



CabinetOffice

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.

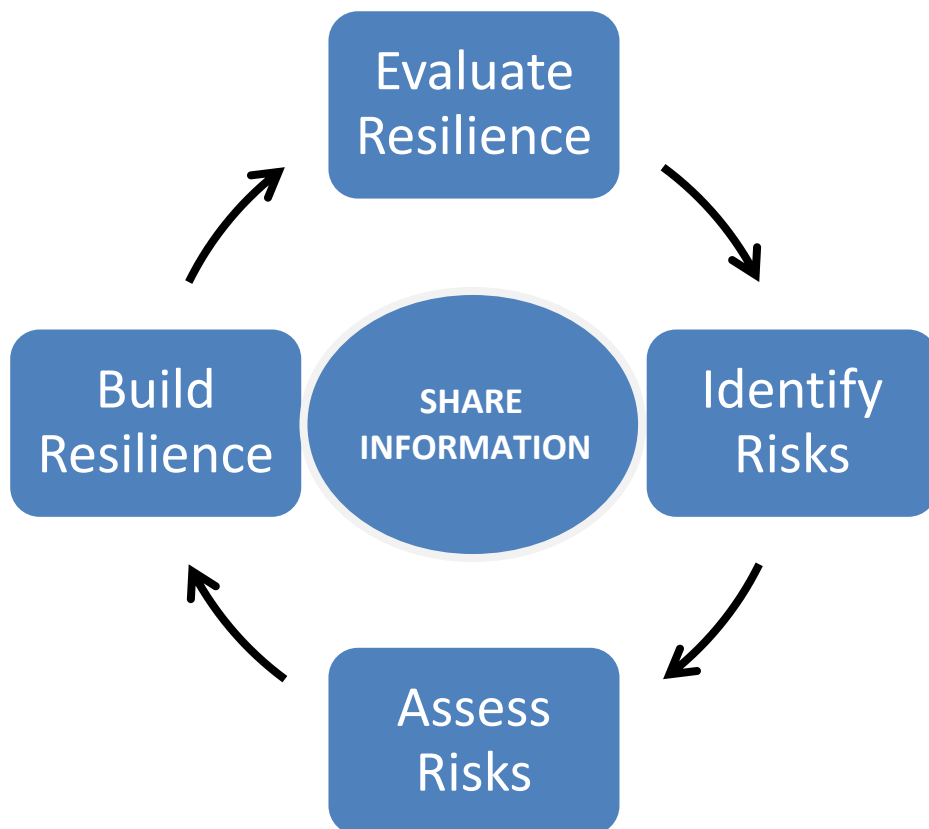


Figure 3: Resilience Cycle for Infrastructure Owners

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).¹ 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.

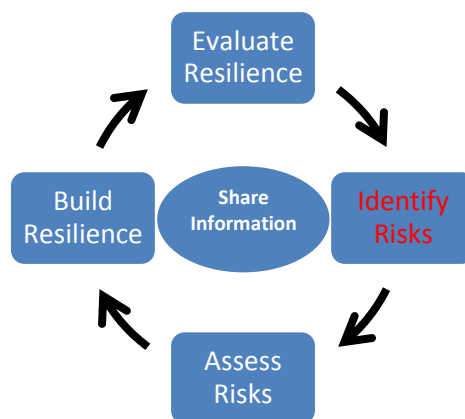
B5. This section provides:

- 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

¹ 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).

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).² 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.

Using the Guidance on Natural Hazards

² 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.

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.³ 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 for an example of this activity in the energy sector). For less critical assets,

³ National Risk Register: www.cabinetoffice.gov.uk/content/risk-assessment

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) Tidal surge Snow Lightning Heavy Rainfall Tornadoes Hail	River and coastal flooding Surface water flooding Land instability Wildfire
Prolonged period of hot weather (at least five consecutive days)	Heat	Thunderstorms Drought Dust/Smog/haze Land instability Wildfire
Prolonged period of dry weather (developing over 3 years)	Reduced Rainfall	Dust/Smog/Haze/fog Reduced ground water flow Water quality Land instability Drought Wildfire
Excessive cold with snow	Cold Snow	Ice Ice accretion Wind chill Fog 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

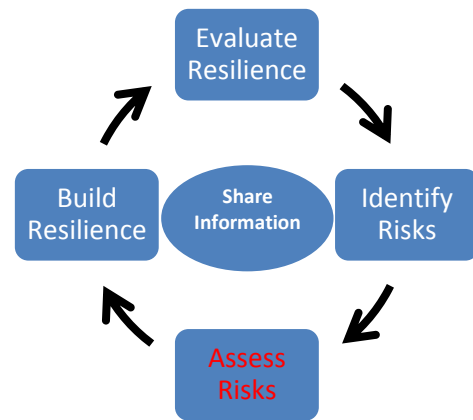
the rest of the century against three different emission scenarios – low, medium and high.⁴

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.

⁴ 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.



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.^{5, 6}

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 reviews and investment cycles. But the standard should be viewed in terms of the broader approach to resilience consisting of the components of resistance,

⁵ The Pitt Review: (Page 257-258 and 264):
<http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/the-pitt-review.html>

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°C and 40°C as calculated over a 24 hour period. Recorded extreme UK temperatures remain within this range, thus components designed to this standard would be expected to continue to operate during periods of extreme weather in the UK. In addition, critical circuits will have 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.

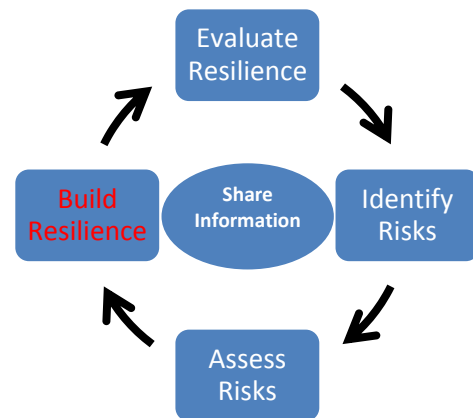
Box 5: Energy Sector Resilience

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.

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.'⁷

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.

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

⁷ Government Internal Audit Standards: http://hm-treasury.gov.uk/psr_governance_gia_guidance.htm

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:

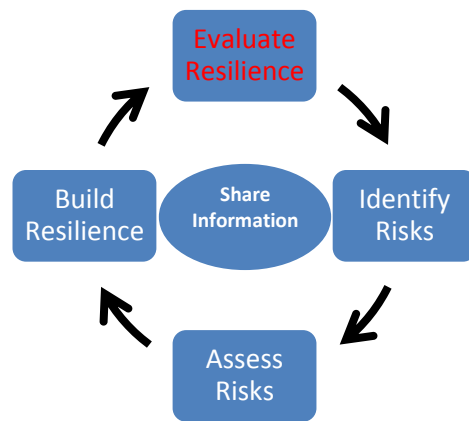
- fully integrates the resilience of critical infrastructure to natural hazards and other threats and hazards;
- is risk based, incorporating, where appropriate, the four components of resilience : resistance, redundancy, reliability and response and recovery;
- is developed / reviewed with stakeholders (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.

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.⁸

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

⁸ Infrastructure Sector Resilience Plans: www.cabinetoffice.gov.uk/resource-library/sector-resilience-plan-critical-infrastructure

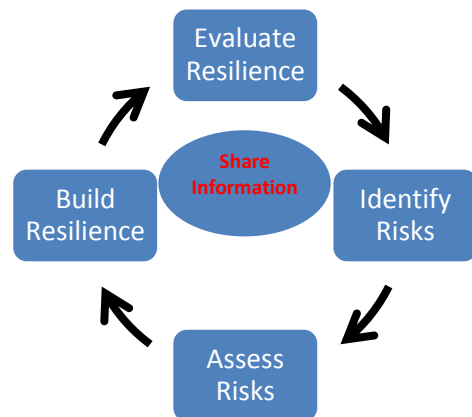
A requirement for Government Departments to undertake business continuity management is set out in the Security Policy Framework.⁹ Departments are supported in their business continuity planning through a Cabinet Office-led cross-departmental forum. To ensure a level of consistency and an objective review 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.

⁹ HMG Security Policy Framework: www.cabinetoffice.gov.uk/resource-library/security-policy-framework

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*.^{10, 11, 12}

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.

¹⁰ www.cabinetoffice.gov.uk/resource-library/emergency-preparedness

¹¹ www.cabinetoffice.gov.uk/resource-library/expectations-and-indicators-good-practice-set-category-1-and-2-responders

¹² 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.¹³ 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.

¹³ 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.

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

(f) 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.

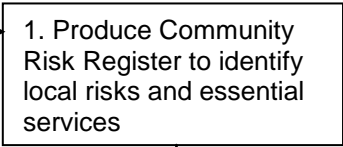
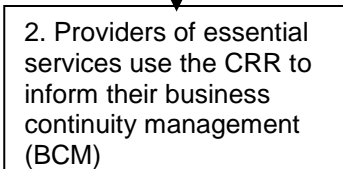
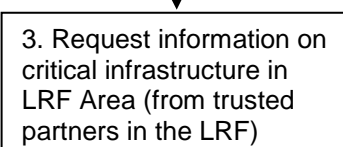
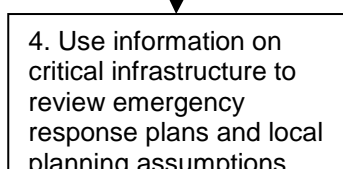
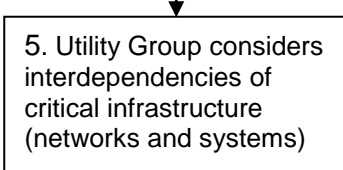
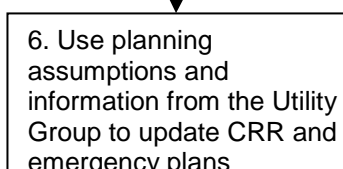
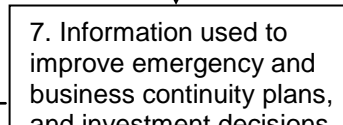
STEPS	WHO	COMMENTS AND LINKS
	LRF	Current CRR process to be used to identify essential services in LRF area. Use Section C: Guide 1- Guidance on Natural Hazards.
	All organisations providing essential services in LRF area	BCM to cover essential services, critical infrastructure and supply chains. Refer to BS25999 or equivalent.
	Lead Cat 1 responder (e.g. Chair of LRF)	Information to be protectively marked. Information must <u>not</u> be used for wider use or for commercial or political gain.
	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
	Organisations providing essential services	See Section C: Guide 4 – Guidance on Assessing Dependencies. See Annex 3: Example Terms of Reference for Utility Groups.
	LRF	Only unrestricted information to be used in publicly available version of the Community Risk Register.
	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 multi 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).¹⁴ 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.

¹⁴ 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.

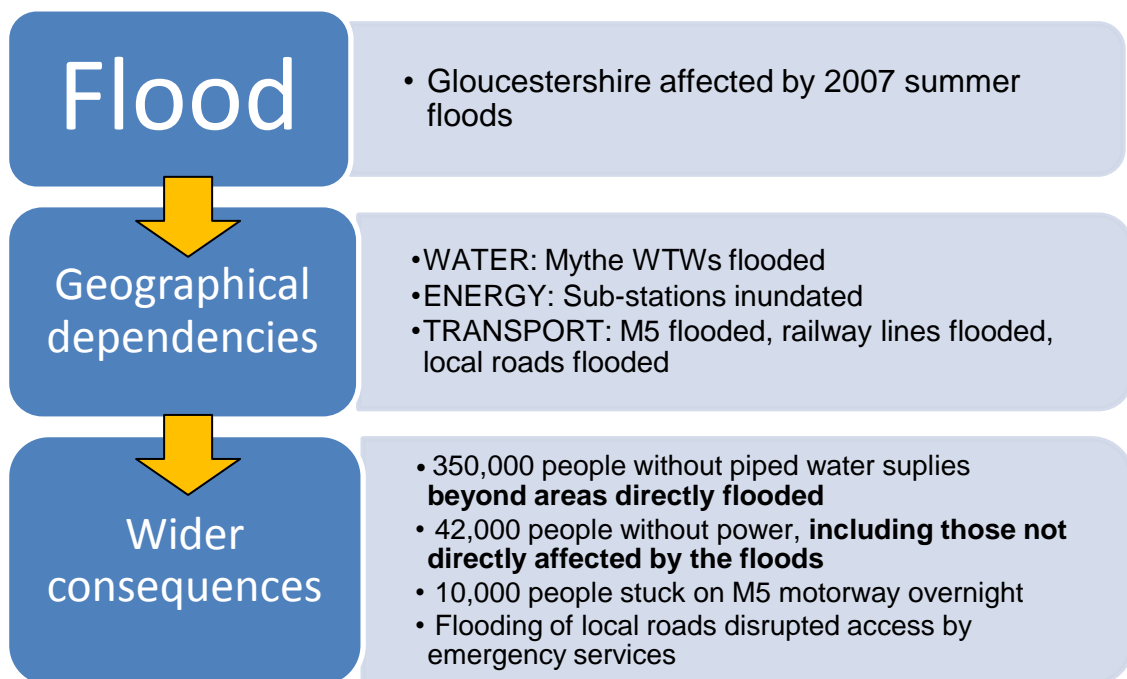


Figure 5: Geographical dependencies highlighted during the summer 2007 floods.

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.

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.¹⁵ 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

¹⁵ 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.¹⁶ 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

¹⁶ 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.