Cabinet Office

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

**A1. This section introduces infrastructure resilience, sets out the background and provides definitions.**

# 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

[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

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:

- improved understanding of the level of vulnerability or risk to which infrastructure and hence wider society is exposed;
- More consistent emergency planning for failures;

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

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

[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.

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.

## 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).

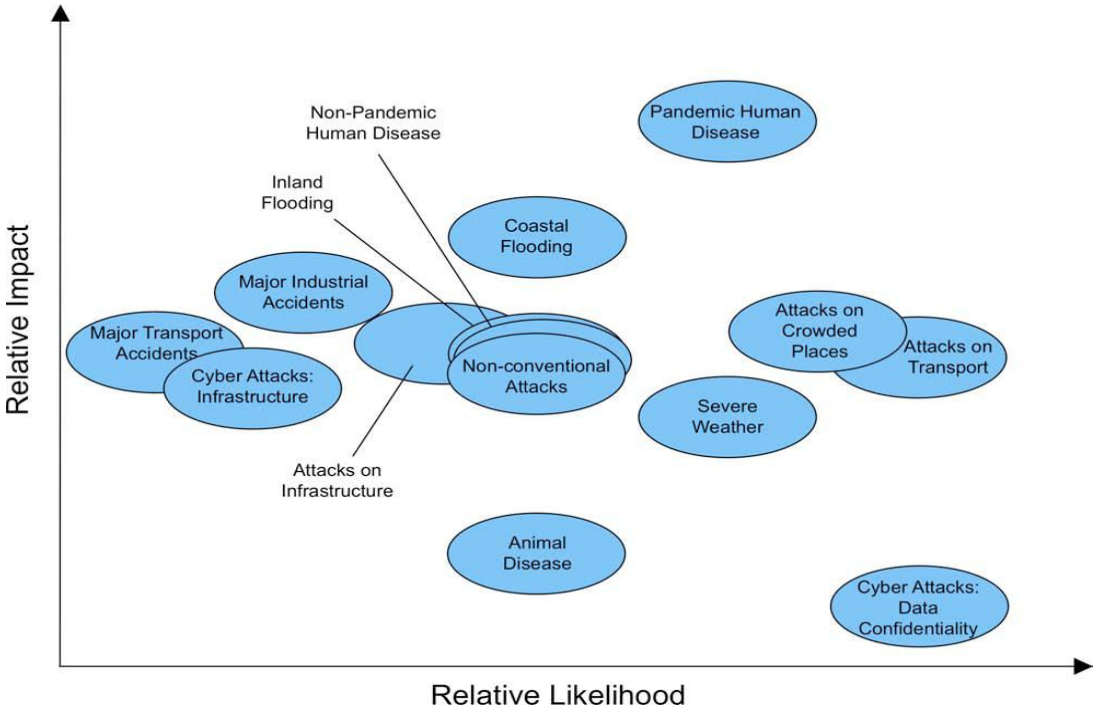


**Figure 1:** An illustration of the high consequence risks facing the United Kingdom.

[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.