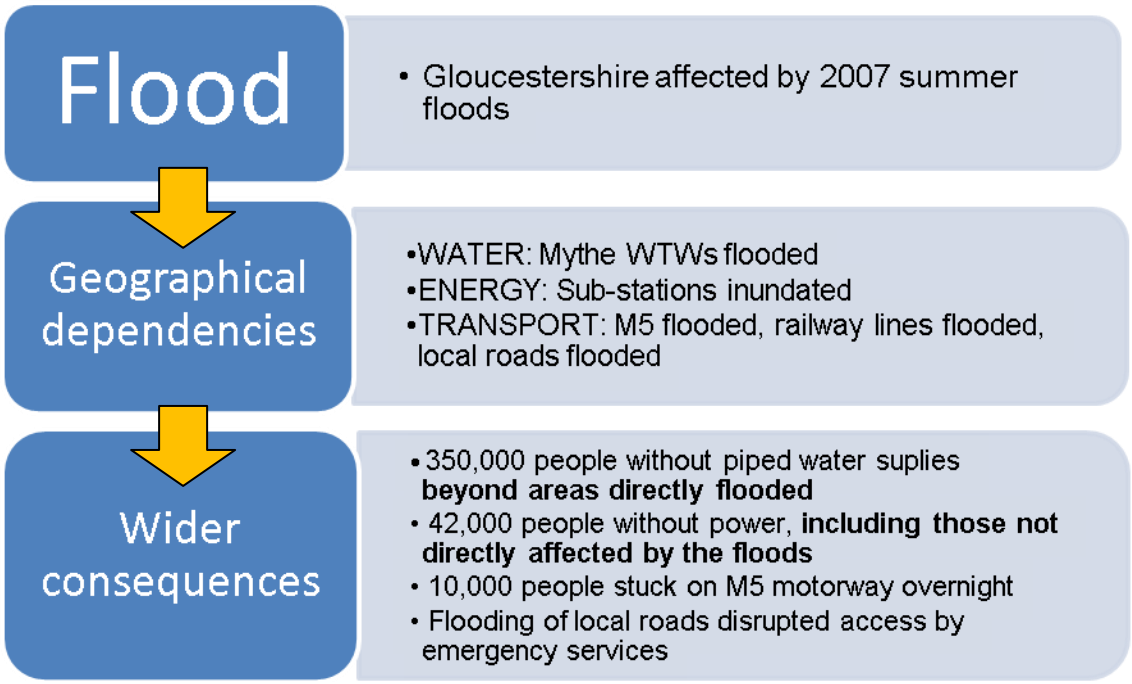



**Figure 5:** Geographical dependencies highlighted during the summer 2007 floods.

7.15 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 to effectively support resilience building.

7.16 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.

7.17 To assist with this process, practical advice is provided in Section C: Guide 4 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 Guidance for Regulated Sectors

## Regulators' Role in Building Resilience

8.1 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.

8.2 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.

8.3 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.

8.4 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.[25] 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 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

[25] Interim Guidance for Regulators: www.cabinetoffice.gov.uk/resource-library/infrastructure-resilience-interim-guidance-economic-regulated-sectors

out throughout this Guide, although specific issues for the regulators are discussed below.

8.5 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*

8.6 Government, infrastructure owners and regulators should use the existing regulatory framework 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.

8.7 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.

8.8 The Digital Economy Act 2010 requires Ofcom to report every three years to Government on the telecoms infrastructure, including a broad assessment of the sector's resilience. The first of these reports is due at the end of September 2011. 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 (legislation came into force in May 2011) imposes new requirements on the communications sector (both networks and services) that require companies to take appropriate measures to mitigate against risks to security and resilience.

8.9 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*

8.10 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.

8.11 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, 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.[26] Ofwat has already published a guide to good practice in this area for the water sector.

8.12 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*

[26] UK Climate Change Projections: http://ukclimateprojections.defra.gov.uk/

8.13 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.

8.14 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.

8.15 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.

8.16 The use of a memorandum of understanding approach between Government, regulators and infrastructure owners , with lightly or unregulated industry, could be considered to encourage and predefine collaboration during national emergencies.

## Section C: Practical Guidance

Guide 1: Guidance on Natural Hazards

Guide 2: Checklist for Infrastructure Owners

Guide 3: Guidance on Information Sharing

Guide 4: Guidance on Assessing Dependencies

## Guide 1: Guidance on Natural Hazards

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

**Purpose**

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

### Background

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

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

- a lack of knowledge (and a lack of understanding of the cross sector vulnerabilities of elements of critical infrastructure) concerning the type and

severity of natural hazards of greatest concern, and the linkage between different natural hazards;

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

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

**Scope**

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

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

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

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

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

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

### Structure

The guidance is divided into two sections:

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

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

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

Infrastructure owners should consider the impact on the delivery of their essential services if an event similar to the scenarios / hazards described in G1.1 and G1.2 occurred. The impact assessment should also consider potential disruption to supply

chains and distribution systems, particularly where other assets of critical infrastructure are part of the chain.

### G1.1 Hazard Descriptions

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

Figure G1.1 illustrates the unclassified summary of the risks, as presented in the National Risk Register.[27]

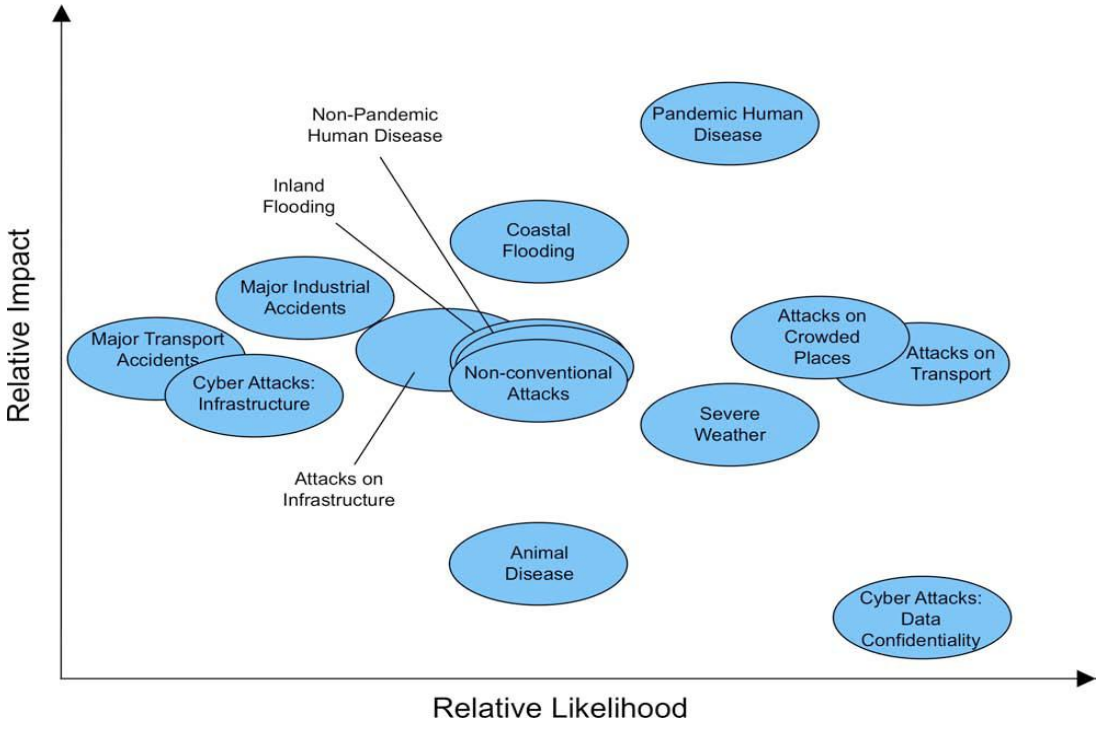



**Figure G1.1:** An illustration of the high consequence risks facing the United Kingdom

Typically, a single natural hazard can carry a variety of challenges for infrastructure owners and planners. For example, a prolonged period of dry weather also carries

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

the risk of thunderstorms and flash flooding; warmer weather, following a cold spell with snow, causes rapid thawing, which leads to flooding. Table G1.1 shows the relationship between different natural hazards.

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

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

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

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

| Scenario | Reasonable worst case scenario | Other related effects | Potential impacts on infrastructure |
|---|---|---|---|
| **Inland flooding** | A single massive inland event or multiple concurrent regional events following a sustained period of heavy rainfall extending over two weeks (perhaps combined with snow melt or intense summer rainfall leading to widespread surface water flooding). The event would include major fluvial flooding affecting a large, single urban area. This is broadly regarded as a 0.5% annual probability flood event. | Storms and gales<br>Snow<br>Land Instability (including offshore and submarine)<br>Heavy rainfall | • Loss of primary transport routes<br>• Lack of staff availability<br>• Impaired site access<br>• Loss of power supplies<br>• Loss or contamination of water supplies<br>• Closure of local businesses<br>• Increased demand for emergency power and water supplies<br>• Increased demand for health and emergency services<br>• Loss of emergency services assets |

| Scenario | Reasonable worst case scenario | Other related effects | Potential impacts on infrastructure |
|---|---|---|---|
| **Coastal Flooding** | Major sea surge, tides, gale force winds and potentially heavy rainfall. Many coastal regions and tidal reaches of rivers affected. Excessive tide levels and many coastal and/or estuary defences overtopped or failing (breaches). Drains 'back-up'. Inundation from breaches in defence systems would be rapid and dynamic with minimal warning and no time to evacuate. Inundation from over-topping of defences would allow as little as 1 hour to evacuate. | Storms and gales<br>Snow<br>Land Instability (including offshore and submarine)<br>Heavy rainfall. | • Loss of primary transport routes<br>• Lack of staff availability<br>• Impaired site access<br>• Loss of power supplies<br>• Loss of water supplies<br>• Closure of local businesses<br>• Increased demand for emergency power and water supplies<br>• Increased demand for health and emergency services |
| **Windstorm: storms and gales** | Storm force winds affecting most of a region for at least 6 hours. Mean speeds in excess of 70mph with gusts in excess of 85mph. Short term disruption to infrastructure including power, transport networks, homes and businesses. | Flooding<br>Land instability<br>Heavy rainfall<br>Wildfire | • Loss of power<br>• Loss of telecoms<br>• Blocked road and train routes and flight disruption |

| Scenario | Reasonable worst case scenario | Other related effects | Potential impacts on infrastructure |
|---|---|---|---|
| **Excessive Cold with Snow and ice** | Snow falling and lying over most of the area for at least one week and after an initial fall of snow there is further snow fall on and off for at least 7 days. Most lowland areas experience some falls in excess of 10cm, a depth of snow in excess of 30cm and a period of at least 7 consecutive days with daily mean temperature below -3ºC. | Storms and gales<br>Flooding<br>Land instability<br>Ice<br>Ice accretion | • Loss of primary transport routes<br>• Lack of staff availability<br>• Impaired site access<br>• Loss of power supplies<br>• Loss of water supplies<br>• Closure of local businesses<br>• Increased demand for emergency power and water supplies<br>• Increased demand for health and emergency services |
| **Prolonged Period of Hot / Dry Weather** | <u>Hot</u><br>Daily maximum temperatures in excess of 32ºC and minimum temperatures in excess of 15ºC over most of the region for at least 5 consecutive days.<br><br><u>Dry</u><br>Periodic water supply interruptions for up to 10 months. Emergency Drought Orders in place authorising rota cuts in supply according to needs of priority users as directed by the Secretary of State. | Thunderstorms.<br>Heavy rainfall.<br>Flash Flooding.<br>Drought.<br>Dust. Haze. Smog.<br>Land instability<br>Wildfire | • Loss or significant reduction of water supplies<br>• Slowed rate of sewage flow through the system leading to public health concerns<br>• Reduction in water quality<br>• Temporary loss of primary transport routes<br>• Loss of power supplies<br>• Closure of local businesses<br>• Increased demand for water supplies from all infrastructure sectors including health, agriculture, energy sectors and emergency services<br>• Increased demand for emergency power<br>• Increased demand for health and emergency services |

| Scenario | Reasonable worst case scenario | Other related effects | Potential impacts on infrastructure |
|---|---|---|---|
| **Volcanic ash** | Volcanic ash incursions for up to 25 days. The entire UK mainland and potentially other parts of Europe could be affected for up to 10 of these days. A single period of closure within the 3 month eruptive episode may last up to 12 consecutive days, depending on meteorological conditions. | None | • Sporadic and temporary closures of significant parts of UK airspace |
| **Severe volcanic Activity** | Severe volcanic eruption, generating large amounts of gas and ash over a five month period affecting UK and northern Europe. | None | • Increased demand for healthcare systems<br>• Closure of UK airspace<br>• Reduced yield from harvests |
| **Severe Space Weather** | Resulting from solar eruptions causing rapidly varying geomagnetic fields on earth. | None. | • Disruption to satellite services for several days<br>• Loss of power supplies<br>• Loss of satellite communications and computer based control systems<br>• Disruption to monetary systems<br>• Interruptions to Global Positioning System (GPS)<br>• Disruption to broadcast services<br>• Disruption to aviation sector |

## G1.2 Other Hazards

### *Geological Hazards*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Guide 2: Checklist for Infrastructure Owners and Operators

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

**Resilience Checklist for Infrastructure Owners and Operators**

### Identify Risks

**Understand your criticality**

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

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

**Understand Hazards**

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

**Self Assessment Questions**

1) Have you worked with external agencies to assess the natural hazards risks to your organisation's critical infrastructure? For example:
    a) Met Office;
    b) Local Authorities;
    c) Environment Agency;
    d) British Geological Survey
    e) Ordnance Survey

2) Does the location of your critical infrastructure make it more vulnerable to disruption from natural hazards?

3) Have you identified your key / critical suppliers / customers? Do some of those deliver an essential service for your community?

## Assess Risk Understand your vulnerability

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

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

**Self Assessment Questions**

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

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

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

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

   a) Their vulnerability to disruption from natural hazards;

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

## Build Resilience

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

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

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

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

**Self Assessment Questions**

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

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

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

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

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

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

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

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

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

15) Have these plans been shared with emergency responders and supply chain partners (up and down stream)?

16) Does the Board seek assurances on the resilience of critical infrastructure to disruption from natural hazards at least annually?

17) Do you have a resilience based education and awareness programme in place within your organisation? If not, do you have board / senior management level support to put in place a resilience based education and awareness programme?

18) Have key staff been trained to implement emergency and business continuity plans?

19) Is there evidence that resilience, and particularly the risk from natural hazards,

has been factored into the organisation's strategic decision making including medium to longer term investment plans?

20) Have your business continuity plans been tested against the British Standard, BS25999?

21) Does your organisation aim to achieve BS25999 alignment / certification?

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

## Evaluate Resilience

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

**Self Assessment Questions**

23) Have you reviewed your Organisational Resilience Strategy?

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

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

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

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

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

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

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

## Guide 3: Guidance on Information Sharing

### Purpose

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

For civil emergency planning it is necessary to understand:

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

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

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

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

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

### Scope

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

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

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

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

**Principles**

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

**Table 1:** "Right issue, right time, right level" Assessment [28]

| 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<br>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)<br>Must satisfy the Baseline Personnel Security Standard (BPSS). |
| Relevant information on critical infrastructure | During an emergency, for prioritisation and response | SCG<br>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.[29]

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.

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

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

CTSAs should continue to provide regular oral briefings to LRFs on the CNI within their area, and continue to disclose information on CNI on a "need to know" basis at the Strategic Co-ordination Group (SCG) during civil emergencies for the purpose of enabling an effective emergency response. All members of a SCG should satisfy the Baseline Standard (BPSS) – see Table G3.1 - which is an appropriate standard for information on CNI for use during an incident.[30]

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

**Guidance**

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

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

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

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

**Suggested Process**

1. LRFs to produce the Community Risk Register (CRR)[31] based on the Local Risk Assessment Guidance, National Risk Register, Planning Assumptions and new Guidance on Natural Hazards. This process should identify the hazards and threats that could affect the area and the potential consequences of these (including the impact on the provision of essential services in the LRF area).

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

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

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

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

[31] Requirement under the Civil Contingencies Act 2004

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

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

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

a) Name of infrastructure network / system;

b) Critical installations or sites in the network;

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

d) Network / site owners;

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

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

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

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

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

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

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

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

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

The Police and FRS officers must be security vetted to SC level and ensure they have measures in place to transmit, store and handle information at RESTRICTED

and CONFIDENTIAL level. They should jointly review the information on critical infrastructure and:

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

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

(c) **Check** that the existing local risk assessment guidance and resilience planning assumptions adequately reflect the potential impacts arising from the failure of critical infrastructure and loss of essential services in the LRF area. Discuss with other Category 1 responders to ensure their plans adequately consider and address those planning assumptions and the potential loss of essential services arising from disruption of infrastructure. The Police and FRS officers holding the information on critical infrastructure may provide supervised access to the information on a 'need to know' basis, to allow other Category 1 responders to review their emergency response plans - providing the individual(s) within those organisations are security cleared to a minimum of Baseline Personnel Security Standard (BPSS). [32]

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

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

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

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

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

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

   LRFs should be invited to send an appropriate representative(s) to the Utility Groups. These groups will support the building of better relationships between

providers of essential services. They will also enable Category 1 responders to understand how category 2 responders plan to deal with service interruptions, and agree trigger points when the Category 1 will be notified of an emergency by the Category 2 responder. Other providers of essential services (not currently covered by the CCA) should be invited to participate as appropriate.

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

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

5. LRFs to use the planning assumptions provided by the Police and FRS alongside the improved information and understanding of infrastructure networks and systems gained through the Utility Group to update and improve the CRR and emergency plans. Improved understanding of potential failures and key weaknesses and dependencies should provide a more accurate understanding of local risks, particularly where these may differ in severity or detail from those listed at a national level. Each LRF will be responsible for deciding which risks to include in their emergency plans to ensure an effective response to emergencies.

   Infrastructure owners and operators may wish to contribute to specific LRF meetings relating to the preparation of emergency plans for their sites. This will enable them to ensure that their sites are appropriately prioritised and prepared for the response they may receive in an emergency. It will also enable them to further improve their business continuity plans and inform their investment planning to improve resilience of the essential services. Active engagement in the Utility Group

by infrastructure owners could reduce the need to regularly attend LRF meetings. The multiple LRF Utility Group in the North West of England has established effective relationships between utility companies such that they are able to share attendance and represent others' interests at occasional LRF meetings across the region when emergency plans are being discussed.

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

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

**Additional notes and recommendations**

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

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

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

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

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

## Guide 4: Guidance on Assessing Dependencies

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

### Understanding Dependencies

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

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

Physical dependencies are those resulting from a connection between installations, sites and with other networks. For example, the physical dependency on electricity supply for the operation of water treatment works, or the dependency upon communications for the control of remote plant and equipment. The physical dependencies are typically not obvious and as such represents a significant and hidden risk to networks and systems. Without a sufficient understanding of physical

dependencies, a loss of a key element of the infrastructure network (such as a major installation) could lead to cascade failures where further disruption is caused beyond the point of failure.

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

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

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

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

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

   b. Other significant asset owners in the area;

   c. Police, fire and rescue service;

   d. Local authorities;

   e. Environment Agency;

f. Counter Terrorism Security Advisors.

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

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

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

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

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

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

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

**Supporting Information Sharing to Understand Dependencies**

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

The Guidance on assessing dependencies is intended to enable local emergency responders and infrastructure owners to work together to ensure a sufficient understanding of infrastructure networks and dependencies across sectors. The

approach involves using the Community Risk Register and business continuity management best practice (as outlined in BS25999 or industry equivalents). Many businesses and organisations that have business continuity management are accustomed to assessing their dependencies and preparing for loss of infrastructure, which is essential for delivery of core functions.

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

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

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

## Section D: Annex

Annex 1: Pitt Recommendations

Annex 2: Related Legislation

Annex 3: Example Terms of Reference for Utility Groups

## Annex 1: Infrastructure-Related Recommendations - "Learning Lessons from the 2007 Floods" an Independent Review by Sir Michael Pitt [33]

**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.

[33] The Pitt Review: http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/thepittreview.html

## 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 Forum (LRF), established to ensure effective delivery of the above duties in a multi-agency environment.[34] 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'

[34] 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 months.[35] 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 together 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 duty of Category 1 responders.[36] There is no matching obligation on Category 2 utility providers. [37] 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.

[35] Civil Contingencies Act 204, Regulations 2005 4(4)
[36] Chapter 2, Emergency Preparedness
[37] 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 NSPs include an "operational continuity obligation" as part of the initial planning assessment to ensure that essential infrastructure is designed to remain operational during floods.

*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 Local Resilience Forums (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

- 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 CTSAs 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