Section 5

Maintaining power and water supplies and protecting essential services

This section looks at the effect of the floods on our critical infrastructure and considers ways in which the resilience of such systems can be enhanced.

It contains chapters which cover:

- taking a systematic approach to reducing disruption to our essential services;
- understanding the level of risk that is tolerable;
- delivering greater resilience in critical infrastructure;
- minimising the loss of essential services;
- enabling better emergency planning through information sharing and engagement; and
- effective management of dams and reservoirs.

Taking a systematic approach to reducing disruption to our essential services

This chapter examines the events of summer 2007 in relation to essential services and explores the issues that need to be tackled to improve the protection and resilience of our critical infrastructure. It contains sections on:

- the 2007 floods – highlighting the vulnerabilities of critical infrastructure;
- lessons learned from summer 2007 floods; and
- taking a more systematic approach to building resilience in critical infrastructure.

The 2007 floods – highlighting the vulnerabilities of critical infrastructure

Introduction

14.1 The summer floods of 2007 had a dramatic effect on electricity power substations, water and sewage treatment works, and the road and rail network. As a consequence of the events there was a strong possibility of the loss of power to 750,000 people leading to discussions about evacuation. Drinking water was lost to 350,000 people for up to 17 days. Tens of thousands of people lost power, some for more than two days, and tens of thousands of people were stranded as the road and rail networks ground to a halt.

14.2 The consequence of the loss of these assets extended beyond the areas that were flooded. This was not an isolated problem but a consistent and significant feature of the emergency. The loss of essential services made everyone affected feel vulnerable. People spoke of feeling isolated, and of 'a return to the dark ages'. In some cases, the loss of supplies sparked panic as people were scared of being left without water. A nation that has become accustomed to, and ever more reliant on, a reliable supply of water and energy was left feeling exposed and underprepared.

14.3 The water industry had previously been considered a fairly resilient sector, but the flooding of the Mythe water treatment works in Gloucestershire demonstrated that there are 'single points of failure' in the water network that, in the event of failure, have massive consequences for whole regions. The loss of Mythe cut off water to 350,000 people for up to 17 days. In total, five water treatment works and 322 sewage treatment works were affected by the floods.

14.4 Similarly, several electricity transmission and distribution assets were affected, with 40,000 customers in Gloucestershire being cut off for up to 24 hours and 9,000 customers on rota disconnection for several days in south Yorkshire and Humberside. However, it

was the 'near-misses' at Walham substation (serving 500,000 people in Gloucestershire and south Wales) and a number of electricity substations around Sheffield (servicing 750,000 people) that brought home the vulnerabilities of infrastructure assets. The failure of supply on that scale in either region would have caused chaos and, almost certainly, loss of life.

14.5 Another potentially catastrophic near-miss occurred at Ulley Reservoir, near Rotherham. The dam was at high risk of breaching, putting in danger life and a number of other infrastructure assets, including the M1 motorway, a major electricity substation and the gas network connection for Sheffield. Although the highest profile incident, it was not alone. Many other dams were also affected.

14.6 Other infrastructure was also disrupted by flooding. There were 148 flooding or bank-slip incidents on the rail network as a consequence of the rainfall and several 'pinch-points' became blocked, destroying the continuity of the network. This in turn caused delays in the bulk supply of fuel products to terminals and other storage facilities, while rail-replacement alternatives were hampered by flooded roads and traffic congestion. Closures affected the motorway network (M1, M4, M5, M18, M25, M40, M50, and M54) and many local and trunk roads were also disrupted with repair costs estimated at £40–60 million.

14.7 Thus, the events of last summer have shown that the vulnerability of infrastructure to flooding can have significant and cascading impacts on the delivery of essential services. The increased frequency and scale of flooding likely as a result of climate change will inevitably introduce greater risks for more infrastructure assets.

14.8 It is clear from the feedback we have received that the public need to be reassured that essential services are resilient to flooding and other civil emergencies. The Government needs to respond by taking action to enable infrastructure operators and local responders to mitigate these risks, especially for single points of failure.

The national infrastructure and the critical national infrastructure

14.9 At the simplest level, infrastructure consists of the basic facilities and installations needed to provide services for the functioning of an advanced, industrialised society. There are many different definitions, developed for different purposes.

National infrastructure

The national infrastructure comprises those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends. These services fall with the sectors of energy, water, communications, transport, finance, government, health, food and emergency services. Within these sectors there are certain 'critical' elements of infrastructure, the loss or compromise of which would have a major impact on the availability or integrity of essential services leading to severe economic or social consequences or to loss of life. These critical elements make up the nation's critical national infrastructure (CNI).

Centre for Protection of National Infrastructure

14.10 The most important sectors for this Review encompass organisations which the Civil Contingencies Act (2004) defines as Category 2 responders. This includes organisations that provide utilities (water, energy and telecommunications) and transport (where the focus is on the national road and rail networks, which are vulnerable to flooding and natural hazards and vital for delivering an effective response). These figured prominently in last summer's flood and it is on these, in combination, that other essential services depend. Other sectors were excluded as follows:

- the main vulnerability of the **finance** and **government** sectors to natural hazards would be loss of the infrastructure providers that underpin their systems, such as telecommunications and electricity, and therefore the sectors are not considered to be a primary concern for this Review;

- similarly, the diversity, complexity and competitiveness of the **food** sector makes it very resilient as a network to natural hazards and means it is most vulnerable through the loss of other infrastructure providers, such as the transport network; and
- the geographically widespread nature of both the **emergency services** and **health sector** also provides a high level of resilience and redundancy to natural hazards.

14.11 References in the analysis below to critical infrastructure cover the utilities and transport sectors outlined above. These sectors will have facilities, systems and networks that are so important that they have been categorised by government as being part of the National Infrastructure and Critical National Infrastructure.

14.12 Reservoir dams represent another key part of UK national infrastructure albeit less for their role in delivery of essential services than for the potential for catastrophic failure and the risk that they pose to life when situated in or near populated areas.

Lessons learned from summer 2007

14.13 Analysis of the evidence submitted to the Review has highlighted fundamental gaps and weaknesses in a number of areas. These gaps and weaknesses have had an impact on the ability of those concerned to anticipate and reduce the vulnerability of infrastructure in advance of events, to ensure that adequate contingency and local emergency plans are in place and that there was an effective response as events unfolded. Evidence indicates the reasons for these failures is:

- the approach taken by the Government to mitigating the risk to the delivery of essential services from natural hazards has largely been uncoordinated and reactive. There is no central understanding of the level of vulnerability or risk to which infrastructure, and hence wider society, is exposed; and there is no centrally defined standard against which to drive action;
- emergency planning for failures has been patchy and inconsistent;
- the amount of information made available at the local level for emergency response planning is insufficient. The emergency response last summer was hampered as a result of an inadequate understanding of:
  - the location of critical sites;
  - the mapping of vulnerability to flooding;
  - the consequences of their loss; and
  - their dependencies on other critical infrastructure assets.
- in addition, the involvement of Category 2 responders in multi-agency response exercises has been poor and their integration into Gold Commands during last summer's emergencies was slow.

14.14 In light of these findings, the interim report proposed a number of interim conclusions that would help minimise disruption to the delivery of essential services if similar events were to happen in the future. The goal of the Review has been to develop an approach that anticipates and manages risks in advance and enables more effective responses to emergencies as they arise.

Taking a more systematic approach to building resilience in critical infrastructure

14.15 The proposals in the interim report relating to critical infrastructure generated a very positive response. This included strong support for a systematic programme to reduce the disruption caused by natural hazards to critical infrastructure and essential services. There was also strong support for improved information sharing and engagement at the local level to enable more effective emergency planning and response.

14.16 The Government agreed with the need to introduce a systematic programme to reduce disruption based on centrally defined standards.

14.17 The Review welcomes the positive feedback from all respondents and, in particular, welcomes the recognition and commitment shown by the Government.

14.18 We strongly believe there is a need for a more systematic insight into the vulnerability of our critical infrastructure and a coordinated approach to driving up its resilience. We welcome the Government's commitment to take this forward and propose that they create a framework to help reduce the risks resulting from natural hazards with the goal of minimising disruption to the delivery of essential services.

Defining protection and resilience

The historic approach to reducing risks to essential services has concentrated on the protection of infrastructure from harm, typically security threats. While this is a useful approach, a focus on protection alone has limitations. Complete protection can never be guaranteed – it is impossible to anticipate all hazards, nor is it practicable on economic or any other grounds to completely protect all elements of the critical infrastructure.

In recognition of this, the protection component has been translated into a broader and more flexible concept of resilience. Resilience is the ability of a system or organisation to withstand and recover from adversity. As such, a resilient organisation is one that is still able to achieve its core objectives in the face of adversity through a combination of measures.

Protection may make up an important part of resilience, but it is not the only factor. Resilience is also underpinned by an effective emergency response to help reduce the impacts of failure.

National infrastructure, security threats and the National Security Strategy

14.19 Protecting critical infrastructure from security threats and maintaining essential services is a high priority for the Government and a comprehensive and well-established programme of protection is already in place. The Government recognises that without these essential services "*the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large scale loss of life*".[1] The Review shares these concerns and the overall aim.

14.20 However, the Government's programme of work to reduce the vulnerability of critical infrastructure to terrorism and national security threats is fundamentally about increasing protective security – it does not address natural hazards or include measures to increase the resilience of critical infrastructure or emergency preparedness.

14.21 The Civil Contingencies Secretariat, which sits within the Cabinet Office, looks at both security threats and natural hazards but its remit is to enhance the UK's ability to prepare for, respond to and recover from emergencies, rather than protect against threats or hazards arising. There is therefore a gap in the Government's policy and delivery related to the protection of critical infrastructure from natural hazards.

[1] www.cpni.gov.uk

Protecting national infrastructure against terrorism and other national security threats

Sector sponsor departments are responsible for deciding the appropriate security approach to be taken in their sectors. This involves identifying and monitoring priorities for security activity in their sector in consultation with industry and relevant security specialists such as the Centre for the Protection of National Infrastructure (CPNI).

CPNI is the Government authority on protective security in relation to national security threats. It comprises teams of expert advisers who conduct security reviews and provide advice across the national infrastructure aimed at reducing vulnerability to these threats. CPNI works closely with businesses and industries to identify risks and vulnerabilities.

Within each sector key steps include identifying and categorising infrastructure, setting security goals and priorities taking account of risk, delivering security advice, implementing advice and monitoring and reviewing progress.

14.22 Since our interim report, the Government has published its new National Security Strategy. This takes a holistic approach, covering crime, pandemics and natural hazards, such as flooding, in addition to traditional security threats. Natural hazards are a security issue on the basis that they can affect large numbers of UK citizens and *"demand some of the same responses as more traditional security threats, including terrorism".* We welcome the inclusion of flooding within the National Security Strategy, and the recognition that risks to individuals and communities are as important as risks to the State.

14.23 In order to deal with these risks the Strategy states that the Government needs *"to understand them better, act early to prevent them where we can, and ensure that we minimise and manage any harm they might cause".* It is clear from the evidence gathered from last summer's widespread events that more must be done to anticipate risks as well as effectively tackle the potential impacts arising from natural hazards to critical infrastructure.

14.24 The Strategy also indicates that the Government is considering how to strengthen its capacity for horizon scanning, forward planning and early warning to identify, measure and monitor risks and threats. It acknowledges that the challenges to our security cannot be delivered by Government alone but demand *"broader partnerships...with owners or operators to protect critical sites and essential services"*.

14.25 The Review believes that these principles – acting to the benefit of the individual citizen and planning and acting in advance of an emergency through tripartite cooperation – should also form the guiding principles for a systematic programme to reduce the vulnerability of national infrastructure to flooding and other natural hazards. The recommendations set out in this report will go a long way to helping achieve the outcomes set out in the National Security Strategy.

The National Security Strategy

The National Security Strategy, published in March 2008, sets out how the Government will address and manage security challenges and their underlying drivers in order to safeguard the nation, its citizens, our prosperity and our way of life. This is the first time the Government has published a single, overarching strategy, and represents a new approach to national security.

The Strategy covers not only 'traditional' security threats, such as terrorism, but includes transnational crime, pandemics and flooding. It is also person-centric, considering not just the protection of the integrity and interests of the State but also threats to individual citizens. Notably, the Strategy recognises climate change as potentially the greatest challenge to global stability and security, in part caused by an increase in the frequency and intensity of extreme weather events. Another important development in thinking is the commitment to focus on the underlying drivers of security and insecurity in order to allow prompt action and improved prevention where possible, and to achieve this through partnership between the public and private sectors.

The Strategy sets out the Government's intention to publish a national-level risk register setting out its assessment of the likelihood and potential impact of the range of different risks that may directly affect the United Kingdom and the safety and well-being of its citizens.

An outline for the systematic programme

14.26 Ensuring safe, secure communities that are at the heart of a robust, growing economy requires resilient essential services. This will require a thorough, infrastructure-wide risk assessment, targeted investment to improve resilience and an effective emergency response capability. The effectiveness of this activity can only be assured through strong co-operative relationships between private and public sector at the national and local level. Government represents the public interest but does not possess the experience or expertise to identify measures to reduce risk. Sectors have much better knowledge about their capability and the measures necessary to make improvements and respond to the interests of their shareholders. **We would welcome the Government and industry working together to foster a collective responsibility for enhancing resilience in line with the values in the National Security Strategy.**

14.27 In order to achieve the level of ambition set out in the National Security Strategy and to minimise potential future disruption of the kind we saw last summer, the Review believes that the Government should develop an enduring programme to take on the challenge of driving up resilience through a coherent national plan that balances risks and costs within and across sectors. The systematic programme should aim to:

- **reduce the most substantial known risks** to critical infrastructure resulting from natural hazards through careful assessment of vulnerability and prudent action based on new centrally defined standards;
- **provide appropriate economic incentives** to increase the resilience of critical infrastructure;
- **enhance the capacity to absorb shock and act quickly** when faced with unexpected events through the introduction of mandatory business continuity planning; and
- **ensure an effective emergency response** at the local level through improved information sharing and engagement before, during and after emergencies.

14.28 Such a programme would need to encourage coordination and integration within and between sectors. It should consist of an overarching plan and sector specific plans that are based on a comprehensive and objectively measurable programme. It should include levels of protection and resilience for individual sectors. At the national level, Government, economic regulators and utilities companies should work together to understand vulnerabilities and develop workable solutions that provide value for money. At the local level,

emergency planners and utilities companies should exchange information and ensure engagement for effective emergency response.

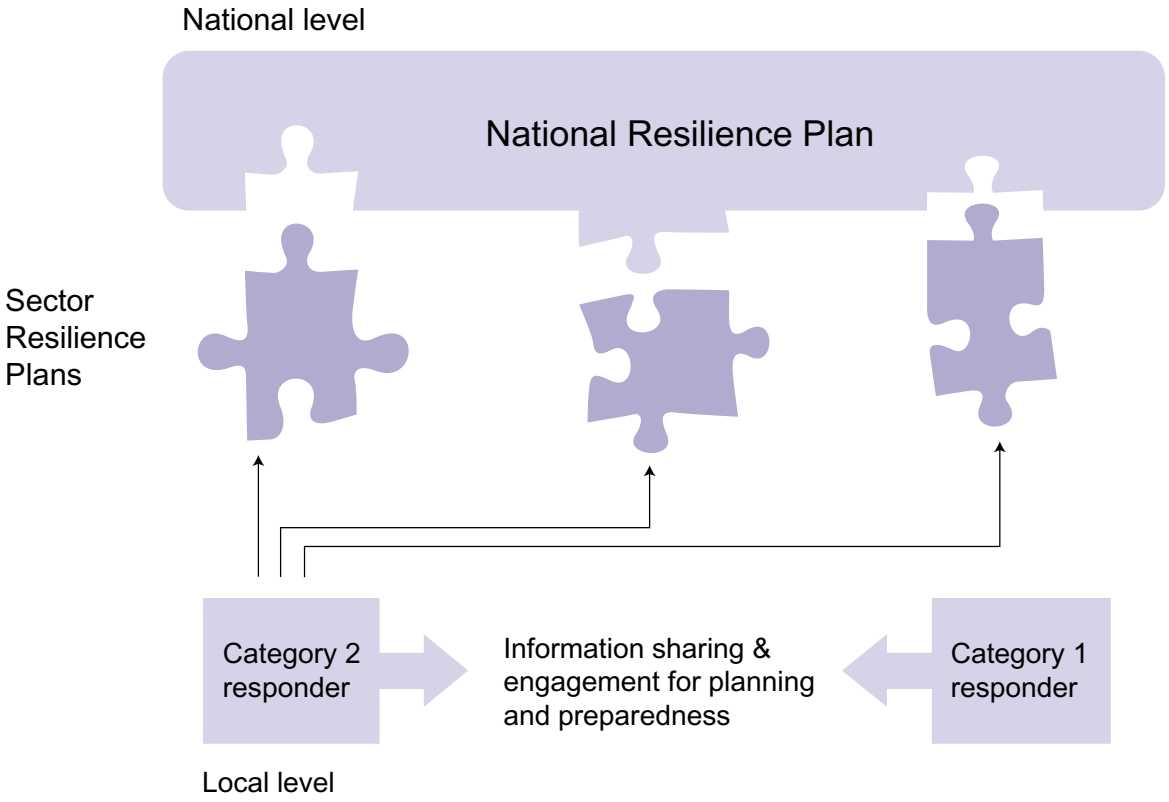
14.29 We feel that this is an appropriate compromise between the needs of national coordination to drive up resilience and improvements in emergency response capability at the local level. While risk and vulnerability information is gathered at the local level, we do not believe it is best placed to derive or drive plans to improve the protection and resilience of nationally critical infrastructure. The systematic programme should comprise:

- a coordinated, coherent **National Resilience Plan** for critical infrastructure, based on a partnership between the public and private sector, which enables coordination between multiple sectors, organisations and localities. The National Resilience Plan should be formed from Sector Resilience Plans; and
- **Sector Resilience Plans**, developed jointly through a tripartite relationship between the relevant government department, economic regulator and industry sector, should be public documents with controlled sections where necessary for sensitive information. The plans should set out:
  - the levels of ambition for resilience across the critical infrastructure (based on standards of protection, economic incentives and business continuity planning for all risks);
  - a picture of risk and vulnerability for the entire sector developed by bottom up aggregation of risk and vulnerability analysis on a periodic basis;
  - a programme of measures for achieving the appropriate level of ambition for resilience, along with the timescales for delivery;
  - a mechanism for reporting progress on the implementation of the programme of measures and updating the plan on an annual basis; and
  - a process for benchmarking and reporting of business continuity plans.

14.30 The national programme would be complemented by a range of measures at the local level:

- 'bottom-up' aggregation of risk/vulnerability analyses through sectors to inform Sector Resilience Plans;
- Local authorities (upper tier) being free to undertake 'ad hoc' scrutiny of infrastructure operators' business continuity plans; and
- getting the right balance between 'need to know' and 'need to share' to enable local emergency responders and infrastructure operators more effectively to plan and prepare for emergency response.

Figure 10 – National and sector-level resilience plans



14.31 Although we advocate a consistent approach across the critical infrastructure, we recognise that there are differences between sectors. Working on a sectoral basis will respect existing sectoral definitions and methodologies, and complement other existing measures and policies.

14.32 The Government should develop guidance and a national policy statement that sets out the national process, timescales and expectations. This would also provide additional guidance on information sharing protocols at the local level.

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.

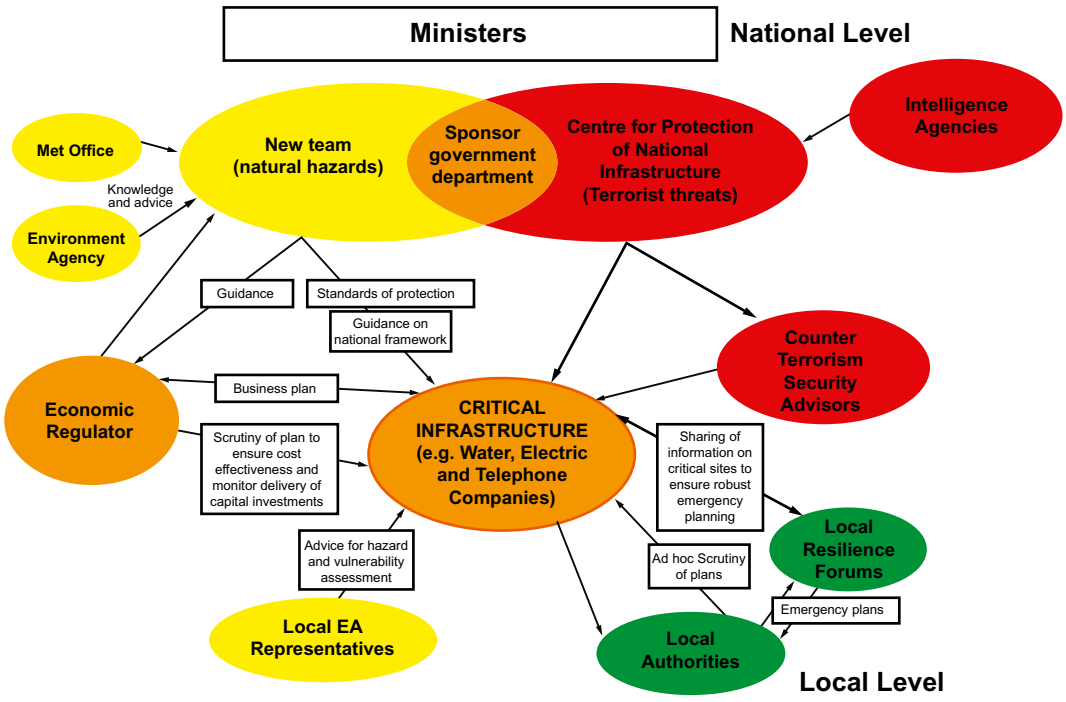
14.33 The relevant Sector Resilience Plans, and the standards that underpin them, should be the basis for work to improve the resilience of existing critical infrastructure and inform the resilience of future infrastructure developments. We recognise that the Government has proposed to introduce a system of National Policy Statements that will establish the national case for 'major infrastructure' development and set the policy framework for Infrastructure Planning Commission decisions. **The Review would welcome the Government considering how Sector Resilience Plans and the relevant National Policy Statements can be aligned.**

14.34 We also call for the appropriate structures and resources within government to manage and coordinate the cross-government effort. Our discussions have revealed that there is currently no single body responsible for driving and coordinating activity to anticipate and mitigate risks from natural hazards to critical infrastructure. The Review therefore believes that the national framework should be driven and coordinated at the national level by a new Natural Hazards Team within Government.

14.35 Past and present approaches to critical infrastructure protection in the UK are driven

by security threats. However, other countries, including the United States and European Union countries that we visited, are starting to take a broader 'all-hazards' approach in response to the conclusion that comparative analyses clearly show that large-scale natural events are more probable and have higher consequences than terrorism. In the short term, the approach set out above should be closely aligned to the Government's approach to tackling security threats to the delivery of essential services. **In the longer term, the Review would welcome the Government pursuing a more integrated approach to critical infrastructure that considers security threats and natural hazards together in a single plan.**

Figure 11 – Natural Hazards Team illustration




© Topfoto

Understanding the level of risk that is tolerable

This chapter examines how risks to critical infrastructure can be assessed and discusses how government should reduce those risks by setting proportionate standards within and across critical infrastructure sectors. It contains sections on:

- the risk assessment and risk management context;
- the complexity of risk assessment;
- coordination of risk reduction across sectors;
- understanding flood risk to critical infrastructure; and
- setting standards as part of a national campaign.

Introduction

15.1 The strategy that we propose in Chapter 14 is two fold: to reduce the most substantial known risks to critical infrastructure in order to prevent emergencies; and to enhance the capacity to absorb shock and respond quickly when faced with unexpected events.

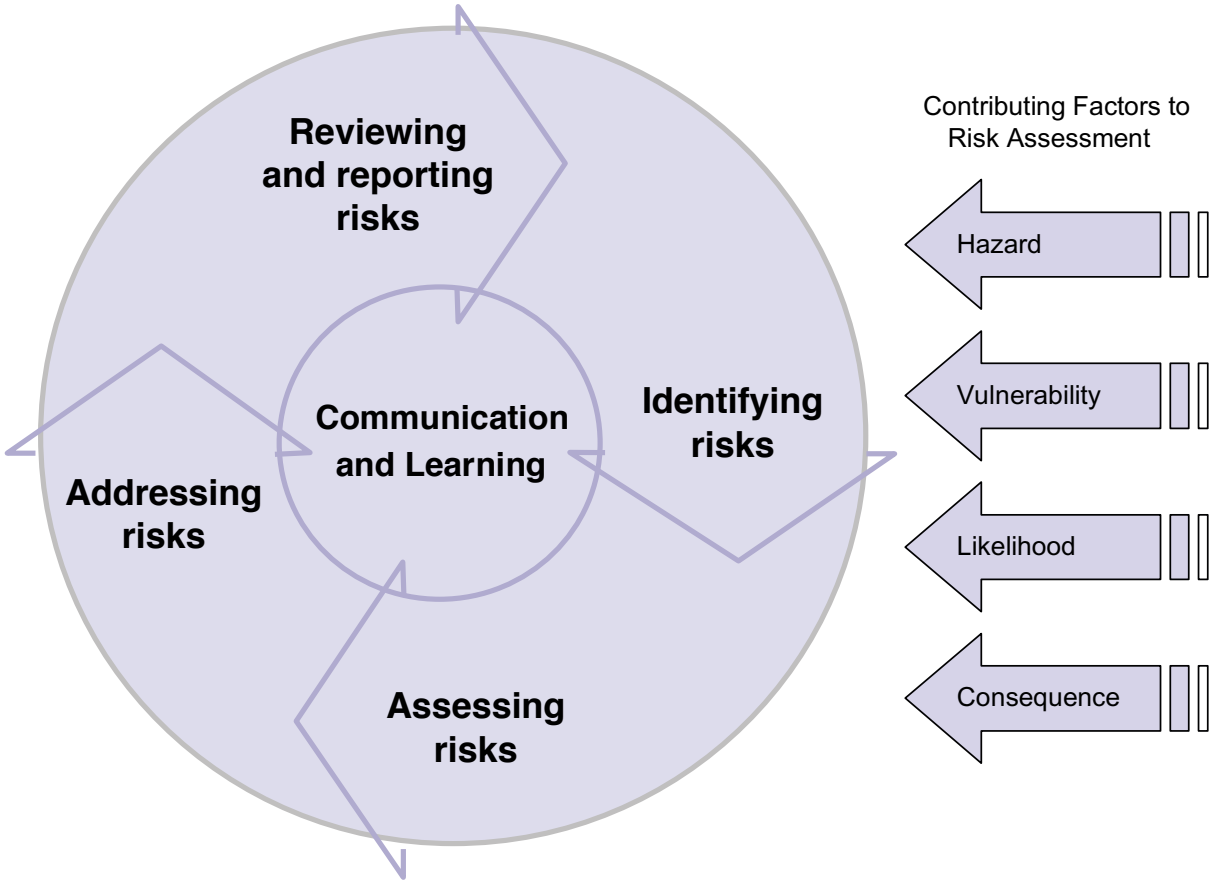
15.2 Our aim of minimising disruption to the delivery of essential services cannot be achieved unless there is a good understanding of what elements of critical infrastructure are vulnerable to the impact of flooding and the potential consequences of their loss. This, in conjunction with standards, will enable the appropriate measures to be developed by critical infrastructure operators to allow them to manage flood risk. This Chapter sets out how the Government and infrastructure operators can cooperate to deliver consistent risk assessment and target action based on proportionate standards.

The risk assessment and risk management context

15.3 There is a large amount of literature on risk, risk assessment and risk management. It is not the purpose of this Review to appraise the subject in detail but some key issues stand out.

15.4 Broadly, understanding risks to infrastructure involves assessment of the hazard, vulnerability of assets and the consequences of their loss. Each hazard has specific characteristics in terms of probability, frequency, intensity, coverage and duration. Failures of infrastructure associated with these hazards reflect the ability of assets and systems to absorb the impact and recover. It is not just the presence of a hazard that leads to a risk but also whether the asset is vulnerable. For example, a critical site might be in the flood plain but if it has a flood defence then the risk is reduced. The principles of the risk assessment cycle are set out in Figure 12.

Figure 12 – The risk assessment cycle and the contributing factors to risk.



15.5 Once a detailed picture of risk has been established, the next step is to work out which risks need to be tackled as a priority and take decisions about preventative action. This is necessary because of the virtually unlimited number of risks and the finite resources available to reduce those risks.

15.6 In policy terms, taking action to reduce any of the elements of risk – hazard exposure, vulnerability to the hazard or the consequence of loss – can help reduce the overall risk: relocating an asset away from the flood plain will reduce the hazard; providing flood defences will reduce the vulnerability; creating additional capacity in networks will reduce the consequences of loss.

What is currently known about risks to critical infrastructure?

15.7 At present, there is an incomplete national picture of the vulnerability of critical infrastructure to flooding. The focus of the existing Government approach is to minimise the impacts of loss of essential services through emergency preparedness and contingency, rather than through reducing vulnerability. In addition, the national flood defence programme is focused primarily on people and properties so while some infrastructure may be protected through community based schemes, it is expected that site owners and operators should assess and address risks themselves. Thus, while there is a core programme of reducing the overall consequences aimed at failure of critical infrastructure in an emergency, this does not enable the Government to understand the overall level of risk and make informed judgements about the level of preventative action that may be necessary.

15.8 The Government does consider natural hazards, including flooding, in its national risk assessment (NRA) process, which aims to identify risks to the UK as a whole and assess their likelihood and impact over a five-year period. Information gathered through the

NRA process is used to improve emergency preparedness for both security threats and natural hazards under the Civil Contingencies Act.

15.9 The Government has also set out its intention in the National Security Strategy to publish a National Risk Register (see previous chapter). This will describe the Government's assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK with the goal of helping local authorities, people and communities, businesses and others prepare for emergencies. Flooding is explicitly recognised in the National Security Strategy and is expected to feature in the National Risk Register when it is published later this year.

15.10 We welcome the National Risk Register approach and believe that the National and Sector Resilience Plans, described in Chapter 14, for critical infrastructure could, if synchronised appropriately, provide the appropriate vehicle to inform the National Risk Register of the risks that natural hazards pose to critical infrastructure and the delivery of essential services.

15.11 It is difficult to say in any objective way whether critical infrastructure is any better prepared for flooding than a year ago. In the areas that were affected last year, critical infrastructure assets now have temporary defences in place and there is improved engagement between stakeholders, which has led to more developed response strategies for emergencies. Nationally there is greater awareness of the risk of flooding and this was highlighted in the level of preparedness demonstrated by critical infrastructure owners in response to the tidal surge risk in autumn 2007. However, while there are some sector specific programmes to assess the vulnerability of critical infrastructure to flooding, it is clear that there is no concerted programme of action to reduce risk nationally across all sectors.

The complexity of risk assessment

15.12 Understanding and taking action to mitigate flood risks is complicated by the tendency for the hazard, vulnerabilities and consequences to change over time. The result is that risk is dynamic. Our evidence shows a number of trends that are of importance to the debate on risk and risk reduction for critical infrastructure. Although these trends are not quantified, they suggest that risk is growing overall and that targeted action is needed in response.

15.13 Chapter 3 sets out some of the changes that are occurring in the frequency and severity of natural hazards as a consequence of climate change. In general, natural hazards, including floods, are set to increase with climate change. Climate change will result in two different effects. The first is gradually increasing mean temperature, which will eventually affect a wide range of infrastructure. The other relates to the effect on extreme weather events, including precipitation and floods, and is especially relevant to the functioning of infrastructure and the delivery of essential services. Climate change will introduce greater challenges for which we need to be prepared.

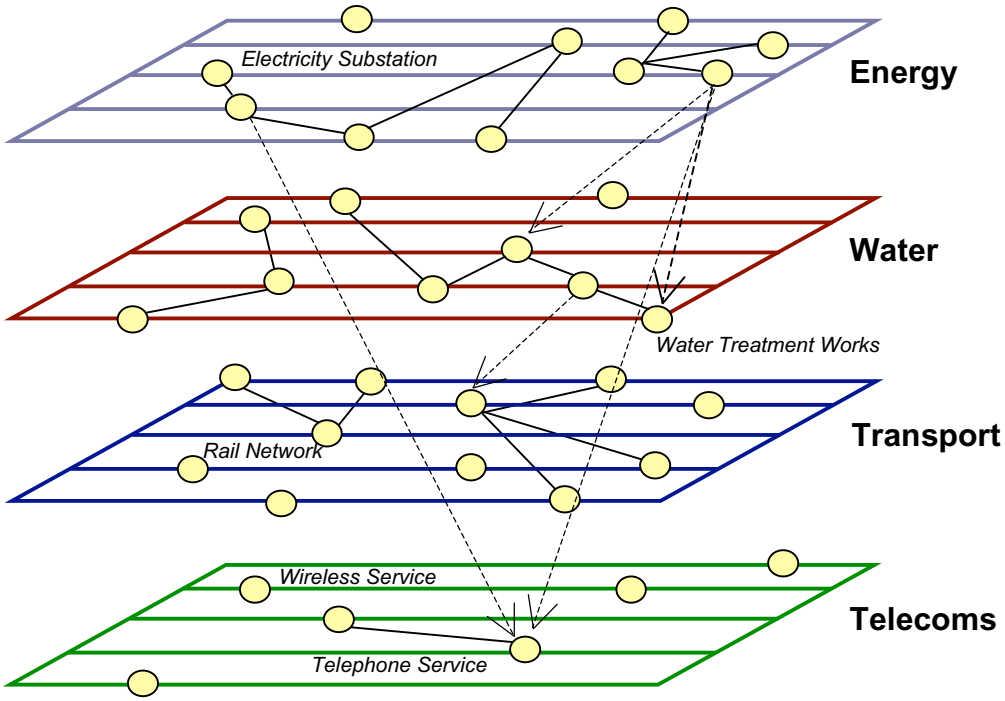
15.14 These changes are magnified by societies' increasing dependency on essential services. Few activities in society function without access to drinking water, electricity and telecommunications. Industry and households have overconfidence in infrastructure's 'always-on' availability, and have little preparedness for outages in the power network.[1,2,3] Increases in population also make it harder to provide emergency supplies in the event of loss of essential services such as drinking water. Consequently, the loss of an essential service has the potential to cause greater disruption, economic and social, than might have occurred in the past.

[1] Amin (2002) Towards secure and resilient infrastructure, Journal of Infrastructure Systems, 8, 67–75.
[2] Little (2002) Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures, Journal of Urban Technology, 9, 109-123.
[3] Blostrom (2006) Third International Conference on Critical Infrastructure.

15.15 Economically, infrastructure operators, in particular the utilities, are striving for efficiency. This is a consequence of the need to be more competitive, which has been supported through the process of economic regulation and the successful Government policy of driving for improved efficiency.[4] However, while this makes good business sense and provides better value for utility bill payers, it drives out any spare capacity within networks that is assessed to be unnecessary, with the unintended consequence that redundancy can be lost. Several asset owners and regulators suggested that this loss of spare capacity means that, in the event of failure, there are fewer options for providing a continuation of service.

15.16 The issue of reduced redundancy has been exacerbated by the increasing interconnections between sectors, creating a complex system of interlinked networks: if one part of the system fails, it is likely to affect another part of the system.[5] Power, transport, communications and water for example, could all be badly affected by a loss of electricity supply, the latter causing a cascading effect into each of the others. This 'domino effect' was seen during the summer floods where loss of power caused water discharge pumping stations to fail resulting in further flooding, for example at Longlevens in Gloucestershire. The Cabinet Office Report "Risk: Improving Government's capability to handle risk and uncertainty" said "…….*interconnected infrastructure brings with it increased exposure to catastrophic events*….". The box on the following page describes these complex interactions and Figure 13 shows an example of just some of the interdependencies between elements of the critical infrastructure.

Figure 13 – A schematic outline of some of the interdependencies between critical infrastructure sectors. The direction of the arrow indicates the dependence[6]



[4] Kearns and Gude (2008) The New Front Line: Security in a Changing World, Institute for Public Policy Research.
[5] Auerswald (2006) eds. Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability. *Cambridge University Press*.
[6] Adapted from Pederson, Dudenhoeffer, Hartley and Permann (2006) Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International Research. Idaho National Laboratory Critical Infrastructure Protection Division. www.pcsforum.org/library/files/1159904563-TSWG_INL_CIP_Tool_Survey_final.pdf

What is the critical infrastructure system?

Critical infrastructure is often described as a 'system of systems', which functions with the support of large, complex, widely distributed and mutually supportive supply chains and networks. Such systems are intimately linked with the economic and social wellbeing and security of the communities they serve. They include not just infrastructure but also networks and supply chains that support the delivery of an essential product or service.

A 'system of systems' is most commonly described at national level, but they also operate locally. For example, the interdependencies of an oil refinery extend equally to the services that support the well-being and social cohesion of its local workforce, such as health, education and transport, which in turn employ local people, as they do to the shipping lanes that bring in the crude oil, the roads that take the fuel away or the telecommunications that link all these elements together. They are not bounded by the immediate geography of the refinery itself or necessarily linked directly to its operational role.

As a complex, interdependent 'system of systems', the challenges faced by critical infrastructure, whether from natural or man-made hazards, are shared across the entire system and its organisational structure and cannot be viewed in isolation.

15.17 While interdependencies between sectors can create vulnerabilities, we also recognise that interconnectivity within a sector can have benefits: for example, in their response to the EFRA Select Committee, Yorkshire Water outlined how the high levels of interconnectivity developed in response to the 1996 drought means that for around 95 per cent of their customers they can switch to an alternative water supply should their usual supply be lost. However, evidence from other water companies indicates that greater interconnectivity may also reduce resilience if the networks allow companies to use a small number of very large treatment works in the search for efficiencies. The appropriate balance needs to be achieved between efficiency and resilience.

15.18 Planning is also complicated because infrastructure assets are typically long-lived. Critical infrastructure resilience must consider risks that might arise over a long time, including hazards that occur infrequently, and which take account of dynamic factors such as climate change, population growth and socio-economic change. Increasingly the risks that we have to be prepared for in relation to disruption to essential services are becoming more complex and interrelated. The challenge is not only to develop a better understanding of the known natural hazards but also the changing and newly emerging vulnerabilities and consequences of loss as well as their interrelationships.

Coordination of risk reduction across sectors

15.19 The ownership of infrastructure is complicated. There is a mixture of privately owned companies, overseen by various economic regulators and government departments. This has created a patchy programme of hazard assessments, regulation and protection strategies within sectors.

15.20 The current Government approach to protecting critical infrastructure focuses on minimising the impacts of the loss of essential services through emergency preparedness and contingency planning. Government does not prescribe standards of protection or measures of resilience to reduce the vulnerability of critical infrastructure to flooding.

15.21 The legislative framework in place for risk mitigation, preparedness and emergency planning and response by Category 2 responders is created by the Civil Contingencies Act and sector-specific legislation. The utilities considered in this chapter are all designated Category 2 responders under the Civil Contingencies Act, 2004 and this places general duties on them to cooperate and to share information with Category 1 responders – emergency services and local authorities – to support the latter's risk assessment and contingency planning duties at the local level.

15.22 Sector specific legislation contains similar, complementary, provisions to plan for, prevent and respond to particular sector specific eventualities. The individual legal obligations are not consistent and there is a degree of uncertainty about the level of risk reduction required. A key issue is whether operators are able to identify and reduce vulnerabilities to an acceptable level themselves or whether a degree of Government advice and intervention is required.[7] Evidence that we have received from Category 2 responders indicates that the priority given to natural hazard risk mitigation varies within and between sectors. As a result, access to funding for resilience work can be variable.

15.23 While most sectors appear to have a national, government-led group to discuss emergency planning issues there is no targeted, consistent programme or forum that acts as a focal point to reduce vulnerabilities and increase resilience across all sectors. Our discussions with critical infrastructure operators have indicated that some companies and sectors have thought more about robustness and resilience than others, depending on the nature of the sector, market conditions, legislative requirements and past incidents.

15.24 The case study below is an example from last summer where two infrastructure assets in different sectors were exposed to exactly the same hazard but had very different outcomes. This resulted from the current approach to dealing with natural hazards, whereby individual sectors and asset owners are responsible for making their own judgements about the degree of risk mitigation.

15.25 These problems point to the need for a cross-sector programme to provide consistent approaches to understand and manage risks and also reduce the likelihood of knock-on failures between sectors. There are already some positive industry-led cross-sector coordination activities, such as the CNI Shared Capability Advisory Network (CNI Scan) and, since last summer's floods, the water and electricity industries have started a process of assessing the vulnerability of their assets to flooding. However, these sectors have highlighted that more central guidance is needed to assist this work and deliver consistency between sectors as well as within them.

CNI Scan

CNI Scan (Shared Capability Advisory Network) is a collaborative programme between public and private sectors that aims to build upon best practice security, risk and resilience planning in the CNI.

The programme objectives are achieved through a series of collaborative projects across the nine CNI sectors. The projects aim to capture and analyse good practice approaches of individual stakeholders through activities including horizon scanning and war games supported by scenario planning, visualisation and experimentation.

The learning generated from these projects feed development of system level best practice approaches spanning the complex web of people, processes, systems, technology and governance of the CNI.

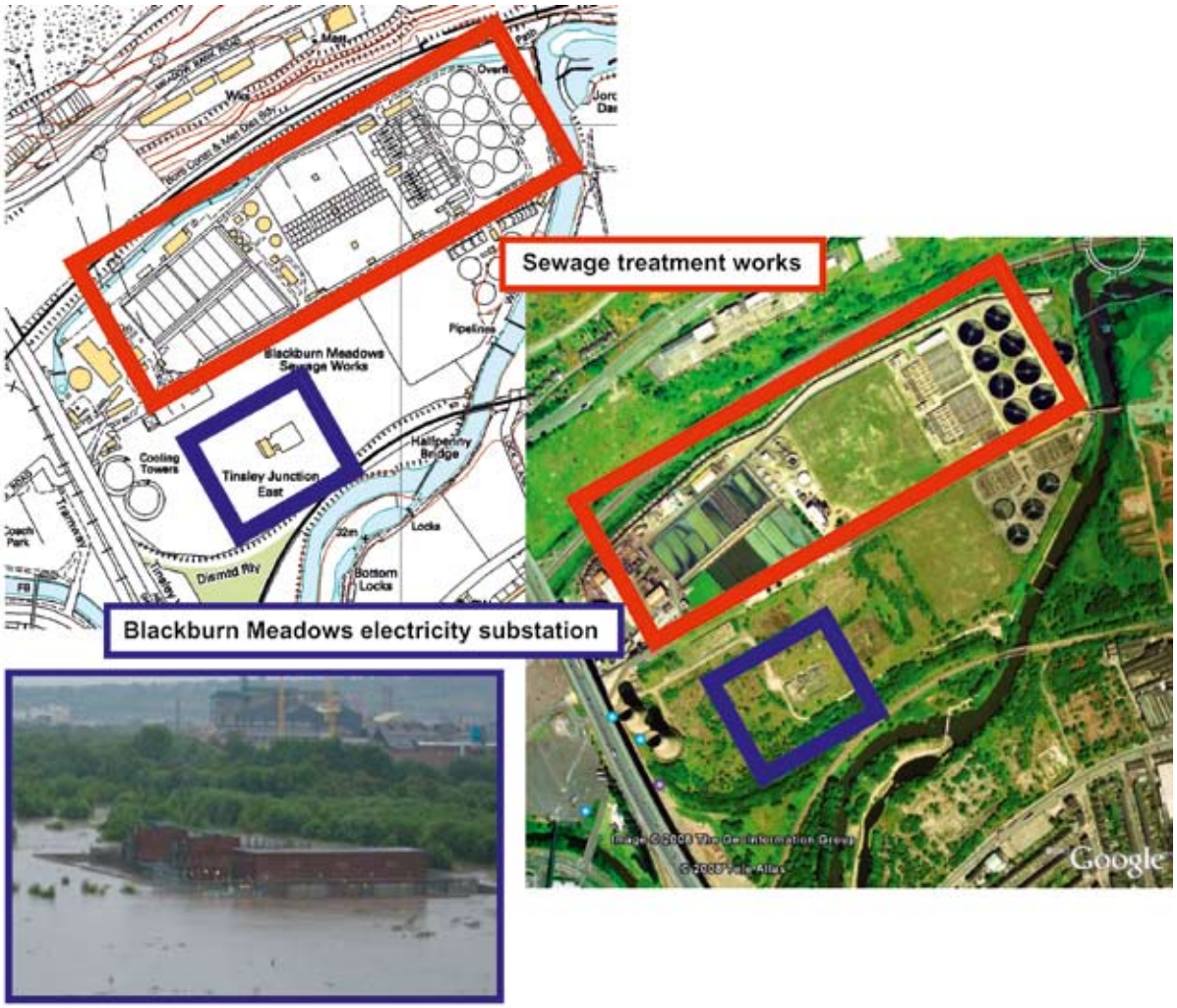
15.26 Thus there is no consistent and targeted focus for flood risk reduction across all the relevant infrastructure sectors. Within each sector the nature of risks and the degree of uncertainty differ. There is no objective process to understand risks and vulnerabilities and there are no specific standards of resilience to flooding. As a result, the Government does not understand the level of vulnerability and risk of infrastructure failure resulting from flooding.

[7] Walker (2008) The governance of the Critical National Infrastructure, Public Law, 323-352

An aerial view of Blackburn Meadows electricity substation in Sheffield, which was defended by a flood defence wall, unlike the neighbouring sewage treatment works

Blackburn Meadows is situated next to the River Don in Sheffield and was heavily flooded last summer. Two infrastructure assets are located on the site: a sewage treatment works and electricity substation.

The operator of the substation had undertaken an audit of its assets following the flooding of 2000 and invested in defences at a number of the highest risk sites. The effectiveness of the defences at Blackburn Meadows substation meant that flood water was largely kept out. However, the neighbouring sewage treatment works had not been defended. The result was that the sewage treatment works, which serves 500,000 people, flooded. Sewage flowed into the river for 5 days following the event. Repair costs are estimated at £17 million.



International cross-sector risk assessments

The uncoordinated approach to the assessment and response to natural hazards in relation to critical infrastructure in England contrasts with the approaches taken in some other countries, which have recognised the importance of critical infrastructure to society and the potential issues related to widespread failure, and have therefore introduced a more coordinated approach to mitigating risks. The two examples described below take a structured approach to dealing with risk. By taking an explicit, systematic approach they have been able to improve their decisions and delivery on a rational and analytical basis. Improvements have been made in: providing systematic assurance that key risks are being managed effectively; identifying and coordinating handling of risks across departmental boundaries; assessing the risk landscape as a whole; and judging capacity for additional risk.

United States

The United States' interest in critical infrastructure protection dates back to the Oklahoma City bombing in 1995 and has developed over time. The current strategy, in the form of a National Infrastructure Protection Plan (NIPP), was launched in 2006 and tackles both security threats and other manmade and natural disasters.

The NIPP provides a coordinated approach to critical infrastructure protection, setting out national priorities, goals and requirements for effective distribution of funding and resources to help ensure that the US government, economy and public services continue in the event of a terrorist attack or other disaster. Protection includes a wide range of activities such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design and initiating active or passive countermeasures.

The Netherlands

The Dutch have also chosen to take a more systematic and coordinated approach to tackling potential disruption to critical infrastructure. They have established a project, Protection of Vital Infrastructure ('Bescherming Vitale Infrastructuur'), which aims to develop an integrated package of measures to protect infrastructure in both the private and public sectors from security threats, accidents and extreme natural phenomena.

The project consists of several steps: a quick-scan analysis of the Dutch critical infrastructure, stimulation of a public-private partnership, threat and vulnerability analysis, and a gap analysis of protection measures. These measures, intended to be embedded in the regular operation of business and government, aim to reduce the occurrence of large-scale disruption and prepare for the consequences of failure or disruption.

Understanding flood risk to critical infrastructure

15.27 Reducing flood risk to critical infrastructure must be about prioritisation. The probable result of trying to protect everything is that nothing will be protected adequately. Efforts related to risk reduction must be based on an assessment of the risk situation.

15.28 The failure of elements of our critical infrastructure has potential consequences for 100,000s or millions of people across the country. Given the scale of the risks, the Review believes that it is vital that the Government should have an understanding of the risks that society is exposed to as a result of failure of critical infrastructure from flooding. This will enable Government and the relevant sector to: understand the baseline vulnerability; allow an assessment of progress and whether further action is needed; and facilitate coordination of risk assessment and management across sectoral and Departmental boundaries. It will also fit with the aim of the National Security Strategy to "…*understand risks better, and act early to prevent them where we can*…".

15.29 The new systematic programme for reducing risk across critical infrastructure,

as agreed by Government in response to our interim report, should be based on an understanding of the flood hazards and vulnerabilities to those hazards. Vulnerability occurs at the local level and needs to be understood and mitigated at the local level. It is therefore appropriate for critical infrastructure operators to undertake the process. However, it is essential that this is carried out consistently within and across sectors, which will require central guidance from Government.

15.30 In the short-term, exposure to flood hazard can be assessed by infrastructure operators by mapping their assets onto Environment Agency coastal and fluvial flood maps. This mapping exercise should also take into account surface water flooding using the surface water "hot spots" map recommended in Chapter 4. This assessment of risk can then be further refined by establishing the consequence of a particular asset failing, that is, the 'criticality' of the asset. The ranking of criticality is already being undertaken by the Government using a system that is based on the principle that 'criticality' is defined in terms of the extent to which its loss will affect the delivery and/or integrity of essential services. This approach is as equally applicable to natural hazards as it is to national security threats.

15.31 The Review recognises that most risks cannot be eliminated altogether. Risk management will require judgements to be made about what level of residual risk is acceptable. These judgements should consider not just the asset providing the service but also the consequence of the loss of that service, and this principle should be taken into account in the appraisal of flood defence projects undertaken by the Environment Agency.

15.32 As a result of last summer's floods, the water and electricity sectors have already started a process of assessing the vulnerability of their assets to flooding. The goal is to be able to identify priorities and propose measures for risk reduction. The Review welcomes the proactive approach taken by both sectors.

Asset Resilience to Flood Hazards: Ofwat's development of an analytical framework

Since the water industry's experience of the 2007 floods, Ofwat have taken the opportunity to review current industry practice for assessing the resilience of assets to flood risks. The report develops an analytical framework for assessing the risk from flooding of critical assets and identifying cost-beneficial resilience options. The intention is that the framework will enable water companies to establish the risks from extreme rainfall events under current and changing climate conditions and consider adaptation options for critical assets in a consistent manner, in order to rank the value of potential investments. Finally, flood hazard specific guidance on the application of cost benefit analysis for justifying potential asset investments is provided.

The framework supports:

- quantification of asset criticality in relation to service criticality;
- assessment of risks resulting from flooding of critical assets; and
- cost benefit analysis of related investment proposals.

The framework considers flooding events that have relatively low probability (< 1 per cent per year) and relatively high consequence of failure, in terms of service disruption. As such, the priority is large, discrete assets (treatment works, pumping stations, communication centres, major pipelines), because the failure consequences could be severe. The effects considered are those that result in loss of service to the customer and environment such as water supply interruption caused by shutdown of a water treatment plant, pollution of a watercourse due to inundation of wastewater treatment processes, contamination of the water supply due to pipeline damage and ingress of flood water.

Energy Networks Association (ENA) Substation Resilience to Flooding report

ENA is the trade association for UK energy transmission and distribution licence holders and operators, acting in the interest of its members in the energy 'wires and pipes' sectors.

The electricity network comprises a mixture of overhead lines and underground cables that generally are not susceptible to flooding. However, substations on the ground can be susceptible and it was the flooding of substations in Yorkshire and Gloucester that caused the power failures experienced in 2007.

After the 2007 floods, in recognition of the vulnerability of electricity substations to such incidents, the Energy Minister requested ENA to lead a comprehensive assessment of electricity substations' resilience to flooding and identify steps that could be taken to mitigate current and future risks. The Task Group included representatives from all the Electricity Networks companies, Department for Business Enterprise and Regulatory Reform, Ofgem, and the Environment Agency.

The ENA report considers primary and higher voltage substations, as distribution substations serve a very small geographic area, and if flooded, the customers they supply are also normally flooded and unable to take supply of electricity

The report describes a number of steps in a cross-sector systematic approach to vulnerability and risk assessment, which will be used to inform investment decisions to ensure the resilience of existing substations against such risk. They include:

- identifying all substations (within scope) in the flood plain;
- establishing flood risk assessment for each substation to identify predicted flood depth and other key factors to establish which substations are 'at risk';
- for all those 'at risk' sites, the identification of the flood impact for that particular site, including potential societal impacts;
- establishing if the site is, or will be, protected by a flood protection scheme sponsored by the relevant local authority;
- if not, establishing the most appropriate protection solutions and the cost of protection works for each substation;
- proposing an appropriate solution based on the levels of flood risk to be considered and the implications for investment;
- reviewing information from the Environment Agency and Scottish Environment Protection Agency on flash flooding as it becomes available.

15.33 The challenges involved in developing the baseline information necessary to undertake the hazard vulnerability analysis should not be underestimated. For example, following the Carlisle floods of 2005, the then Department of Trade Industry and electricity industry started a process to assess the vulnerability of the electricity transmission and distribution network to flooding. However, the Review understands that the process of mapping vulnerability was hampered by the lack of flood depth information. Although more and better quality information is increasingly available, there is still a need for improved flood depth data for the current work. This is expected to be achieved through the Environment Agency's new topography data and modelling work, being undertaken as part of its commitment to the European Floods Directive.

15.34 The Review recognises that gaps in the information available need to be filled, particularly in relation to the most critical assets. The current availability of up-to-date information on both flood hazards (likelihood) and critical infrastructure criticality (consequence) make the approach described above, combined with site-by-site consideration of vulnerability, an ideal short-term strategy for prioritising action to reduce vulnerability to flooding.

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.

Setting standards as part of a national campaign

15.35 The approach proposed above will allow some rapid progress to be made in identifying and prioritising the most significant risks. However, in order to ensure a consistent approach to risk reduction within and across sectors, the Government needs to be able to articulate a maximum level of risk which is acceptable on behalf of society.

15.36 The Review believes that Government should set clear, unambiguous standards to reduce the vulnerability of infrastructure and essential services. The Review does not feel that mandatory, inflexible standards would be appropriate at this stage, as these could hinder fast-paced industries and may simply become obsolete by the speed of change. Instead, we feel the Government should be seeking to develop strong relationships with industry and regulators and to introduce sector-specific plans that are based on non-mandatory standards. Of course, if non-mandatory standards are not embraced, consideration will need to be given to the option of a regulatory approach.

15.37 Responses to the interim report strongly supported the establishment of standards by government in order to provide certainty over the level of protection required within and between sectors.

15.38 The Review believes that in the short term the Government should use the 'reasonable worst-case' scenarios derived from the NRA process to determine the level of flood hazard to drive risk reduction. The worst case scenarios for flooding are based on flooding events of the scale experienced in 2007, and the Review believes that a new standard of protection should ensure continuation of supply of essential services during such an event.

15.39 While the precise scale and nature of these events varies, and extreme flows can be difficult to measure accurately,[8] the Review considers that for the purposes of building resilience in the critical infrastructure, a minimum standard of 1 in 200 annual probability would be a proportionate starting point.

15.40 However, the Review notes that Planning Policy Statement 25 (PPS25), which sets out the Government's national policy on land use planning development in relation to flood risk, allows new 'essential infrastructure' assets to be built in 1 in 100 fluvial flood zones or 1 in 200 coastal flood zones if an 'Exception Test' is passed and the asset is '*designed and constructed to remain operational and safe for users in times of flood*'.[9]

15.41 The Review would welcome Government aligning the standards of resilience across both existing and new critical infrastructure by updating the Practice Guide Companion to PPS25. This should state that essential service assets within PPS25 designated flood risk zones 2, 3a and 3b (see Table 6) need to be designed and constructed to remain operational and safe for use (including any necessary access and egress) in at least a 1 in 200 annual probability flood event.

[8] Marsh and Hannaford (2008) The summer 2007 floods in England and Wales, National Hydrological Monitoring Programme, Centre for Ecology and Hydrology

[9] www.communities.gov.uk/planningandbuilding/planning/planningpolicyguidance/planningpolicystatements/planningpolicystatements/pps25/

Table 6: PPS25 Classification of land according to flood risk

Zone Name	Flood Risk Classification	Annual probability of River Flooding	Annual probability of Coastal Flooding
Zone 1	Low Probability	less than 1 in 1000	less than 1 in 1000
Zone 2	Medium Probability	between 1 in 100 and 1 in 1000	between 1 in 200 and 1 in 1000
Zone 3a	High Probability	1 in 100 or greater	1 in 200 or greater
Zone 3b	The Functional Floodplain	1 in 20 or greater (land where water has to flow or be stored in times of flood)	

15.42 The Review also notes that PPS25 currently considers water treatment and sewage treatment assets separately from other essential services, classifying them as 'Less Vulnerable'. Based on the evidence of last summer, this would appear to be inappropriate. **The Review would welcome all utilities and transport being classified as essential services within PPS25, and therefore being subject to the same planning conditions in terms of flood risk assessment.**

15.43 Priority action for applying these standards to existing critical infrastructure should be focused on those assets defined by Government as critical for the purposes of protective security. The Review understands that the process of re-assessing criticality is ongoing but believes the total number of critical assets across the utilities (water, electricity, gas, and telecommunications) and transport (road and rail) sectors will be in the low hundreds.

15.44 In addition, priority should be given to single points of failure. The interim report considered the importance of single points of failure, based on the example of Mythe water treatment works, which is one of five in Severn Trent Water's region that represent a single point of failure resulting in a complete loss of supply to a significant number of customers; and that in only one case had a specific scheme been developed to ensure supplies in the event of failure. The interim conclusion was that single points of failure and complete loss of assets should be explicitly considered in risk assessment and contingency planning. We would now go further: we consider that, in taking this work forward, the Government should provide particular weighting for such single points of failure and identify them for priority action to increase resilience.

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.

15.45 Action at the local level may vary in order to achieve this resilience standard, taking into account the particular vulnerability of assets and the most cost-beneficial option to minimise disruption. For example, in the interim report we pointed to three ways in which resilience might be improved:

- **relocation of the asset.** This would involve moving high-criticality assets out of the floodplain altogether and into a low-risk area;
- **improving the robustness of flood defences.** This could include permanent defences for high-risk sites through to demountable or temporary defences for sites at medium risk; and
- **increasing resilience of the service or asset.** This may involve making the service more resilient by building additional network connections and/or making the asset more

resistant to flooding through waterproofing key components or raising them out of harm's way.

15.46 While action should be progressively extended to other sectors of the critical infrastructure, we would expect standards to be proportionate to criticality, with the less important sites being subjected to only business continuity requirements (discussed in Chapter 17). Crucially, the same standards should be applied across all sectors at the same level of criticality.

15.47 In the longer term, the Review sees merit in a more holistic approach to standard setting, which would be service focused, rather than hazard focused. We see value in a measurable index of resilience being developed that may comprise several vulnerability and resilience parameters such as level of interconnectivity, redundancy and consequence of loss. This approach would be intended to inform how resilience can be improved across critical infrastructure networks, rather than focusing on a particular hazard and individual assets. Such resilience standards should be embedded into the planning procedures for future critical infrastructure.[10,11]

15.48 In order to ensure that the long-term approach is well informed, a systems approach to building resilience should be adopted, including research, analysis and policy development of risk determination, risk communication and economic regulation and incentives. To achieve this, it will be essential to engage with a wide range of government departments, industry sectors, economic regulators and academics to achieve a forward-look approach to risk assessment beyond the five year scope of the NRA process.

15.49 The Review considers the activities in the longer term could include:

- expanding the range of hazards considered beyond flooding;
- identifying all sources of long-term natural hazard information in order to inform decision making;
- reviewing economic framework and associated incentives;
- setting out expectations for business continuity service levels;
- considering options for 'designing in' resilience to new assets;
- other key considerations such as appropriate application of cost-benefit analysis (to include the impact of loss of service) and issues of planning permission.

[10] Garbin and Shortle (2007) Measuring resilience in network-based infrastructure. Critical thinking: Moving from infrastructure protection to infrastructure resilience, CIP Program Discussion Paper Series, George Mason University.

[11] Moody (2007) The need for resiliency at the corporate level. Critical thinking: Moving from infrastructure protection to infrastructure resilience, CIP Program Discussion Paper Series, George Mason University.

Delivering greater resilience in critical infrastructure

This chapter explores issues related to the delivery of greater resilience in critical infrastructure. It contains sections on:

- economic regulation;
- incorporating resilience into regulators' and utilities' activities;
- funding additional resilience in the privatised utilities;
- incentivising greater resilience;
- better co-ordination across sectors; and
- enhancing the resilience of the road transport network.

Economic Regulation

Introduction

16.1 Our analysis of essential services has focussed on the facilities, systems and networks that are provided by Category 2 responders under the Civil Contingencies Act 2004. These include the privately owned assets of utilities companies and the state owned road network.

16.2 The privatised utility companies' obligations, investments and prices are overseen by the economic regulators due to their position as industries with vital monopoly networks or network elements. This is true of electricity and gas (overseen by Ofgem), water (overseen by Ofwat), telecommunications (overseen by Ofcom) and railways (overseen by ORR). The strategic road network is publicly owned and not subject to the same economic regulation. For this reason, roads are dealt with separately later in this chapter.

16.3 The interim report concluded that the economic regulatory frameworks provide an obvious route for funding work to reduce the vulnerability of infrastructure assets owned by the private sector. They also provide a framework within which standards can be set, incentives provided and progress monitored.

Economic regulation in practice

The main responsibility of the economic regulators is to ensure that customers are provided with a secure supply of acceptable quality, at the minimum price. This includes a rate of return to shareholders that allows privately owned and financed companies to meet their investment needs.

In the UK, companies agree 'overall revenue allowances' in advance with their economic regulators over five-year planning periods. This may be for total investment (as with the water companies) or just for all or some part of network investments in pipes, wires and similar (as with electricity, gas and telecoms). The companies' investment plans take account of expected demand, likely efficiency improvements, quality standards and other factors, including changes in UK government or EU-mandated standards. If companies can meet their obligations with lower investment or operating costs, they can keep the revenue savings for up to five years; if their expenditures exceed the projected expenditures, they earn a lower rate of return than projected.

The investment plans of the regulated utilities – and of roads – include the costs of environmental requirements agreed with the Environment Agency and of health and safety regulations as agreed with the Health and Safety Executive. These costs, which are subject to prior cost-benefit appraisal, are treated as an allowable cost by the economic regulators in setting revenue targets and projected capital and operating costs at the five-yearly regulatory reviews.

In contrast, there are no *explicit* standards for the resilience of infrastructure to flooding and similar events. The resilience of infrastructure assets is usually an *implied* item in the projections for operating and capital expenditure, for example, as a guaranteed service standard in the water supply industry.[1]

16.4 In response to the interim report, the Review received a number of submissions from utility companies supporting the principle that improvements in resilience should be considered more explicitly as part of the existing regulatory process. Views were also expressed by the Government, regulators, consumer bodies and a number of utilities who agreed with the principle but set out the need for effective analysis to ensure that the benefits of any future improvements were balanced against the costs.

16.5 The Review explored a number of issues related to how economic regulation could help improve resilience, including holding discussions with a wide range of people including utility companies, regulators, financial specialists, academics and other experts, as well as reviewing the literature.

Efficiency at the expense of resilience

16.6 Utility regulation has focused primarily on monopoly issues and their implications for prices and quality. The general objective of economic regulation has been to promote competition where possible and to regulate where it is not. The evidence is clear that the Government's policy on economic regulation has successfully delivered by driving up efficiencies and reducing costs to customers. It has also facilitated billions of pounds of investment in improving customer service and, in the case of the water and energy industries, on improved environmental outcomes. In addition, regulators have acted with the regulated companies, where economically justified, to maintain and improve quality standards and day-to-day reliability. This will have contributed indirectly to resilience.

16.7 The events of summer 2007 have focused attention on other aspects of the operation of these utilities – their resilience to flooding events. Some commentators have suggested, that while efficiency and underlying performance have been improved, it may have been at some loss of resilience to low probability, high consequence events such as flooding.[1,2] For example Helm states: *'…that*

[1] Helm, D., February 2008, Utility Regulation and Critical National Infrastructure, www.dieterhelm.co.uk
[2] de Bruijne, et al., 2006, Assuring high reliability of service provision in critical infrastructure, Internation Journal of Critical Infrasstructure, Volume 2, Number 2/3

critical national infrastructure has not received much attention and this comparative neglect has begun to be reflected in the responses to a series of events – from terrorist threats [to]...the impacts of flooding'.

16.8 Discussions with a number of utility companies in the water and electricity sector during the course of the Review has suggested that the drive for efficiency may have removed some of the redundant capacity in the networks, which would make them more vulnerable than otherwise. For example, utilities companies have replaced large numbers of small assets with fewer, larger assets in order to become more efficient. While there are clear benefits for consumers and the wider economy in the form of reduced costs, a number of commentators believe that this step has increased public vulnerability as the consequences of failure will be much more significant.[3]

16.9 The Review found no clear quantitative evidence that overall resilience has declined under the current regulatory approach. Nevertheless, the events of summer 2007, and other events such as the Carlisle flooding in 2005 and the November 2007 near miss coastal surge show, firstly, that there is a clear need for improvement in the resilience of utilities to low probability, high consequence events where this can be demonstrated to be necessary; and, secondly, that stronger incentives should be placed on the utilities to achieve this. The predicted trend of increasing likelihood of high consequence events such as flooding[4] mean that current levels of resilience are likely to be insufficient for the future.

16.10 We agree with the ENA's assessment that whilst weather and flooding together accounted for around the same level of outages as aging equipment, the summer 2007 floods demonstrated the potentially catastrophic one-off loss that people affected found so difficult to accept.

Taking account of low likelihood, high consequence shocks

The Energy Networks Association (ENA) report that during the period April 2004 to December 2007, which included the exceptional level of flooding in 2007, losses of supply due to flooding accounted for approximately 4 per cent of the total customer minutes lost at high voltage and above. By comparison other weather events such as lightning strikes and high winds accounted for some 22 per cent and ageing equipment accounted for about 25 per cent of the total customer minutes lost.

The ENA have said that *'In view of this, expenditure to reducing the overall level of customer minutes lost is unlikely to be targeted at flood risk. However, the societal impact of electricity supply loss during a flooding incident, in particular the possibility of a large concentration of consumers being disconnected in a single incident will provide a substantive focus for any additional investment to improve resilience to flooding'* .

This shows that, since flooding is a relatively rare event, it also is a relatively low cause of average annual disruptions in supply. However, as the summer 2007 floods demonstrated, while these events are low likelihood, when they do occur they can be potentially catastrophic to a large population of people. We need to have the right framework in place to ensure the utilities make sufficient provision to protect against such events.

16.11 In economic terms resilience to flooding or other extreme weather is an 'externality'. While utility companies are concerned with resilience for longer term reputational commercial effects as well as for short term supply consequences, it is doubtful that they will take into account the full social costs and benefits of resilience to low probability, high

[3] Egan, M., 2007, Anticipating future vulnerability: Defining characteristics of increasingly critical Infrastructure-like systems, Journal of Contingencies and Crisis, Volume 15, Number 1

[4] Foresight Future Flooding, 2004, Office of Science and Technology

impact events. For example, given the low overall impact of flooding on annual average outages, there is not likely to be a strong enough incentive to ensure sufficient provision and investment in response without explicit Government intervention. Defra Ministers said, when giving evidence to the House of Lords Select Committee on Regulators, that:

> *"if you have economic regulation that is focused narrowly on the economics you miss all the important externalities, such as the impact on the environment ..."*

16.12 As for other externalities, such as the environment and health and safety, we are proposing that the Government set out explicit standards against which investments should be planned and appraised (see previous chapter).

What is an externality?

An externality occurs when a decision by people involved in an activity causes a cost or benefit to a 'third party' who were not involved in the original decision and whose interests were not taken fully into account. Because the 'third party' costs and benefits do not form part of the calculations of the people deciding to go ahead with the activity, they are not fully reflected in the price and are a form of market failure.

For example, air pollution may be generated by some manufacturing processes which has adverse consequences on others who live down-wind and whose interests were probably not taken into account.

In general, the best way of correcting for externalities is to require the costs and benefits to the third parties to be included (internalised) into the calculations of those engaged in the economic activity. This can be done in many ways including: the use of classic regulatory controls, by economic instruments and by voluntary agreements between the parties. An example where internalising costs has been used to good effect has been the regulatory induced reductions in sulphur dioxide emissions from power stations over the last 20 years

Incorporating resilience into regulators and utilities activities

16.13 Utility regulators are 'independent' of government with each having a series of primary and secondary duties in legislation. Primary duties tend to be general and focus on promoting customers' interests and ensuring that efficient utilities can finance their functions. Secondary duties cover a range of considerations that regulators must have regard to, such as sustainable development. Balancing the tensions between these objectives is part of the regulators' role. The post-privatisation focus on monopoly issues has led a number of commentators to conclude that resilience for critical infrastructure will not be provided for without intervention.[5,6]

16.14 In the opinion of the Review the resilience of critical infrastructure to low probability, high consequence events is a fundamental point of public interest. The statutory framework within which the economic regulators work includes a range of terms including 'consumer interest', 'public interest', and 'citizen interest'. The recent House of Lords Select Committee Report provides a detailed examination of what this means in practice. The Report concluded that the *"regulators can therefore be given specific duties that are considered by Government and Parliament to represent the public interest ..."* . In its response to the Report, Government agreed that it was for *"Government and Parliament collectively to define the public interest and the specific duties which flow from it, and for regulators to decide how best to satisfy ... those duties in accordance with its statutory framework".*

16.15 In line with the House of Lords Report[7] and the Government's response on 'public interest' and duties that flow from it, the Review believes that regulators should be given an explicit duty to take resilience into account, along with guidance to ensure clarity and that it is given appropriate regard. This would ensure that the issue was incorporated into price reviews and providing allowances in the operating and capital expenditure plans

[5] Helm, D., February 2008, Utility Regulation and Critical National Infrastructure, www.dieterhelm.co.uk
[6] Lewis, J.A., 2005, Cyber security regulation in the United States, Telecommunications Policy, Volume 29, Number 11
[7] House of Lords Select Committee on Regulators, First Report of Session 2006-07: UK Economic Regulators

of the utilities on a sustainable basis. Indeed regulators may in turn consider agreeing with the companies a specific licence modification to improve the resilience of critical assets and networks. The House of Commons Environment, Food and Rural Affairs Committee report into the floods[8] included a recommendation that a specific duty be placed on utilities companies to ensure the resilience of the supply system. However, it is also essential that, in making changes to improve the level of provision for resilience, regulators ensure that companies are not incentivised or allowed to make enhancements that do not represent good value for money.

16.16 The Review recognises that it may take some time to legislate for a new duty, but would welcome the Government issuing interim guidance to the regulators in the form of resilience obligations to be met by utilities companies that are based on the Government set standards to ensure essential services are appropriately protected against low likelihood, high consequence events. These could then be implemented via existing licence procedures. This should happen in time to inform the next price review processes.

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

Funding additional resilience in the privatised utilities

16.17 Action will be required in order to meet the standards for resilience, including protection. The expectation would be for companies to develop options for a programme of measures and submit this to the economic regulator for approval. In particular, we would expect companies to prepare plans specifying how in practice they intend meeting the standards for their defined criticality band.

16.18 It would not be for the economic regulators to construct these plans; it is for the companies to do so. The role of the regulators is to discuss and eventually approve both the plans and then, subsequently, the agreed capital and operating expenditures necessary to implement them. This will:

- maximise the use of specialist knowledge that companies have to target investment, developing efficient solutions to resilience problems;
- give companies strong incentives to devise improvements in technology, management and organisation to meet the standards more efficiently; and
- define the risks that the regulated companies must manage but where the regulator supervises and approves the risk approaches and models adopted by the regulated companies and then monitors and enforces their operational use by the companies.

16.19 As indicated earlier, this approach builds on current models of how utility regulators such as Ofwat and Ofgem handle environmental rules that are set by the Environment Agency. The agreed obligations (justified by cost-benefit analysis and other information) become part of companies' licence conditions which provides monitoring and enforcement powers. They are also included in the appraisal and approvals of companies operating and capital expenditure proposals.

16.20 The Review believes that the goal should be to try and optimise investment to get the greatest value for money. Cost-benefit analysis will be an important element in assessing what is acceptable to both private and public sectors. The first important test is whether the benefits of action outweigh the costs. Not all measures identified to improve the resilience of infrastructure or services will pass such a test. Hence, in some cases, it may be more appropriate to take lower cost options or simply prepare for unexpected events through business continuity and emergency planning. Even if the cost-benefit test is passed, questions of affordability and prioritisation will still arise.

[8] House of Commons Environment, Food and Rural Affairs Committee, Fifth Report of Session 2007-08: Flooding

16.21 The Review recognises that investment in resilience will need to take a phased approach over a number of periodic reviews. This will ensure that investments in improvement are both affordable and realise an optimal return by taking account of priorities, cost-benefit analysis and asset replacement strategies.

Incentivising greater resilience

16.22 By creating incentives, the Government and regulators can encourage certain types of behaviour. Ofgem have developed a set of incentives on quality of performance by all regulated companies (e.g on number and duration of supply interruptions). This included rewards for out-performance as well as penalties for under-performance. Figures indicate that there has been significant improvement in underlying performance since the introduction of the incentive scheme. Ofwat also has standards for water quality as well as leakages.

16.23 The Review believes that operational targets could be delivered for flooding and/or natural hazard resilience that allow out-performance to be financially rewarded and under-performance to be penalised. This would be analogous to current treatment of other quality standards e.g. by Ofgem.It may be that rewards or penalties could be attached to performance in business continuity or emergency exercises.

16.24 We suggest that these and other methods of incentivising resilience improvements are best considered by the economic regulators in discussion with the companies, consumer panels and other relevant parties.

Severe weather clauses

16.25 Regulators impose economic sanctions on utilities for prolonged disruptions to service. For example, in the water industry the Guaranteed Service Scheme requires water companies to pay compensation to customers for failure to supply. However, the regulations also contain a severe weather clause, which allows companies to claim exemption from paying compensation in the case of an event such as last summer's floods.

16.26 The rationale for this exemption is to provide a 'safety valve', so that companies are not liable to pay compensation in circumstances that are beyond their reasonable control. Other exemptions include unforeseen circumstances and industrial action. Interestingly, water companies do have to pay compensation where essential household water supplies are interrupted as a result of restrictions authorised by emergency drought orders. However, because of the lead-time, problems can be foreseen and planned for.

16.27 In the water industry, there are no formal criteria setting out what constitutes 'severe weather', leaving it to the discretion of the regulator whether or not to allow the exception. This means that there is no clear signal about the level of performance expected in relation to severe weather events. Had the severe weather exemption not been applied, Severn Trent Water would have been liable for approximately £35 million in compensation. The result of a lack of robust economic sanctions during severe weather events may have had a perverse effect on resilience. Thus, when water companies are considering the risks to their business and/or undertaking cost-benefit analysis for enhancements, there is no clear incentive to improve the resilience of assets to low probability, high consequence events.

16.28 The electricity regulator Ofgem has taken action in this area. Following wind storms in 2002, Ofgem realised that it needed to improve resilience by taking steps to restore the supply of electricity to customers cut off by bad weather more quickly. Following an industry review, Ofgem decided to increase the incentives to restore supply quickly and make distribution companies liable to compensate customers for prolonged loss of service for all but the severest of storms. Unlike water, the electricity sector does have defined service thresholds for what constitutes severe weather payments. This provides clarity on the rights of customers and the obligations on companies, sending stronger signals as to the level of service required.

16.29 The Review did not have sufficient time to come to a conclusion on a definitive solution to this issue, but the Review would welcome Ofwat examining whether stronger signals can be provided by setting out what constitutes severe weather for the water industry.

Defining an agreed set of expectations

EDF Energy told the Review that the strengthened Guaranteed Service Standards that came in following the severe storms in 2002 to improve compensation arrangements for loss of supply due to severe weather, has had a number of impacts which have acted to improve resilience.

The standards define restoration times for given sizes of event and a common framework and standards for customers across all regions. The company said: *'this has focused our management of events on meeting these expectations' and that 'much of this has come from there being an agreed set of expectations about what level of service should be delivered and what the customer can expect if this is not achieved.'*

Valuing the benefits of greater resilience

16.30 The events of summer 2007 underlined the severe impact on society of a prolonged loss of supply of essential services to a large population. This can be potentially catastrophic, particularly where the loss is combined with the failure of other infrastructure or other aspects of the emergency response. For example, in the summer 2007 events, the loss of electricity supply to large concentration of people who had already lost mains water was only just narrowly averted – if it had happened it could have extended the emergency caused by the flooding to something much bigger, the evacuation of hundreds of thousands of people and, in turn, to potential social unrest and risks to public health.

16.31 However, although cost benefit tests are the appropriate method of ex ante appraisal, they may well currently underestimate not only the full impacts on customers but fail to take proper account of the costs to the wider economy and society resulting from large-scale emergencies. Valuing the benefits of more protection to large scale emergencies and the catastrophic losses that they cause can be very difficult and great care must be taken if it is to be done adequately.

16.32 The economic regulators and utilities companies' use of 'willingness to pay' measures seems appropriate for relatively minor and/or short duration interruptions to supply. This is, not least, because consumers are likely to have experienced such interruptions. However, we have doubts about whether this tool can incorporate the impact of large-scale events where 100,000s of people are without essential services for extended periods. They cannot be readily scaled up – a week long interruption to water or electricity supply that causes a major civil emergency, puts major industrial facilities out of commission, or which ruins all the food stored in household deep freezers has a far greater cost than a simple multiple of the cost of a six-hour interruption that has little impact beyond inconvenience.

16.33 More significantly, because very few people have any experience (let alone recent experience) of the consequences of extreme weather events, it is very difficult for most people to set a value of the cost of avoidance.

16.34 Standard 'willingness to pay' and similar techniques deal badly with unusual and extreme risks, particularly when difficult ethical issues such as the value of peoples' lives are involved. Hence, it would seem sensible for 'willingness to pay' methods as currently used in cost-benefit analyses of utilities' proposed expenditures to be supplemented by additional and better-suited information so that the actual costs of the worst case credible scenario can be properly accounted for.

Case study: Risks from major electricity supply interruptions

The impact of the loss of electrical power extends well beyond the immediately obvious consequences. For example, loss of traffic lights can lead to traffic chaos and motorway gridlock, which will have a knock-on effect on peoples ability to go about their daily lives as well as on the emergency services' ability to respond. The mobile telephone system will become overloaded and probably fail completely within eight hours. Domestic central heating – even gas fired – will fail as boilers and central heating pumps require power.

Water supplies and sewerage will be affected to varying levels. Petrol pumps, tills and ATMs fail, radio and TV broadcasts would stop. There is an increased risk of fires as people resort to using candles and cooking over fires. Only those sectors equipped with stand-by generators and fuel supplies would be able to continue for a time.

In summer 2007, flooding at Walham substation in Gloucestershire – which would have led to power loss to 500,000 people – was only averted by the deployment of 250 military personnel and temporary defences which were only available because they had not been used at Upton-upon-Severn.

16.35 Other possibilities for measuring the benefits of resilience include more sophisticated survey methods that include attempts to take account of the consequences for whole areas, the wider economy and society as well as the costs on individuals and specific firms. Simple questionnaire approaches are not likely to be as useful as 'citizen jury' and other expert-led focus group techniques. Participants are exposed to a variety of different approaches and views; they can pose questions to the experts and debate amongst themselves; and the final verdict can be compared with the initial position. When these work well and the issues (and trade-offs) are clearly spelled out, such techniques can provide useful, informed guidance on 'willingness to pay'. The Review has heard of an example of where one utility company are developing new techniques to take better account of the value of avoiding large-scale service failure and consequential civil emergency. Economic experimental approaches may also be potentially useful.

Deliberative approaches to understanding consumers' views

Deliberative approaches to understanding consumers' views have been used by the Consumer Council for Water (CCWater), particularly where it has been important to get behind consumers' views of issues, or where there are difficult trade offs involved.

For example, in its work on fair charging for water, CCWater has involved participants by first meeting in small groups at the start of the process. They were presented with a range of informative material to guide them in self-deliberation over the next one or two weeks. Groups were then reconvened in workshops across England and Wales where participants engaged in group-deliberation around the key themes. The research provided real insight into consumers' perspectives, for example revealing little understanding of how water bills are calculated and what they are actually paying for; concerns over perceived excessive water industry profits and its monopolistic position; strong and swift rejection of social tariffs; little appetite for alternative metered tariffs, and rejection of private subsidy for those who are vulnerable.

16.36 The Review would welcome economic regulators working with companies to develop new tools to improve and complement the 'willingness to pay' studies to incorporate the costs of large-scale disruption into the decision-making process.

Better co-ordination across sectors

16.37 The problems that can arise as a result of vulnerabilities at interfaces between networks and the gaps that can occur between boundaries of organisational responsibilities are well known. Recent studies and reports emphasise how, since the 1980s, critical infrastructure in the industrialised world has become increasingly interrelated and dependent on each other's 'always on' availability. Commentators have expressed alarm at the ability of these complex systems to be managed under stress and their increasing vulnerability to large-scale cascading events across sectoral boundaries.[9,10] The summer 2007 events come close to realising these fears.

16.38 The critical infrastructure must be viewed as an interdependent system, where resilience improvements within one sector could be completely negated by the vulnerability of a key supply component in another. Even if that vulnerability has been identified in a business continuity plan (see Chapter 17), the question will still arise of who bears the costs, since improving resilience in one sector such as electricity will also bring benefits to customers in others.

16.39 Such issues will need to be considered in cross-sectoral discussions to exchange information and ensure coverage of potential gaps and minimise overlaps. They can consider how best to target investment across networks in order to optimise the benefits to the critical infrastructure system as a whole and identify appropriate funding mechanisms. This approach is in agreement with the House of Lords Select Committee conclusion that *"action is necessary to improve regulators' joint working. There needs to be a more structured and formal cooperation between the regulators if it is going to be meaningful."*

16.40 The Review would welcome, that the issues related to better coordination across sectors, be tackled at a joint regulators group. This would help to support the implementation of measures flowing from the proposed National Resilience Plan where issues of cross-subsidies between sectors are raised.

Enhancing the resilience of the road transport network

16.41 The road transport network presents different issues in relation to improving resilience to flooding and severe weather events. In broad terms, for trunk roads and motorways – the strategic network, which is the focus of this section – the levers to improving resilience are with the Department for Transport (DfT) through its funding of the Highways Agency. For local transport the levers are with the local authorities and, for London, the Greater London Assembly.

Roads network: funding mechanisms

DfT funds trunk roads and motorways through the following broad channels, subject to the DfT's or the Highways Agency's project appraisal requirements:

- Local Network Management Schemes. Programmes of small schemes making better use of the existing network;
- Targeted Programme of Improvements – major schemes funded by DfT or public-private partnership; and
- Capital and Routine Maintenance funding.

16.42 The Highways Agency's current activities to improve reliability of the strategic network fall under its PSA target for journey time reliability, within which severe weather is an important factor. For 2007, flooding on one day alone – 20 July – caused 2 per cent of the delays for the whole year. The flooding of what was a small part of the road network last summer led to up to 10,000 people being stranded. As part of its mapping of high risk weather sites under this target, the Highways Agency is identifying those parts of the strategic network liable to flooding.

[9] Little, R. G., Controlling Cascading Failur: Understanding the vulnerabilities of interconnected infrastructure, Journal of Urban Technology, Volume 9, Number 1

[10] Amin, M., 2002, Towards secure and resilient infrastructure, Journal of infrastructure systems, volume 8, Number 3

16.43 The Highways Agency has a number of measures to improve resilience including establishing "Off Network Diversion Routes" (pre-identified routes that by-pass sections of the strategic network) and improved response procedures. We note that the Highways Agency has also taken a number of measures to provide priority access to emergency related services, localised flood protection, sand bays (for storage and filling of sand bags) and drinking water contingency supply to ensure road users health and safety in the event of disruption due not only to flooding, but also accidents or high summer temperatures.

Responding to climate change

16.44 The 2004 Foresight Future Flooding Study identified that carriageway flooding incidents were expected to increase substantially by 2085 due to a 20 to 30 per cent increase in predicted rainfall. In anticipation of climate change and more frequent and heavier rainfall, drainage standards were reviewed following the severe flooding events of autumn 2000. Since then standards for new works and drainage maintenance renewals have been raised to provide increased capacity for the 20% to 30% increase in rainfall intensities expected up to 2085. Also, a programme of work is in its early stages to identify those structures, such as culverts, which may not function as intended within the frequency and higher levels of rainfall now predicted and experienced.

16.45 We consider that, in relation to trunk roads and motorways, there are enough levers available through funding and other mechanisms for a programme of improvements to the resilience of these networks. We note the work that is currently under way to address resilience to today's events and to cope with the effects of climate change.

16.46 The Review would welcome the Highways Agency looking at the vulnerability of the most significant elements of the road network to flooding. The Government should specify for the Highways Agency those standards of performance that the strategic network should aim to meet in relation to its resilience to flooding.

Minimising the loss of services

This chapter proposes a way in which organisations' abilities to absorb the effects of emergencies can be enhanced. It contains sections on:

- summer 2007;
- business continuity management and its benefits;
- British Standard 25999;
- the current framework: business continuity and the law
- proposals for enhancing capabilities;
- accountability and governance; and
- planning assumptions: expecting the unexpected.

Introduction

17.1 It is not possible to anticipate all hazards, nor is it practical on economic or any other grounds to protect all assets against all risks. Exceptional events have the potential to overwhelm defences; so an essential element of minimising disruption should be to plan to withstand and recover from such events. However, the events of summer 2007 suggest that planning for failures has been patchy and inconsistent.

17.2 The Government's national approach to civil emergencies seeks to minimise the impact of events through planning and preparedness. Improved business continuity management (BCM) has an important part to play in attaining that goal by minimising the potential for disruption to essential services in the event of a flood or any other disruptive event.

Summer 2007

17.3 Last summer, Gloucester Gold Command anticipated that if Walham electricity substation had been inundated, electricity would have been lost for up to three weeks. The flooding of Mythe Water Treatment works left people without water for 17 days. We believe greater uptake of effective BCM could minimise the potential for such lengthy disruption occurring in the future.

17.4 That is why our interim report proposed Government introduce a duty on national infrastructure operators to undertake business continuity planning to more closely reflect that on Category 1 responders. We also suggested that the British Standard on BCM, BS 25999 should be prescribed.

17.5 Our proposed recommendations generated a positive response. For example, evidence from Water UK emergency planners' group pointed out that a significant number of water companies support the adoption of BS25999 for their business continuity planning and are adopting the standard to protect against disruption to their businesses. A number of other Category 1 and 2 responders also agreed with this proposal. The Review welcomes this feedback.

17.6 However, some responders believed that the intention of the interim conclusion was to replace current sector-specific operational emergency planning duties placed on them through sector-specific legislation. The intention was not that BS 25999 should replace current approaches to risk management, emergency planning or mandatory contingency requirements such as the Security and Emergency Measures Direction (SEMD) in the water industry. The Review takes the view that, though they are complementary disciplines, sharing similar ideologies, the focus and methods of business continuity differ from those of emergency or risk management.

17.7 We note and endorse the work being undertaken by some Category 2 responders since summer 2007 to update and improve their business continuity arrangements. Severn Trent Water has acknowledged that the floods led it to question the appropriateness of accepting such widespread interruptions to service. The company is now taking the opportunity to review and update its plans.

17.8 There is still scope for improvement. The Chartered Management Institute's (CMI's) 2008 review of BCM reports that, of the 17 utility companies that responded to their survey, a third had not exercised or tested their business continuity plans (BCPs) at all.[1] This, along with evidence from consultation responses and our discussions, indicates that organisations are taking forward business continuity initiatives at different speeds and to different standards. Some were not motivated to act at all; especially those that were not affected by the 2007 floods.

Business continuity management and its benefits

17.9 A resilient organisation is one that is still able to achieve its core objectives in the face of adversity. This means not only reducing the size and frequency of crises (by identifying and managing vulnerabilities in advance), but also improving the ability and speed of the organisation to manage crises effectively when they occur.[2] BCM is a process which increases organisational resilience by helping manage risks to the smooth running of an organisation or delivery of a service and ensuring that it can either continue to operate and deliver critical functions in the event of a disruption or that, in the event of loss, it is reinstated as quickly as possible.

Defining business continuity management

The British Standards Institution defines BCM as: "*A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*."[3]

17.10 Evidence suggests that some Category 2 responders do not understand what BCM is and how it differs from emergency management. For the purpose of the Review, emergency management is defined as the process that deals with the initial or acute phase of an incident. BCM has a wider focus, providing a wider strategic and operational framework for reviewing how an organisation delivers its products and services and increasing its resilience to disruption, interruption or loss. As such, BCM would not replace emergency management but would complement and work alongside such systems.

[1] CMI 2008 report, utilities-only data.
[2] E. Seville, *Organisational resilience: Researching the reality of New Zealand organisations*, Journal of Business Continuity and Emergency Planning. Vol.2, No.3 p.258.
[3] BS25999-1 British Standards Institution's Code of Practice for Business Continuity Management.

17.11 Defining what is within the BCM system is influenced by the environment and context within which the particular organisation delivers its services. Decisions on which products, services or locations are included within the scope of BCM may be prompted by regulatory or statutory requirements or by perceived high-risk locations due to physical threats such as flooding. This may mean that an individual business continuity manager sees security, IT availability or risk management as the key issue with other areas taking a less prominent role. This is why it is so difficult to reach a consensus on precise BCM responsibilities.

Benefits of BCM

17.12 The insurance broker Marsh surveyed BCM and identified the following benefits of its adoption: a better understanding of the business; faster recovery and reduction of negative impacts after incidents; improved risk-intelligent decision-making; and reduced insurance premiums.[4] The report concluded that such benefits yield rewards for businesses. Such findings are supported by the Chartered Management Institute's survey on BCM in which 76 per cent of managers' questioned reported that they regarded BCM as important to their organisation.

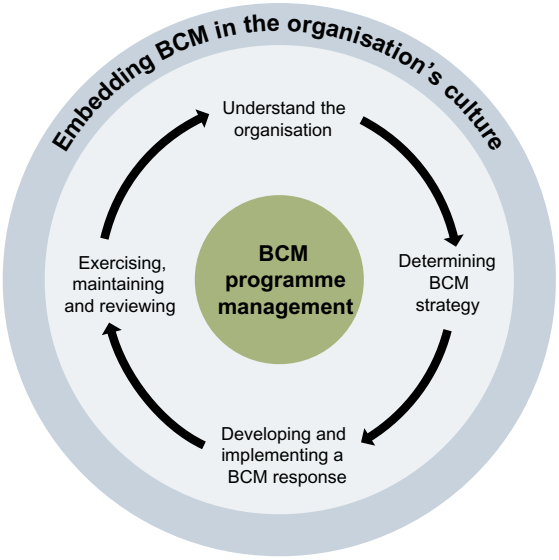
17.13 Within the wider business community, acceptance of the need for BCM is now almost unanimous. Many organisations view it as a good practice tool which they can use to manage their overall operational risk management challenges and help them protect their reputations as well as recovering critical business processes.

17.14 The CMI's 2008 report found that many organisations, including infrastructure companies, across the UK are failing to provide adequate protection for their key assets and, therefore, for the public. The report concluded that, while many companies appear to be failing to carry out BCM, 93 per cent of respondents with plans in place agreed that such plans had reduced disruption to the delivery of their services.

The BCM lifecycle

BCM is an iterative process which aims to ensure that organisations monitor and manage business continuity on an ongoing basis. There are five stages in the process:

- **Understanding the organisation**: identifying key products and services and the critical activities and resources that support them.
- **Determining the BCM strategy**: this will depend on a range of factors, including the maximum tolerable period of disruption of the critical activity, implementation costs and the consequences of failing to act.
- **Developing and implementing a BCM response**: plans and arrangements should cover incident management and continuity of key services.
- **Practising, maintaining and reviewing the BCP**: a BCP cannot be considered reliable until it has been thoroughly tested and proved workable.
- **Embedding BCM in the organisation's culture**: creating understanding and acceptance of BCM within the organisation is essential.



[4] M Caddick, *The upside to business continuity*, 2008. www.continuitycentral.com/BCMbenchmarkfindings.pdf

17.15 The Review believes that identifying risks and making plans for managing disruption in advance can reduce the costs to an organisation in terms of both financial expenditure and management time. As such, the benefits of implementation far outweigh the potential costs of not acting.

Identifying interdependencies

17.16 The Review takes a systems view of critical infrastructure, recognising that there are multiple interdependencies within and between different organisations that influence their ability to respond and recover. This means that effective organisational resilience for any one organisation must look beyond that single organisation and consider the resilience of other organisations on which it depends.[5]

17.17 The events of summer 2007 saw infrastructure fail as a result of flooding and due to interdependencies which had not been recognised ahead of time. Subsequent discussions with utility companies have revealed that, before the summer, electricity companies were unaware they were supplying other elements of critical infrastructure, such as large water treatment works, in their distribution area.

17.18 BCM requires that organisations look not only at the resilience of internal structures, but also at the resilience of the structures they rely on – their supply chains. They should then look at ways of ensuring the plans of those they rely on are resilient as BCP is only as strong as its weakest link. We give a specific example of this in Chapter 18.

British Standard 25999

17.19 The British Standard on business continuity, BS 25999, aims to promote greater consistency in organisations' approaches to BCM and reassurance to all stakeholders of conformity to best practice. Our dependence on essential services such as electricity and water means that society itself is a stakeholder in this context.

17.20 The Standard, is intended for use by all organisations in the public, private or voluntary sector with responsibility for business operations or the provision of services. However, levels of awareness and adoption vary widely. Discussions with Category 2 respondents show that some Category 2 responders are completely unaware of the standard, some have drawn on it to maintain business continuity for their office-based businesses and others have applied it to their whole operation. Of the 17 gas or electricity companies that responded to the CMI's 2008 survey, 20 per cent had evaluated their plans against BS 25999. This is a good foundation on which to build. But the Review is concerned that the same data suggests that a third of Category 2 responders do not evaluate their BCM capability against anything at all.

17.21 A number of responses to the interim report have asserted that BS 25999 is not applicable to asset-based services. The Review recognises that BCM has historically been associated with financial services but does not believe such claims are substantiated by evidence. As mentioned above, the scope of BCM is influenced by the environment and context in which the organisation delivers its services. There are pre-existing examples of infrastructure operating companies applying the standard to the critical elements of their business, and Category 2 responders were involved in the Standard's development. Some Category 2 responders who were not already using the standard were positive about how it could benefit their operations. For example, in its response to the interim report, Anglian Water stated: '*we have already begun to explore what will be required for Anglian Water to achieve BS 25999. We support this approach and believe that it will complement our current Quality Management Systems and Environmental Management Systems*.' Ultimately BS 25999 is a flexible management standard that can be adapted to take into account the individual needs of businesses of all shapes and sizes.

[5] E. Seville, Organisational resilience: researching the reality of New Zealand organisations, Journal of Business Continuity and Emergency Planning, Vol.2, No,3 p.258.

17.22 The Review believes that BCM undertaken in conjunction with additional investment for protection will go a long way to decreasing disruption to essential services resulting from flooding and other natural hazards. The use of a standard will make the desired outcome – more resilient critical infrastructure – consistent and certain for all stakeholders, public and government included.

PAS 55 Asset Management Specification

17.23 Evidence from the electricity industry indicated that they were positive about the use of BSI Publicly Available Specification (PAS 55) as a possible alternative to BS 25999. PAS 55 lays out a process for the optimised management of physical infrastructure assets. The specification is intended to apply in cases where an organisation is primarily dependent on the function of its assets in the delivery of services or products, the objective being to ensure that the assets deliver required function and level of performance in terms of service or production (output). The Review notes that electricity network owners were asked by Ofgem to adhere to the specification as part 7 of an Asset Risk Management Project – (which has now been discontinued). All major gas and electricity companies had been certified by February 2008.

17.24 We commend the use of the specification as an asset-specific approach to risk management. However, we do not believe the specification is as applicable to overall organisational resilience. BS 25999 is focused on all the factors surrounding and associated with disruptive events and can be applied to a far wider range of organisations. The focus of PAS 55 is not applicable to the task of broader event management and limits its use in connecting with the planning of others. The focus of PAS 55 does provide it with value as a component in the establishment of BCM within organisations, but the Review believes that alone it would not be as strong as the BCM planning required by BS 25999.

The current framework: business continuity and the law

17.25 There are no clear obligations in law on utility companies to undertake BCM in a consistent way. Contingency and preparedness for extreme weather events exist in some sectors, and some may have a strong financial incentive to recover as quickly as possible from an event. Even when there are such requirements, plans and policies are often found in a number of different documents relating to a number of different obligations.

Scottish Power

As a diverse company, involved in trading, generation, transmission and supply, Scottish Power recognises that implementing a meaningful and enduring BCM System can present a considerable challenge. The company decided to utilise Part 2 of BS25999, on the grounds that it provides a common framework for identifying key services and the measures needed to restore or maintain these services should they suffer interruption.

Along with the rest of the electricity industry, Scottish Power has well-rehearsed emergency plans for dealing with the consequences of severe weather and the safe restoration of supply; these are complemented by robust BCPs. The company recognises that alignment, or indeed certification, to the Standard does not guarantee that, when major events such as floods occur, there will be no problems. However, the application of the Standard does demonstrate that there is a quality management system in place to identify, monitor and continually improve continuity of key services.

The company's business continuity arrangements focus on protecting and resuming critical activities that support key services, including fault and emergency management.

Managing business continuity within a quality management system has enabled Scottish Power to effectively and demonstrably manage the risk to key service disruption, ensuring that the company has arrangements in place to recover key services, their critical activities and enabling resources.

Scottish Power have on several occasions utilised their plans and recovered the business within the expected timescale, or better. They believe the financial and non-financial impact mitigation has more than justified their initial investment in BCM.

Sector-specific legislation

Water and sewerage

Section 208 of the Water Industry Act 1991 and the existing direction of 1998 requires an undertaker "to make, keep under review and revise such plans as it considers necessary to ensure the provision of essential water supply or sewerage services, at all times, including a civil emergency". The Act also contains provisions about the assumptions on which plans should be based, and sets out specific requirements, for example for personnel to receive appropriate training and essential equipment to be stockpiled. Plans are presented to the Secretary of State and revised annually.

Electricity and gas

Under the terms of the operating licences issued by Ofgem, electricity and gas companies are under a general legal duty to ensure adequate levels of security of supply. This may include introducing some form of preventative, risk-assessment control.

For electricity providers, regulation 3 of the Electricity Safety, Quality and Continuity Regulations 2002 is the key provision, requiring generators, distributors and meter operators to construct, install, protect, use and maintain their equipment to prevent interruption of supply so far as reasonably practicable.

Gas companies are obliged to comply with the Gas Safety (Management) Regulations 1996. These are primarily aimed at safety rather than security of supply and set out a number of specific areas to be covered by continuity plans, including: dealing with gas escapes and averting danger; arrangements for minimising the risk of a supply emergency; and arrangements for dealing with supply emergencies or other incidents that could endanger persons.

Telecommunications

The Communications Act 2003 gives Ofcom the power to impose conditions requiring or regulating the provision, availability and use, in the event of a disaster, of electronic communications networks, electronic communications services and associated facilities on providers of electronic communications networks and electronic communications services.

Roads

The relevant highway authority for most roads will be the local authority, a Category 1 responder under the Civil Contingencies Act 2004. Beyond this, there are preventative planning obligations on the relevant highway authority such as the Highways Act 1980, although these fall short of requiring the preparation of statutory plans.

Rail

Rail operators are licensed by the Office of Rail Regulation. Licences require operators to provide a service which an efficient rail operator would be expected to provide. They are also under a statutory duty to operate in a manner which does not endanger the public under the Health and Safety at Work Act 1974. The Railways Act 1993 allows the Secretary of State to make directions in relation to railways in the event of a great national emergency.

The Civil Contingencies Act 2004

17.26 The Civil Contingencies Act 2004 (CCA) places very few direct legal obligations on Category 2 responders relating to BCM. Instead, it puts the emphasis on cooperation with Category 1 responders.

17.27 The CCA takes a principle-based approach, requiring Category 1 responders to maintain BCPs in order to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable. This duty relates to all their functions, not just their emergency functions. The CCA does not mandate a framework: rather, it allows Category 1 responders to choose their own model for meeting the legal requirement. However, the statutory Guidance issued under the CCA does provide a common approach for Category 1 responders to follow. This Guidance is based on PAS 56, the forerunner of BS 25999. This means that, unlike Category 2 responders, Category 1 responders have a more systematic and consistent approach to BCM.

Proposals for enhancing capabilities

17.28 The driver for business continuity and wider organisational resilience should be the long-term interests of stakeholders and all those who depend on the organisation in some way.[6] In the case of essential services delivered by critical infrastructure, these interdependencies are even more significant. Given the importance of this relationship, the Review believes the Government should act to increase the overall capacity of critical infrastructure operators to resist failure for as long as possible and recover quickly when faced with unexpected challenges. While we recognise that risk cannot be totally eliminated, the likelihood of an event threatening the business can be anticipated and the potential impact reduced.

17.29 The scale and complexity of critical infrastructure, coupled with the uncertain nature of natural hazards, means that effective cross-sector preparedness is a real challenge. Inconsistencies between required levels of preparedness for distinct sectors add to that complexity. Although there is a foundation of business continuity planning on which to build, coverage is patchy and approaches are inconsistent.

17.30 The events of summer 2007 serve as a reminder that this is an issue to be tackled. To shy away from it would leave society open to the possibility of a more serious loss of essential services – particularly as vulnerability to risk appears to be growing with time. As a society, we must deal with risks effectively. Ensuring that the essential services delivered by Category 2 responders are resilient to a consistent standard is a key aspect of this. The Review believes that this resilience is vital and that consistency of approach should be promoted by introducing BCP on a statutory basis.

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.

[6] Business Continuity Institute, *The good Practice Guide 2008*, www.thebci.org

Case study: Business continuity law in France

In France, business continuity is seen as a key part of the resilience framework. In 2006, a law was passed on the Security of Vital Infrastructure Activities in response to growing awareness of the risk posed to infrastructure operators by both natural hazards and security threats. The law obliges operators to include business continuity in their emergency plans.

It has been implemented sector by sector since 2006, with the energy, transport and water sectors being the fastest to comply. The state provides a framework for business continuity planning, and individual operators form their own security plan (with the help of government).

Accountability and governance

17.31 Nevertheless progress must be monitored. The Review has consulted stakeholders on a mechanism that could be used in order to hold companies to account. This involved the use of local scrutiny committees. Such committees have an important part to play, but also present a number of security issues. Concern was also expressed about the level of technical capability in local authorities (see Chapter 30 for a full discussion of making scrutiny work).

17.32 Each organisation needs to assess how to apply BS25999 or equivalent to their own organisation *'ensuring that their BCM competence and capability is appropriate to the nature, scale and complexity of their business, and that it reflects their individual culture and operating environment'*.[7]

Case study: Severn Trent Water and Gloucestershire Scrutiny Committee into the summer 2007 floods

As a result of exceptionally heavy rainfall in July 2007, Gloucestershire experienced two major emergencies and narrowly avoided a third.

Following the emergency, Gloucestershire County Council undertook a scrutiny exercise in order to build up a picture of the event, the response and what lessons could be learnt.

The committee was modelled on Select Committee proceedings. Approximately 35 organisations provided written evidence to the Inquiry, and of these 22 were selected to attend hearings to answer questions from the panel. These included Severn Trent Water, National Grid and Central Networks. Both Severn Trent and National Grid agreed to take part in the scrutiny process, but Central Networks declined on the basis that they were already working with the Local Resilience Forum. Questioning of companies focused on the events of July 2007 and how both organisations reacted to them. It covered areas such as each organisation's emergency plans for dealing with flooding, contingency arrangements and plans to improve future resilience.

The concept of attending a scrutiny committee was new to Severn Trent Water. However, in their experience the approach has facilitated:

- engagement with community leaders;
- enhanced working relationships with the community;
- assurance to the community that they are concerned with increasing resilience in their area and have contingency arrangements in place to respond and recover from an incident; and

[7] Business Continuity Institute, *The good Practice Guide 2008*, www.thebci.org

Case study *(continued)*

- increasing the awareness in the community of what the company does as an organisation

Although unfamiliar at first, Severn Trent Water conclude that the experience of the enquiry was valuable in rebuilding trust with the community and developing good working relationships.

The committee's final report, along with copies of the uncorrected transcrpits from hearings, can be downloaded from the Glousester County Council website: www.glousestershire.gov.uk/inquiry

17.33 However, we believe that the Government must ensure business continuity provisions are technically robust and deliverable. **We would welcome Government utilising a light-touch, benchmarking approach, ensuring accountability for BCM by obliging regulators or sponsor sector departments to conduct sector-wide benchmarking exercises through which companies can assess whether their level of business continuity is average, or significantly above or below average.** This approach will have the added benefit of allowing the Government to assess the level of resilience within each sector and would form part of the proposed Sector Resilience Plans. The output of the benchmarking exercise could be made public as part of the annual reporting process. This could act as a powerful incentive for companies, as a good reputation is often important for companies who would rather change their behaviour than lose their good reputation.

Case study: accountability and BCM in the financial sector

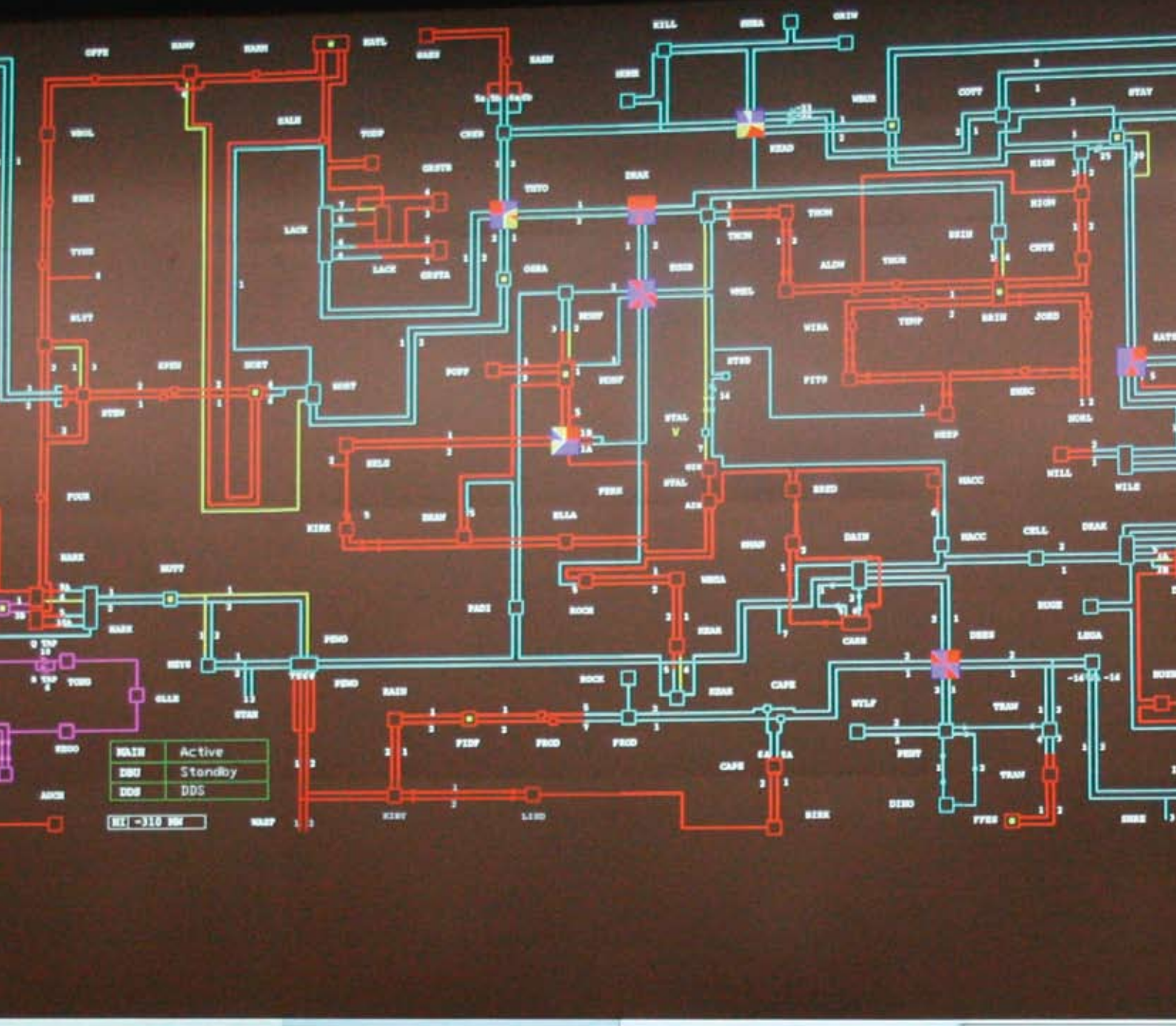
Resilience in the financial sector is crucial to the operation of the economy. For this reason, financial services, like utilities, are part of the CNI. The Financial Services Authority (FSA) takes a principle based approach to BCM. It stipulates that a firm must have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function in the event of an unforeseen interruption. It goes on to say that "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems".

To ensure compliance, the FSA runs a benchmarking exercise which firms pay to take part in. It consists of a detailed online questionnaire, where participants answer around 1,000 questions relating to their business continuity and crisis management arrangements. This allows the FSA to assess the overall business continuity preparedness of the UK financial sector, as well as seeing how individual firms perform against a benchmark and how they compare with their peers. Participants are those institutions which are critical to the well-being of the UK financial system in the first vital hours or days following a major operational disruption. Participants have responded well to this approach, with 76 per cent of those consulted by the FSA saying that the exercise has heightened business continuity awareness in their firms and 81 per cent agreeing that it had raised awareness in the sector as a whole.

Planning assumptions: expecting the unexpected

17.34 The work done by companies needs to be measured against clear outcomes. But business continuity and other forms of contingency planning are only as good as the assumptions that they are based on. In the UK, these take the form of National Resilience Planning Assumptions (NRPAs), published by the Cabinet Office and based on the Government's national risk assessment process. They are designed to inform emergency planning and policy formulation at all levels, and include estimates of the most significant consequences of various risks – including extreme weather events such as flooding – facing the UK over the next five years were to materialise. As such, they are intended to set the bar for resilience planning and capability building at national, regional and local levels.

17.35 The Review is concerned that because events such as floods are perceived as rare, they – along with other high-impact, low probability risks – may not be accounted for sufficiently in planning. The 2008 CMI report noted that only 31 per cent of respondents considered extreme weather as a threat in their BCM plans. We would like to see national infrastructure operators enhance their planning thresholds for flooding in the same way as they have done for recent high-profile risks such as human influenza. To this end, **we welcome the use by Category 2 responders of the NRPAs to inform the vulnerability assessment of critical infrastructure and develop measures to mitigate the risk**.


MAIN Active
DBU Standby
DDS DDS

Enabling better emergency planning through information sharing and engagement

This chapter explores issues around increasing preparedness through information sharing and enhancing response capabilities through early engagement.
It contains section on:

- information sharing in summer 2007; and
- local-level engagement for more effective emergency response.

Introduction

18.1 If local emergency planners (Category 1 responders) are to mitigate potential harm and respond effectively to events, they must first understand the scale and nature of the risks. The infrastructure sectors of interest in terms of the Review are all Category 2 responders under the Civil Contingencies Act 2004. Comprehensive community risk and vulnerability assessment cannot be done by any single organisation acting in isolation. Information is the lifeblood of effective emergency planning, and, as such, the sharing of information across the Category 1 and 2 divide and among all bodies involved in dealing with natural hazards such as flooding is essential. Effective working should also be based on wider engagement and cooperation with Category 2 responders. In particular, multi-agency response is likely to be more effective where all responders are well practiced and versed in the relevant protocols.

Information sharing in summer 2007

18.2 The events of summer 2007 exposed the fact that emergency responders had an inadequate understanding of the location of critical sites, their vulnerability to flooding, the likely consequences of their loss and interdependencies between sectors. The information local emergency planners needed in advance of events to enable emergency planning for loss of essential services was at best inconsistent, and at times completely unavailable.

18.3 As a result, agencies were severely hampered in their ability to respond quickly as events unfolded. For example, evidence to the Review indicates that the Gloucester Gold Command was initially unaware of the vulnerability and criticality of Mythe water treatment works and Walham electricity substation. As the EFRA Select Committee report notes, Gloucestershire County Council was unaware until the summer floods that

there was only one source of water supply and electricity supply in the area.[1] Discussions with other local authorities and Local Resilience Forums (LRFs) across the country indicate that many are similarly unaware of the risks associated with the loss of national infrastructure.

18.4 Had Gold Command been aware in advance that the loss of Walham would threaten the supply of electricity to half a million people in England and Wales, it would have been in a position to make contingencies accordingly. As it was, a huge effort by the military, fire services and others combined with the availability of temporary barriers, narrowly prevented the loss of Walham. Questions remain as to why information about such assets, their vulnerability and the potential consequences of their loss are not shared routinely with local responders in advance.

18.5 In light of these observations, the interim review report recommended that LRFs should ensure that Community Risk Registers reflect risks to critical infrastructure from flooding and other hazards. It also recommended that single points of failure and the complete loss of an asset were explicitly considered in the risk assessment and contingency planning undertaken by operators, emergency planners and responders. The success of both of those conclusions is dependent on an effective exchange of information.

Implementing recommendation 10

18.6 As a first step, the interim report recommended that *"Category 1 responders should be urgently provided with a detailed assessment of critical infrastructure in their areas to enable them to assess its vulnerability to flooding".* The Government agreed to the urgent recommendation and the Cabinet Office wrote to LRF chairs in mid-March 2008 setting out a standardised procedure for the secure sharing of such information (see Annex F). The Government's response to the review, which set out how each urgent recommendation had been fulfilled, highlighted the difficulty of overcoming security concerns but also stated that significant progress had been made in response to this recommendation.

18.7 The Review welcomes the spirit of the procedure but is not convinced that adequate progress has been made in attaining the level of sharing envisaged by the interim report. Feedback from stakeholders has been mixed with some LRFs displaying uncertainty and confusion over the process. At least two LRFs we heard from had received no briefing as yet, due to security sensitivities. Others had received their briefing but were advised not to cascade this information down to their risk and planning sub-group, again due to security concerns. As such, many planners are still taking an ad hoc (and possibly inefficient) approach to obtaining the information that they need.

18.8 LRFs in the south west of England reported that the briefing had been a step in the right direction as they were now in a position to map impacts of loss and consider single points of failure. Those who had found the process successful tended to be those who had recognised the validity of security concerns and acted to deal with them by ensuring all risk and planning group members had been security cleared to Security Cleared (SC) level. Others were concerned about the level of detail that they were given, which they deemed too high-level to assist planning for loss of services such as those witnessed last summer. Overall the view appears to be that, while oral briefings have been a basic introduction, what is really required is an ongoing dialogue with the utilities themselves.

18.9 More than one piece of feedback from LRFs mentioned problems with accessing the Environment Agency's Receptors Vulnerable to Flooding (RVF) data. On further consultation with the Environment Agency, it appears that there are legal issues around the sharing of RVF data. The data is composed of information from Ordnance Survey and the Centre for Ecology and Hydrology and is subject to an Environment Agency approved-access procedure. This deals with issues around third-party intellectual property and contractual rights and as such, the Environment Agency cannot license it for access by others.

[1] EFRA Committee, Fifth Report of Session 2007–08, Flooding, pp.36, 94

18.10 We understand that the Environment Agency has managed to reach agreement with certain data providers to release sections of the study to Category 1 and 2 responders for Civil Contingencies Act 2004 purposes, but only on a case-by-case basis. This position is unacceptable. **The Review would welcome greater effort by all parties concerned to overcome the problem in order that such information can be used effectively for contingency planning purposes.**

Gloucestershire LRF – work since summer 2007

Following the summer flooding and water supply failure, Gloucestershire LRF realised that it was not fully aware of vulnerabilities and single points of failure within the Critical National Infrastructure (CNI) supplying their county. It was concerned that without information on impact of loss emergency planners were not in a position to successfully plan for contingency.

As a result of their experience, the LRF infrastructure sub-group was tasked with gathering information to indicate the potential consequences if other components in Gloucestershire's infrastructure were to fail. To achieve this, five focus group meetings (highways, water, energy, telecoms and waterways) were convened with representatives of infrastructure operators in the county.

The aim of these meetings was to bring to light any resilience issues that may be known within the relevant industry, but which the emergency responders were unaware of, and also highlight the possible knock-on effects to other parts of the infrastructure. The groups also discussed mitigation options to deal with these issues.

The information from the focus group meetings has been passed to the LRF risk sub-group to challenge the Community Risk Register and where necessary to change local risk assessments, mitigation measures and planning priorities.

Why is information sharing important?

18.11 Sharing information at all levels has numerous benefits: sound risk assessment at the national or local level relies on obtaining accurate information about the nature of hazards and their potential impacts; effective business continuity planning involves understanding links and dependencies on suppliers; and joined-up emergency planning relies on understanding partners' priorities and plans. Without information, responders will be unable to make the right judgments, from what risks to plan for to how responses might be coordinated. Sharing information will also ensure that Category 2 responders' own arrangements are fully linked with those of the wider emergency management community.

18.12 Responses to the interim review on this issue were resoundingly positive and included very strong support for a shift in the direction of sharing information. For example, in light of the floods, Water UK reported that information sharing between Category 1 responders and the industry had been an issue. It recommended that water companies *"… review the data and information available within the sector that can be securely shared amongst key stakeholders to better aid the planning and response process. Areas where data may not be available should be identified and solutions proposed to redress these gaps*."

Information sharing in law

18.13 Local authorities involved in the floods state that duties imposed on Category 2 responders under the CCA have enabled them to opt out and avoid making an appropriate contribution to the development of emergency response arrangements.

18.14 Central government guidance, as set out in *Emergency Preparedness,* states that Category 2 responders are required to share information about the performance of functions related to emergencies with Category 1 responders and other responders. It recognises that information sharing is a crucial element of civil protection work, underpinning all forms of cooperation, and goes on to state that responders should share information both formally and as part of a culture of cooperation.

18.15 Under the current framework, Category 2 responders are supposed to work on the presumption that non-disclosure is the exception rather than the norm. Evidence from the response to the 2007 floods indicates that Category 2 responders have not been putting this principle into practice effectively.

18.16 The CCA recognises that the release of some information, and of information to some audiences, may need to be controlled. We believe that this balance is not being effectively achieved. Exceptions to the disclosure of information can be made where the release of the information to the requesting responder would be prejudicial to national security or public safety, or where the information is commercially sensitive or personal. However, the regulations do make provision to protect sensitive information. As such, the receiver cannot pass on commercially sensitive or personal data without consent, even where there is a strong public interest in doing so.

18.17 Importantly, if there are repeated instances of apparent failure to comply with obligations by sharing information, ministers may use powers under Section 9 of the CCA to ask for information and explanations. **The Review would welcome, in the short term, further use of these provisions to redress the balance and drive change.**

Regulatory uncertainty

18.18 Sir Ken Knight's review of the operational response to the floods points out that providing an effective, joined-up response to major incidents that affect Category 2 assets and resources is difficult if Category 2 responders are not fully involved in the heart of planning. As things currently stand under the CCA, Category 2 responders are obliged to 'cooperate and share', a phrase which, Sir Ken Knight argues, is open to interpretation, leading to variations in the levels of engagement of Category 2 responders during both the planning and response phases. He notes that it is hard to see how responders can be 'heavily involved' in a response if they have been 'less likely to be involved' in planning and exercising.

18.19 Category 2 responders indicated that they feel they face a myriad of conflicting requirements, and that this is leading to uncertainty about what they can and cannot share. This in turn increases anxiety about the disclosure of material and discourages positive action.

18.20 Evidence to the Review identified various legal impediments to transparency. These included the common law of confidence, Competition Law, the Data Protection Act, and the Official Secrets Act. Stakeholders were aware of the existence of a multitude of legislation restricting information sharing, but did not necessarily understand the precise implications. Sectors are also subject to tailored advice, via sponsor departments and CPNI, on what constitutes a designated site and what information can be released externally. As a result, Category 2 responders tended to avoid discussing even the most minor issues for fear of breaching some part of the law.

Competing interests

18.21 In their response to the interim conclusions, Category 2 responders noted that it was not only the lack of a formalised process that led to their reluctance to share information. Security concerns were also a major issue. Western Power Distribution's submission states: *"When previously asked by local government to advise where loss of more than 100,000 customers might occur, WDP sought advice from the then DTI…[they] were advised to provide a 'footprint' showing an area affected but not to provide site location detail… the provision of such information is currently… against written advice."*

18.22 The Review recognises the legitimacy of such concerns. The potential damage that could result from releasing sensitive information too widely must be balanced against the need for Category 1 responders to get planning right. However, we believe that the events of summer 2007 highlighted that, for individuals and communities at risk from flooding and the resulting loss of essential services, the balance is currently tipped too far in favour of security

concerns. A fresh look must be taken at current provisions to enable greater transparency.

18.23 The tension between greater transparency and control of information is common in countries that share a similar risk profile to the UK. The USA, Australia and the Netherlands are three countries that have developed strategies for dealing with that tension.

National Infrastructure Protection Plan – Network approach to information sharing

In 2006, the US Department of Homeland Security (DHS) released the final version of the National Infrastructure Protection Plan (NIPP), which defines roles and responsibilities for all levels of U.S. government and private industry that must work together to secure the nation's critical infrastructure and key resources. One of the NIPP's unique features is its network approach to information sharing, which represents a fundamental shift in how security partners share and protect critical infrastructure/key resources (CI/KR) information.

Prior to the creation of the NIPP, private-sector critical infrastructure security partners used information sharing and analysis centers (ISAC) that served as mechanisms for collecting, analysing and sharing information on CI/KR threats and vulnerabilities within private infrastructure sectors and the US government.[2] However, the US government itself did not possess any comprehensive unifying networks or systems that could facilitate this kind of real-time information sharing within and between all levels of government and private sector partners for all 17 sectors.

The NIPP's network approach builds on the basic concept of these ISACs to enable secure and cross-directional information sharing between and across the US government and private sector, in order to protect key assets. It provides improved and more centralised mechanisms that support a real-time relay of strategic and tactical threat assessments, vulnerability assessments, threat warnings, situational or incident reports, lessons learned and best practices for CI/KR protection.

The network approach has been gradually gaining traction, however much work still needs to be done. Its effectiveness varies significantly across each sector. For instance, the public health and health care sector's diverse nature has made collaboration difficult, while the commercial nuclear reactors, materials and waste sectors have been successful because the grouping itself is relatively homogenous and has a long history of collaboration.

A lack of an effective relationship and trust between the DHS, other federal agencies and the private sector is another challenge to the NIPP's networked information-sharing strategy. Stakeholders frequently cite prior working relationships with federal partners as well as access to contractor resources and technical assistance through the DHS as key ingredients to establishing effective information-sharing councils within each sector.

[2] *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sector's Characteristics*. GAO, GAO-07-39 (www.gao.gov/cgi-bin/getrpt?GAO-07-39).

Australia's Trusted Information Sharing Network for Critical Infrastructure Protection

Critical-infrastructure protection has become a general label for a range of activities undertaken jointly by government and the operators of key locations, facilities and systems to ensure that they are adequately managing risk. In recognition of this, the Australian government has set up the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). The network allows members (who include national and state ambulance, police and fire services) to share security-related information in a protected environment. The TISN is not an operational network but is concerned with policy issues in a medium-to-long timeframe. Through its peak committee, TISN members have a direct line of communication to the Attorney-General and the National Counter-Terrorism Committee.

Information sharing in the Netherlands

In Holland, the private sector manages 70-80 per cent of critical infrastructure. In 2002 the Dutch government set up the Critical Infrastructure Protection project in order to prevent disruption against technical failings, overloading, extreme natural phenomena and intentional or unintentional human action.

As part of that project, the Dutch have held workshops where representatives of three or four critical infrastructure sectors met with emergency planners from regional authorities. Two scenarios were developed (pandemic flu and coastal flooding) and participants were asked to describe sector and cross-sector effects if such scenarios were to occur. To make sharing of sensitive information possible, they recognised that there were three types of information: information that could be shared with everybody (green); information that could be shared in a previously defined professional group (orange); and information that would only be shared with the participants of the meeting (red). All participants were asked to sign a confidentiality agreement in which they promised to keep red information confidential. The classification of information was also used to ensure that the reports of the workshops were produced in such a way that confidentiality was respected. The reports are now available to other critical infrastructure operators and government.

Another initiative used in the Netherlands has been the National Advisory Centre for Critical Infrastructure (NAVI), which is a public–private network between government and critical-infrastructure operators who are able to share information on threats, risks and vulnerabilities. They use a similar colour-coding system for defining the level of confidentiality. Information can be shared via face-to-face contact, but also through closed websites.

One of the major gains of the operation has been decompartmentalisation, as sectors have begun entering into dialogues among themselves and are better informed about each other's possibilities and needs. Consequently, they are even more aware of their own vulnerabilities and those in the sectors that are dependent on them. As a result, preparedness measures have been aligned more effectively. The Minister of the Interior in the Netherlands believes that the benefit of the project has been that *"a network has emerged where individuals from the public as well as the private sector know where to find each other".* Everyone involved in it regards this informal network as highly valuable.[3]

[3] Remkes, Report on critical infrastructure, 2005.

The public domain

18.24 Many Category 2 responders see the sharing of information with their Category 1 counterparts as analogous with putting it in the public domain. In the water sector, for example, companies are restrained by a Security Service Advisory Note that aims to ensure that information placed in the public domain does not compromise the security of the water company. Such information includes emergency plans. Legal advice to the Review indicates that, unless such advice is withdrawn or amended, water companies will be very wary of going against it.

18.25 Submissions to the Review point out that local responders are not widely security-cleared. Local authorities do not receive sensitive information from Government and local authority emergency planning officers do not generally have security clearance. Although this is changing, particularly in London, this privilege still does not apply to all officers or to local authority chief executives.[4]

18.26 All of this raises the question of why Category 1 responders, who have been entrusted with responsibility for leading civil protection work, are not equally trusted when it comes to accessing information that will allow them to perform that role effectively. **We would welcome Government driving change, moving away from 'need to know' towards 'need to share'.** If necessary, this could include putting all emergency planners in local authorities through security clearance. Some LRFs we spoke to had chosen to take this path, security clearing all of their emergency planning staff, and found that this avoided such serious problems in terms of being trusted with sensitive information. However, this process had been both time consuming and costly.

The risks of relying on generic assumptions

18.27 Evidence from Category 2 responders indicates that there are times when they fail to see the benefit of giving responders prior knowledge of risks that affect their infrastructure. They argue that generic planning assumptions are sufficient, and should encompass all the scenarios that local responders need to plan for.

18.28 However, Cabinet Office advice is clear that while generic assumptions are designed to inform emergency planning and policy formulation, they do not remove the need for LRFs to make judgements about area-specific key hazards and their consequences. These judgements will then form the basis for their Community Risk Registers.

18.29 Before the events of summer 2007, Category 1 responders were not aware that Mythe water treatment works was a potential single point of failure and that the consequences of losing it would be so significant and far-reaching. Generic assumptions would not have allowed responders to sufficiently plan for such an event.

18.30 While providing information on which assets are susceptible to flooding goes some of the way, it does not go far enough. Planners will be unable to prioritise sites and identify appropriate, adequate contingencies without an understanding of which sites are considered to be critical and which are not.

Developing national guidance

18.31 We believe that, without such information, it will not be possible to ensure an adequate emergency response to any civil emergency. At present, there are too many obstacles to sharing information. What is more, there appears to be little consistency both in terms of the type of information which Category 2 responders will and will not share and within individual organisations, where different actors seem to apply variable degrees of stringency on sharing. This leads the Review to conclude that companies are free to share (or not to share) pretty much as they choose.

[4] C Walker and J Broderick, *The Civil Contingencies Act: Risk, Resilience and Law in the UK*, p. 258

Information sharing in Yorkshire and the Humber

Following the 2007 floods, the Government Office for Yorkshire and the Humber (GOYH) undertook a study to gauge how effectively Category 1 and 2 responders in the region were liaising with each other. Findings highlighted the reluctance of Category 2 responders to share information with other responders due to both commercial and security concerns.

Levels of transparency varied greatly between organisations, as did expectations regarding information sharing. The study also showed that LRFs operated differently across the region and, by extension, across the country, suggesting that responders have varied expectations in terms of interaction and cooperation. This is a cause of confusion and concern for Category 2 responders dealing with multiple LRFs.

Some Category 2 responders are working to identify the risks they face and find ways of sharing that information. The GOYH believes that more should be done to work out how this information can best be integrated into emergency planning and risk assessment processes and how sensitive information can be given adequate protection. The study concludes that more work is required at all levels to build relationships between partners, including the security services and central government, with a view to developing robust protocols for information sharing.

18.32 While we recognise that there will always be security concerns over making information on critical infrastructure sites too readily available, the experiences of summer 2007 suggest that a better balance needs to be struck between security and information sharing in order to improve preparedness and, therefore, ability to protect the public at all levels. The Review believes there is no reason why information relating to the vulnerability and risks to infrastructure should not be shared with emergency planners as quickly as possible. This should be an ongoing process as risks are dynamic and assets change over time.

18.33 In the short term, the Review would welcome clearer guidance at the national level to raise awareness of this issue and set out what Category 2 responders are expected to do under the CCA. Such guidance should, as far as reasonably practicable, define exactly what should and should not be shared and what information Category 1 responders can reasonably ask for. In the longer term, we believe the CCA needs to be revisited and information sharing obligations strengthened to ensure compliance.

From 'need to know' to 'need to share'

18.34 Experience shows that the impact of natural disasters (such as floods) on critical infrastructure can be as big – or even bigger – than that of a security threat. In summer 2007, many tens of thousands of people were left without water and electricity, and hundreds of assets were flooded. Forward planning for such an event is impossible without information. Responders cannot legitimately be expected to identify what is critical without improved input from Category 2 responders. Greater willingness to share will also lead to greater cooperation, as individuals and agencies start to form effective working relationships and learn more about each others' roles.

18.35 The CCA states that: *'In most instances, information will pass freely between Category 1 and 2 responders, as part of a more general process of dialogue and cooperation. This is the means by which the overwhelming majority of information sharing should happen…if this is not the case, it is probably evidence of a wider systematic failing in the way the Act is operating.'*[5] The events of summer 2007 show that, in practice, neither the culture of cooperation nor the obligation to formally contribute information has flourished.

18.36 The interim report argued that the Civil Contingencies Act should be extended

[5] CCA, Emergency Preparedness Guidance, p.25, 3.7

to require Category 2 responders to engage more fully by formally contributing information on critical sites, their vulnerability and the impact of their loss. **Where problems are being experienced, we would welcome an increase in the use of the protection of information provisions within the CCA.**

18.37 We recognise that changes to the CCA will not improve the sharing of information by themselves. The problem is as much cultural as it is legal. The challenge for government is to reconcile legitimate but competing objectives: the need for security and the need for information sharing to enable planning and preparation. Government must rethink, with the public interest at heart, the balance between security restrictions on information sharing and the need for access to such information.

18.38 In order to develop clear and consistent guidelines, lead government departments should work together to develop guidance that clearly specifies what information can and cannot be released about critical infrastructure sites. Such guidance will also help to ensure that responders across the country have access to similar levels of information, that Community Risk Registers better reflect risks to critical infrastructure from flooding and other hazards and that the implications of both single points of failure and the complete loss of an asset are explicitly considered in all risk assessment and contingency planning undertaken by responders. Clearly defined information sharing protocols must be developed and new information sharing networks established as necessary to enable the level of sharing intended by the CCA.

RECOMMENDATION 55: The Government should strengthen and enforce the duty on Category 2 responders to share information on the risks to their infrastructure assets, enabling more effective emergency planning within Local Resilience Forums.

Local-level engagement for more effective emergency response

18.39 Category 2 responders are the experts when it comes to their assets, and the risks those assets face in both day-to-day and exceptional circumstances but Category 1 responders are the experts when it comes to managing wider civil emergencies. It is in the interests of those who suffered a loss of essential services during the summer and everyone who may be at risk from such events in the future for these areas of expertise to be combined effectively. Experience has shown that preventing and preparing for civil emergencies requires the active participation of appropriate responders. This in turn requires meaningful engagement between Category 1 and 2 responders. The CCA recognises the role both Category 1 and 2 responders have to play in the planning, preparation and response to an emergency and requires organisations to work together towards greater system resilience.

Multi-agency working in summer 2007

18.40 Evidence from the summer suggests that Category 2 involvement in multi-agency emergency response exercises has been patchy. As a result, the integration of Category 2 responders into Gold Commands set up over the summer was initially slow. Feedback from Category 2 responders who attended Gold Commands indicated that they were often unfamiliar with the Gold Command structure, and as a result arrived without any clear idea of what to expect.

18.41 The EFRA Select Committee found that councils were critical of the performance of Category 2 responders during the floods. Sheffield City Council claimed that the floods highlighted significant issues in relation to the engagement of Category 2 electricity and gas utilities in planned exercises, stating that the utilities had 'not been round the table' and were not even 'entirely equipped to be round the table.'[6]

[6] EFRA Committee, Fifth Report of Session 2007-08, Volume 1, 94.

18.42 Severn Trent Water admitted that it had not previously taken part in a multi-agency exercise simulating an event of the summer's floods. As such, they were initially unaware of the dynamics of the team, which had been running for the previous day and a half. Severn Trent Water may have been able to cope better in the early stages of the loss of Mythe water treatment works had they been more actively involved in multi-agency planning and had both the company and its partners been better informed about local circumstances and infrastructure. The company has responded positively to its experience by ensuring that all relevant staff receive appropriate training to allow them to integrate successfully into the structure.

18.43 The experiences of Gold Command in Gloucester proved that giving team members the opportunity to get to know each other before an emergency arises speeds up multi-agency working when an incident does occur. Stakeholder evidence has supported such diagnoses, Water UK concludes that water companies should rehearse emergency plans on a regular basis and that such rehearsals should include the local emergency response organisations. In addition, training such as the 'Gold Standard' course provided by the Government's Emergency Planning College can help ensure that responders know what to expect before attending an actual Command.

Current approach to planning and response

18.44 The Civil Contingencies Act places the primary duties for response planning for events in the local domain. The intention of the Act was that Category 2 responders, defined as entities that perform 'functions vital to the life of the community' or are 'key parts of the local infrastructure which maintain the life of the community', play a part in civil protection at local level by responding to reasonable requests and adhering to principles of effective representation.

Anglian Water and Lincolnshire LRF

Lincolnshire's LRF welcomes Category 2 attendees to its meetings and consistently aims to reinforce its links with the emergency planning community.

Being part of numerous LRF sub-groups and exercises has enabled key Anglian Water staff to build relationships and work effectively with other agencies' representatives. As a result, those agencies now have a greater awareness of the water company and its role, something which proved to be of great benefit during the floods when Anglian Water was able to provide technical advice on aspects of the incident relating to sewage flooding. Often, a representative from Anglian Water was the only Category 2 attendee; those staff attending Silver Command reported significant benefits in terms of their ability to respond.

As a result, Anglian Water now attends other multi-agency commands in person, wherever they are established. Although this can seem costly in terms of time, allocating the resources to regularly attend LRF meetings and build up working relationships can pay huge dividends in the event of an emergency event. Key Anglian Water staff are now being put through training to enable them to represent the company more effectively.

18.45 The events of summer 2007 have led people to question whether this is happening successfully in practice. Sir Ken Knight's report states: *"An initial survey of five of the worst affected areas, and subsequent wider consultation showed that the problem of Category 2 engagement in both planning and response was experienced at different levels in many areas."*[7] It goes on to say: *"of thirteen organisations that responded to CFRA's Emerging Issues Report, 12 agreed that the involvement of Category 2 responders needed to improve. One response said that their local arrangements were working well."*[8]

[7] K Knight, *Facing the Challenge*, p.86.
[8] Ibid.

EDF Energy and the North Sea tidal surge

In November 2007 a tidal surge coincided with high tides along the Norfolk and Suffolk coasts, giving rise to an early warning of coastal flooding. EDF Energy sent senior management to both the Norfolk and Suffolk Gold Commands. Contact was also made with Kent and Essex, but the lower level of risk meant there was no need for the company to attend in person although it was important to keep the channels of communication open.

Based on the importance of one site in Great Yarmouth, Norfolk Gold Command decided to ask the Environment Agency to send temporary flood barriers to the site to supplement existing measures. Effective Silver and Bronze coordination between EDF staff, the Agency and fire service ensured the barriers were successfully deployed before the morning high tide. Thankfully, severe flooding was avoided and the defences were not put to the test, but the event demonstrated that an effective response can be mounted when proactive multi-agency working is initiated in good time.

18.46 When the CCA was devised, Category 2 responders, and in particular utilities which are often nationally based, feared the practical and financial difficulties associated with the obligation to undertake planning and response on a local level. They would have preferred a greater emphasis on regional and national planning forums.[9]

18.47 This preference persists, as highlighted in a report by the Electricity Networks Association. *'Electricity Network Owners are fully engaged with Resilience Forums although, because Network Owners span many LRFs, this engagement is necessarily with Regional Resilience and Utilities Sub Groups who can respond to requests from Category 1 responders.'*

18.48 The interim report concluded that Category 2 responders should be required to participate fully at Gold and Silver Commands and that this should be delivered through a revision to the CCA or other regulatory regimes. Numerous submissions indicated that, due to the size and scope of some Category 2 responders, a mandatory requirement for all such responders to attend all exercises would be impossible. For example, the electricity sector includes transmission and distribution, water includes waste and clean water, and in both sectors communications are provided by numerous actors. Responders also noted that providing an appropriate officer, that is one who both understands fully the utility's obligations and capabilities and is empowered to interact with the Command and take binding decisions, is a challenge given that such skills will also be in high demand for the direct management of the incident. By extension, having to find more than one such officer to resource multiple events across the utility's area could well prove beyond many organisations' capabilities.

18.49 Whilst recognising the validity of such concerns, the Review agrees in principle with the idea that emergency response should be managed at the local level and sees merit in LRFs acting to consider how best to accommodate and communicate with numerous providers. We note that some regions have managed to streamline engagement in planning by setting up regional utilities engagement forums, enabling generic issues to be dealt with at a higher level. While such groups are invaluable for the reasons described below, responders felt that they were just one half of the picture, almost unanimously stating that relationships and information sharing which the latter engender could not be developed via a Utilities Group alone.

[9] C Walker and J Broderick, *The Civil Contingencies Act: Risk, Resilience and Law in the UK*, p.89

North West Regional Utilities Resilience Forum

The North West Regional Utilities Resilience Forum was created in September 2004. It meets 3-4 times a year to improve understanding, cooperation and coordination between regional Category 2 Utility responders themselves and between that group and LRF/Regional Category 1 responders. Representation includes electricity and gas suppliers and distributors, telecommunications companies (mobile, cable and landline) and the regional multi-utility companies (electricity, water and sewerage services). Representatives of four of the six LRF attend regularly. The Government Office participates and provides the secretariat.

Benefits of the forum include:

- networks of trusted relationships between Category 1 & 2 responders;
- Category 1 awareness of national, regional & sub-regional utility roles and boundaries;
- publication of lay guide to Category 2 Responders' duties & roles;
- presentations and discussions on infrastructure issues and interdependencies;
- verbal briefings on sensitive exposures (e.g. single points of failure);
- joint awareness of contingency plans, resources and sector mutual aid schemes;
- 24/7 contact arrangements between members; and
- development of members' resources to support needs.

The London model was mentioned by more than one responder as providing a good framework which could be adopted nationally.

The London model

In London, utilities companies engage with responders at a regional level. Representatives from the telecommunications, energy and water sectors and the London Resilience Team meet quarterly as the Utilities Sectors Panel.

Through this mechanism, utilities are involved in planning, exercising and awareness raising events. Meetings also serve to enhance communication between utilities, ensuring greater understanding of interdependencies and familiarity with each other's emergency planning and response mechanisms.

'The strength of the arrangement was evident to me on 7.7.05. When the crisis started, the group rapidly came together to support each other whilst our representatives convened at Gold. The benefits of a well developed working relationship were quickly evident in the mutual support and joined up working and information sharing.' EDF Energy, Emergency Planning and BC Manager

Lack of consistency

18.50 Evidence to the Review highlighted large inconsistencies in the approaches taken by LRFs to engaging Category 2 staff. In their submissions, Category 1 responders pointed out that individuals in some Category 2 responder organisations had been given emergency planning as an add-on to their core role. They felt that inadequate resources were being assigned to local engagement by national infrastructure operators. A number of Category 2 responders agreed that attendance at meetings should be mandatory, acknowledging that civil contingency planning would otherwise not get the level of attention or resource necessary from their organisations.

18.51 The Review considers that LRFs, if necessary acting together at regional level, should consider and agree with their Category 2 responders how they should engage with each other for planning and response purposes. Government should not leave this entirely to local discretion but facilitate debate. We also believe that there is a need for a national focal point for each sector and that this should support discussions around the development of the Sector Resilience Plans (as set out in Chapter 14).

Lack of awareness of capabilities and dependencies

18.52 The Business Continuity Institute's submission to the review indicates that a number of businesses acknowledged that their plans had not taken into account reliance on other service providers. This appears to be due to a lack of awareness and understanding of what they could expect in terms of reconnection from energy companies. These findings, along with other stakeholder evidence, lead the Review to conclude that it was not only responders who had a limited understanding of the vulnerabilities of the utilities and their own dependency on supply.

18.53 The Review believes that greater engagement at local level will lead to better understanding of what utilities can and cannot provide. This will in turn lead to greater clarity as to what communities and businesses should be planning for. It is impossible for communities and local businesses to prepare themselves if they are kept in the dark over the potential for failures.

National guidance

18.54 Civil protection is a multi-agency activity. Responders must work together and develop a good understanding of each other's capabilities and vulnerabilities if they are to be effective. Submissions to the Review almost unanimously recognise that the events of summer 2007 highlighted shortcomings in the current arrangements.

18.55 The Water UK review states: *'The experiences during summer 2007 showed a patchy and inconsistent picture in the level and timing of involvement…the degree of participation of water companies ranged from none to full. The points at which water companies were invited to attend also varied…once a water company was directly incorporated into the emergency command structure and reported to the command leader then both communications, understanding of needs, and decision-making improved rapidly… participation in and training with LRFs will allow the development of working relationships...that will have benefits in the event of an emergency.'* It concludes that: '*Water companies should ensure they are appropriately involved with key agencies in planning, training and rehearsing for critical incidents.'*

18.56 Evidence has shown that, as things stand, the quality and extent of engagement in a local area is too dependent on the individual character of the LRF and the awareness level of the Category 2 responder. Some Category 2 responders are not even aware of their own status. It is reassuring to hear that a number of Category 2 responders are reviewing how they interact with LRFs and Gold Commands and putting their senior management through training in civil emergency planning and response. This approach must now be adopted across the board.

18.57 The Review would welcome an awareness raising exercise, conducted by government, to increase understanding of responsibilities under the CCA, remove the uncertainties around engagement and deliver a clear message on expectations of engagement.

18.58 Sectors have begun entering into dialogues amongst themselves, and are consequently better informed about each other's vulnerabilities and dependencies. The next step must be to adopt this approach both between sectors and across the public/private sector divide. While recognising the difficulties this presents, especially for organisations with a national footprint, we believe such engagement is essential.

18.59 There are good models of how this engagement can be streamlined to work effectively. However, the Government should provide additional guidance on the expected levels of engagement, increase awareness of these duties and also carry out enforcement actions to ensure the Act is complied with.

RECOMMENDATION 56: The Government should issue clear guidance on expected levels of Category 2 responders' engagement in planning, exercising and response and consider the case for strengthening enforcement arrangements.

18.60 The Government should issue this guidance and distribute it to the regulators, who should then act to inform every organisation within their sectors of their duties under the CCA. As the level of engagement increases, enforcement action should be considered more seriously where responders are failing to comply with engagement obligations.

Effective management of dams and reservoirs

This chapter considers dam and reservoir safety and makes recommendations as to how it could be improved. It contains sections on:

- balancing the needs of security and safety;
- the nature of the risks of dam failure;
- reservoir flood plans;
- achieving a risk-based approach;
- a new legislative framework for reservoir safety; and
- succession in the civil engineering profession.

Introduction

19.1 The events which occurred at Ulley reservoir, Rotherham, in summer 2007 highlight the potential risks facing communities living in dam inundation areas. While emergency responders were repairing damage to the reservoir caused by excessive flows down its spillway, around 1,000 people were evacuated and main roads (including the M1) were closed. In the absence of contingency plans because of the restrictions on the sharing of information, responders had to improvise during the event by drawing flood maps and making evacuation plans on the spot. The evacuation took place in the early hours of the morning and people who were evacuated at short notice had no knowledge of the risks. Had the incident happened in a more densely populated area or with less time, it is doubtful if this improvised approach would have been adequate. Although the incident at Ulley reservoir gives cause for concern, other reservoirs overtopped during the course of the summer, albeit without such serious damage.

Balancing the needs of security and safety

19.2 There is an unresolved dilemma in our current attitude to reservoir safety. This arises from the vulnerability of reservoirs to both malicious attack and to natural failure. The former has resulted in an insistence on secrecy about the area that would be flooded from a dam breach, so as not to give information to would-be attackers; but this has meant that we cannot be as ready to respond as we should be, whether a breach occurs because of attack or natural failure and this puts lives unnecessarily at risk. Emergency planners and responders do not have the information they need and the public are not aware of the risks to plan effectively.

19.3 Thus, while we try to reduce the risk of one cause of dam breach, the trade off in doing so is that we increase the risks to life and property arising from all causes. The balance between security concerns to reduce risks of attack and planning to save lives in the

Ariel view of Ulley Reservoir after heavy rain © Empics

event of a dam breach has not been properly addressed. Secrecy leaves us in the curious position that there is a strong chance that we now defeat our own ends. This contrasts with the situation in other countries which also face a similar threat of malicious attack. France and the USA for example are more open about providing information to the public to help save lives in the event of a breach. Below we give a best practice example of the kind of information made available in another country, Switzerland (Lake Sihl).

19.4 The Government needs to urgently resolve the dilemma in its attitude to reservoir safety. We believe that the current approach to security concerns is misguided: we explain below that the issue is about security of the reservoir site, not having knowledge of where flooding would occur if a reservoir were to breach, since anyone with an Ordnance Survey map and purpose can work that out. There is good work going on to improve reservoir safety and emergency planning but it is, worryingly, hampered by security restrictions on sharing of information on impacts and flood zones.

The nature of the risks of dam failure

19.5 The likelihood of breaches is remote: there has been no dam failure in this country since the 1920s. But the consequences are potentially catastrophic. We do have large reservoirs near to built up areas. “Near” does not mean within view: the area in which buildings would be destroyed can be several kilometres from the dam itself. By “destroyed” we mean just that. The best way to describe it is as similar to the Boscastle flood of 2004, when the power of the deluge destroyed

Boscastle, 2004.

buildings and cars without, miraculously on that occasion, killing anyone. That is the force that we could expect to see unleashed if a dam were to breach. But in an urban area, below a very large reservoir, the consequences would be very much greater.

19.6 The conditions following a major dam breach are much more severe than normal flood flows. The effect of catastrophic dam failure is to create a high speed wall of water that sweeps along debris and rubble, killing people and with the energy to destroy buildings and other infrastructure in its path.

19.7 The photograph below is taken from an incident in Sweden a few years ago, which is included to show the potential impact of a dam breach.

19.8 People are at risk if they are within the inundation zone. The impacts are greatest for people and property immediately downstream. The speed of flow and extent of the immediate area will depend on a number of factors including topography. For example, if a downstream valley is confined and narrow for great distances the area of immediate impact will be some distance from the reservoir. Although there may be cases where some notice is possible, this may not always be the case. A quick and effective warning and emergency response is necessary to save lives in the event of a dam breach. However, this is not enough; people also need to know in advance how to respond to warnings for example by knowing what evacuation routes to take. The importance of this was dramatically underlined for us during a site visit, where we saw from the inundation map that a school lay directly downstream of the reservoir, in the path of what would be the inundation flow.

Scale of the risk

19.9 In the last 200 years there have been 14 dam failures that resulted in the deaths of 465 people across the UK. However, there were 10 dam failures that did not cause loss of life between 1960 and 1971. Various serious incidents have occurred since then but fortunately these have not resulted in dam failures.

Breach of Noppikoski Dam, Sweden, 1985

19.10 In England and Wales there are over 2000 reservoirs (Large Raised Reservoirs – LRRs) covered by the Reservoirs Act, of which 956 are currently categorised as posing a risk to life if they breach. Figures from the Environment Agency reveal that in England and Wales there are at least six emergency draw downs of reservoirs each year. These are instances where draining a reservoir is the last resort to prevent dam failure.

19.11 The Chair of the British Dam Society (BDS) has provided the Review with a statistical comparison using data on Large Dams from across the world. This suggests a catastrophic failure leading to loss of life at a rate of around one every 45 years on average in the UK. Whilst this figure must be treated with caution – it does not reflect differences in construction standards or dam size – the Chair of BDS concludes that *"there is no obvious reason to assume that UK dams are significantly safer than [Large Dams worldwide]".* A report to the Government *("Climate Change Impacts on the Safety of British Reservoirs"* Defra 2002) indicates that risks of failure will increase as a result of climate change reducing safety factors by 20 per cent because of increased subsidence of embankments in summer droughts, stronger winds causing more wave activity and more severe rainfall events leading to greater overspills. At the same time, climate change will create a need for new reservoirs particularly in the densely populated South East, where there are also strong pressures to develop.

19.12 We have been able to obtain a limited number of inundation maps to try and understand the scale of risk that we face from potential dam breach. This data is not currently publicly available and covers less than 10 per cent of the England and Wales stock of LRRs. Our analysis has focused on reservoirs whose inundation areas include major urban centres. The analysis suggests that the overall risks are extremely serious.

19.13 The analysis included some reservoirs with overlapping inundation zones. This shows that, within the total combined inundation zones, the night time populations at risk total nearly 350,000 people (day time populations are higher at over 430,000 people). In addition, although available information on infrastructure is incomplete, there are for example over 40 sites belonging to the emergency services, nearly 80 educational establishments, including schools and three items of Critical National Infrastructure. It is clear from this that the consequences of reservoir breaches present significant risks to people and property. These figures can be scaled up by a factor of 10 to gain an indication of the total risks in England and Wales alone.

19.14 While we have not been able to do this analysis for inundation maps for Small Raised Reservoirs (SRRs), those maps we have seen indicate that people, property and infrastructure could be at risk. As such, we support the proposal of the Environment Agency in its biennial report that the Reservoirs Act should be amended to provide better, risk-based, criteria for inclusion in its controls. The implications of this are discussed further below.

Reservoir flood plans

19.15 The Government is making progress towards introducing flood plans for LRRs. The Water Act 2003 amended the Reservoirs Act allowing ministers to direct reservoir undertakers to prepare a flood plan setting out how they would control or mitigate the effects of flooding likely to result from the escape of water from a reservoir. The aim, to ensure that the correct emergency procedures are in place to deal with any breach, is clear and correct. A flood plan comprises three components, which are currently under development by Defra:

- an **on-site plan** detailing the response to a potential breach to reduce the risk or extent of any uncontrolled escape of water;
- a reservoir **inundation map**, showing the area that would be affected by any escape of water; and
- a **communications plan** setting out how the undertaker and local emergency services should communicate with each other.

19.16 Local Resilience Forums (LRF) would draw up an off-site contingency plan based on the reservoir inundation map.

19.17 Some of this work is already in place: a number of water companies have drawn up reservoir inundation maps, and some LRFs have prepared off-site plans. In 2007, Defra asked water companies to be ready to share their plans with LRFs. Defra also plans to hold a public consultation on the direction under the Water Act 2003. Finally, Defra is working with contractors on a pilot methodology for producing inundation maps to meet LRFs' contingency planning needs, including evacuation. The aim is to provide a generic methodology for identification of any raised body of water and the possible inundation areas in the event of a breach. But restrictions still control the extent to which detailed information is released to emergency planners and, in particular, to organisations such as other utility companies.

LRF planning

19.18 In our view, the LRF is best placed to assess the risks, as it is the only body with access to information on populations and property, including that which may be at risk underground, in the inundation area. We therefore consider that LRFs should have access to inundation maps for all LRRs. They should then carry out risk assessments and inform the Environment Agency and the undertaker of the result. This will enable the inspecting engineer to judge the priority that should be attached to any works recommended in the interests of safety.

19.19 The importance of good inundation maps was brought out in the post-incident report on the Ulley incident which said: *"estimates of downstream areas likely to be affected had to be assessed fairly crudely by those on site and then passed to Gold Command in case evacuation had to be called for. In the absence of definitive mapping, estimates had to be conservative."*

19.20 Inundation maps should also be made available to development planners. We have seen evidence of one case (Benfield Hazard Research Centre Technical Paper 1 "The Dams and Reservoirs Problem") where residential development had been allowed in the inundation zone of a reservoir without any inundation map or contingency plan being available at the time. This cannot be an isolated case. We consider that PPS 25 should be made explicit on the need to take into account risks from reservoirs. In particular, any developments leading to a change in a reservoir's risk category must be communicated to the undertaker, who may in turn need to carry out an inspection to assess whether work, such as the enlarging of spillways, is needed to ensure the future safety of the reservoir. The Government should make clear how such works should be funded.

19.21 Responses from water companies suggest that they broadly agree with the approach set out above, subject to concerns about putting information on critical assets into the public domain and sharing it with other Category 2 responders. Similarly, infrastructure operators such as the National Grid support the introduction of inundation maps and are keen to have access to them. The LGA is concerned about funding for off-site planning, the adequacy of some undertakers' resources and the need for good practice guidance (preferably with statutory force). The Association is also concerned about access to inundation maps and, in particular, about Defra's timescale for making them nationally available.

19.22 Defra's inundation map pilot should also bring another benefit if extended to include the identification of SRRs. Although the full range of controls under the Reservoirs Act cannot be applied to these reservoirs, there is no reason why LRFs should not carry out risk assessments on them based on inundation maps. LRFs can then assess the risks across the spectrum and put in place contingency planning as necessary. Ahead of the proposed Floods and Water Bill, we consider that the Government should also explore whether a suitable legislative vehicle is already available

to introduce legislation to require undertakers of all SRRs to cooperate with LRFs in preparing contingency plans.

Engaging the public

19.23 The Review considers it essential that LRFs engage fully with downstream communities in relevant emergency planning. This would bring the UK into line with other parts of the world, where evidence suggests that involving the community in local planning increases awareness and lessens the risk of fatalities and damage. This should include identification for the public of evacuation routes and procedures for the public to follow, particularly where the main impacts of potential destruction of buildings and loss of life would be felt. See Figure 14.

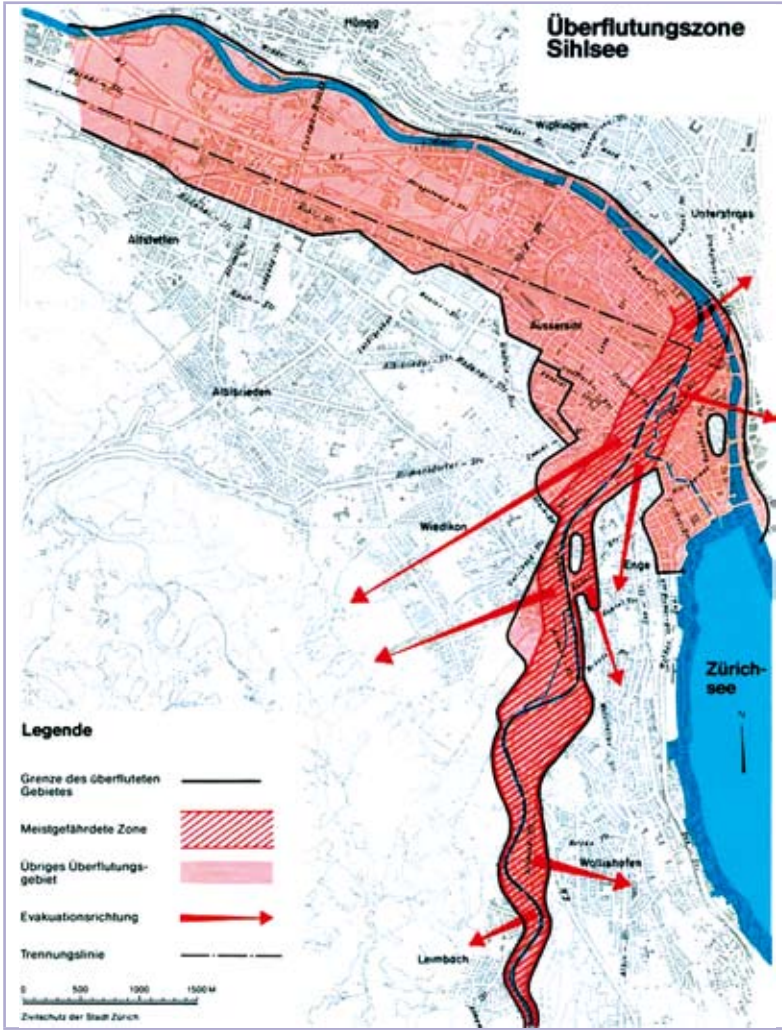
19.24 The main weakness of current restrictions on the release of information is illustrated by the fact that anyone can prepare this information for themselves with just an OS map. This is not to dismiss security concerns, but to place them in their proper context. In our view, risks arise not from knowing the location of reservoirs but from having access to sites and, more importantly, knowledge of how to cause sufficient damage to create a breach. We agree with Professor Hughes' evidence to the Review that *"it is quite obvious just by looking at a map which dams have the highest consequence of failure. Keeping information from people will cost lives rather than save lives and the Government could be criticised in this event."* We also note that the Floods Directive will require the preparation and publication of flood risk maps and plans.

19.25 Evidence to the Review is that the key to stopping any potential threat would be to make tunnels and galleries, valve houses and gate areas secure and limit vehicular access to the crest and spillway areas of dams. Frequent surveillance with associated CCTV coverage would be an essential element of maintaining security. We believe that more emphasis should be placed on on-site security measures and preparedness instead of restrictions on inundation maps.

RECOMMENDATION 57: The Government should provide Local Resilience Forums with the inundation maps for both large and small reservoirs to enable them to assess risks and plan for contingency, warning and evacuation and the outline maps be made available to the public online as part of wider flood risk information.

19.26 For both LRRs and SRRs, the aim should be to identify those where any breach would have the most serious consequences, supporting a risk-based approach to reservoir management and contingency planning. We consider this to be the only feasible approach. Nevertheless, we consider that the Government should look at whether the current categorisation is adequate and, in particular, at whether more detailed mapping is needed in some cases.

Figure 14 – Lake Sihl flood alert system



Lake Sihl flood alert system

If the dams across Lake Sihl failed, the areas of the city shown pink on the map could end up under 8 metres of water in some areas within 2 hours.

Alert signal – a wailing siren sounding for 1 minute; plus local radio broadcast. **Practice alert** each year to test sirens

Immediate evacuation from the red hatched area in directions indicated by arrows

People in the **pink (unhatched)** zone to move to higher floors.

Other measures: check that no-one has been left behind when evacuating; close shutters and turn off gas and water taps and electrical appliances; help elderly and infirm and those who are unwell.

Follow instructions from the police and the authorities closely.

Achieving a risk-based approach

19.27 The Environment Agency has also proposed a number of other changes to the Reservoirs Act. These are summarised here.

Funded powers to act at reservoirs with no owner

19.28 This refers for example to those cases where ownership cannot be determined or no undertaker identified (the latter being anyone who has an undertaking at and actively uses the reservoir). Although the Reservoirs Act grants the Environment Agency reserve and emergency powers, these do not enable it to act as an undertaker in all respects, for example in operating the reservoir. Also, the question of funding is obviously important if the Agency is to be able to use these powers effectively in the event that works in the interests of safety cannot wait until ownership issues are resolved. We consider that Defra should address this issue urgently.

Mandatory post-incident reporting

19.29 The Environment Agency has instituted a voluntary post-incident reporting system, with mixed results. The aim is to ensure that undertakers and engineers can benefit from the experiences of others and to enable the Agency to identify problem areas. For example, the Ulley incident and other earlier incidents highlighted the importance of remedial works to limit damage to masonry spillways which may otherwise be undermined by high, turbulent flows, leading to the erosion of dam embankments. We consider that anonymous reporting and information sharing is an important component in risk awareness. A voluntary system does not provide for this comprehensively and a mandatory route should be instituted.

Better quality of inspection reports

19.30 The Reservoirs Act calls for reports to be written by inspecting engineers, but is silent on the subject of how the quality of those reports might be assured. Inspecting engineers are appointed for a period of five years, subject to advice from the Institution of Civil Engineers (ICE). The role of inspecting engineers does require them to assess the need for new work, for example on spillways, and to supervise that work. We therefore consider that ICE should look to introduce a system of quality assurance for reservoir inspections, although we do not consider this should necessarily be mandatory within any amending legislation.

Better regulation of canals and disused mine and quarry tips

19.31 The Environment Agency's biennial report also called for extension of controls to canals and disused mine and quarry tips. Although these are not always the same types of structures, there is potential for them to create risks. However, we note that progress is already being made towards putting safety concerns on a firmer statutory footing and we do not therefore think that these sectors need to be brought within the Reservoirs Act.

Canals and other inland waterways

19.32 British Waterways (BW) has statutory responsibility for the canal network and maintains a risk-based system of asset management. This has recently been updated in accordance with its Asset Inspection Procedure (AIP) 2008, a comprehensive asset inspection and prioritised improvement programme. A recent review by BW, the Agency, plus an independent engineer concluded that BW's current regime is a satisfactory risk-based asset management system. **We would welcome moves to recommend to ministers that the regime should be placed on a statutory footing to ensure that it is a duty on BW.** We also consider that the Government should assist BW in sharing its assessments with LRFs so that appropriate off-site planning is in place

19.33 The basis of BW's approach is to concentrate monitoring and maintenance priorities on principal (ie high consequence) embankments (those over six metres high; or 3-6 metres high for a length of 200 metres or more) and culverts, which historically have been the main source of failure. We agree with this approach. While canals are unlikely to cause flooding on the same scale as dams, they can nevertheless pose risks: on average, there are several canal breaches every year. These occur mainly in rural, sparsely populated areas. In what was an unusual and extreme recent breach on the Monmouth and Brecon canal, a flow of debris-laden water caused considerable (albeit very localised) damage.

Mine and quarry tips

19.34 'Tailings' lagoons are used for settling water-borne waste from mine and quarry workings. Here, new rules introduced at European level following an incident in Spain a few years ago provide for waste sites to be categorised according to risk and managed in accordance with statutory rules. These are discussed further below.

A new legislative framework for reservoir safety

19.35 As the evidence above shows, good progress is being made in the area of reservoir safety. There remain, however, two key areas for discussion, relating to the Environment Agency's proposal for a fully risk-based approach. One is the nature of the controls that currently apply to LRRs; the other is the lack of statutory controls on SRRs. It should be noted that, due to the lack of controls, there is no requirement for a register to be kept. Hence there is very little information available about SRRs and even their numbers are an informed guess at best.

19.36 Under current legislation, LRRs are subject to a regime of construction, supervision and inspection by engineers appointed for five-year terms by ministers. At least once every 10 years, these inspecting engineers may make recommendations for works in the interests of safety to the undertaker; in England and Wales, these recommendations will be enforced by the Environment Agency. While in many cases this system has been effective in avoiding loss of life from reservoir breaches, there is scope for improvement in a number of areas, in addition to those already mentioned above:

- inspecting engineers' reports are not made available to the Agency unless they recommend works in the interests of safety. Any report which does make such recommendations can in effect be overturned by a further inspection, thus delaying any works;
- although the legislation is not itself risk-based, as noted above inspecting engineers do categorise reservoirs according to risks to people and property and may make recommendations in the interests of safety on that basis. Nevertheless, inspections can be as long as 10 years apart in all cases. Also, again as noted above, SRRs are outside the scope of the legislation, regardless of the potential impact of any breach;
- there are no provisions relating to the competence and financial soundness of undertakers to perform safety-related duties. At the moment, anyone can own and operate a reservoir; and
- the definition of 'reservoir' is problematic. In one recent case, a blocked culvert in a causeway effectively made it a reservoir, caused it to fill with water and overtop. This led to emergency action including the evacuation of people in properties downstream. It is not clear, however, whether such a structure falls within the Act; a situation which, in the light of the possible consequences, is clearly undesirable.

19.37 We consider that all these issues should be addressed legislatively. Existing laws provide useful models. For example, the Control of Major Accident Hazards (COMAH) Regulations require sites that pose significant risks to have on-site and off-site contingency plans for any incident. The steps being taken by the Government now to develop reservoir flood plans reflect this approach. However, we consider that more should be done to minimise the risk of incidents taking place. Another possible model, the Mining Waste Directive, provides for measures, procedures and guidance to prevent or reduce as far as possible any adverse effects on the environment, and any resultant risks to human health, brought about as a result of the management of waste from the extractive industries. It requires:

Monmouth and Brecon Canal breach

- a waste management plan to be provided by operators to the satisfaction of the regulatory authority (the 'competent authority' for the purposes of the Directive) for the minimisation, treatment, recovery and disposal of extractive waste;
- a major accident prevention policy, including a safety management system and internal emergency plan, to be drawn up by the operator for those waste facilities classified as Category A under the Directive (that is, facilities containing hazardous waste or dangerous substances) or those where failure or incorrect operation could give rise to a major accident. The 'competent authority' is also required to draw up, with public participation, an external emergency plan;
- a permit to operate a waste facility for extractive waste;
- waste facilities to be managed by a competent person, and sets out requirements for the construction and management of waste facilities;
- closure and after-closure procedures to be put in place for waste facilities; and
- a financial guarantee (or equivalent) prior to commencement of operations involving the deposit/accumulation of waste in a waste facility.

19.38 Clearly, not all of these requirements are appropriate to reservoir safety; but they do provide a comprehensive system of legislative controls which, in our view, should be considered for application to reservoirs.

RECOMMENDATION 58: The Government should implement the legislative changes proposed in the Environment Agency biennial report on dam and reservoir safety through the forthcoming flooding legislation.

Succession in the civil engineering profession

19.39 Professor Hughes, in his evidence to the Review, notes a serious decline in the number of appointed supervising and inspecting engineers. At the same time, the average age of those remaining has increased and is now in the 50s. This is not to suggest any lessening in competence; but we consider that the Institution of Civil Engineers should provide leadership at this time of change, taking action to encourage more people to enter the profession in order to ensure an adequate succession.

Dams and reservoirs – a technical overview

Dams and reservoirs form an important part of our national infrastructure providing valuable functions which include water supply, hydro power generation, irrigation, navigation, canal supply, flood control and protection and amenity use. Some dams are constructed to serve one purpose whilst others are built to serve several.

Historically the main purpose of dams has been to enable people to collect and store water when it is plentiful and then use it during dry periods – and this function is likely to become more important in years to come.

The types of dams found in the UK include earthfill dams, rockfill dams and concrete dams (gravity, buttress, arch) but the most common type is earthfill which often have a central clay core, a wall of clay which forms the watertight element within the body of the dam. We have around 2,800 dams subject to reservoir legislation in the UK and perhaps as many as another 2,000 small dams not subject to reservoir legislation

The most common type of dam found in the UK is the embankment dam, some 88% are earthfill dams. The average age of dams in the UK is now over 110 years. We obviously know a lot less about the construction of our dams which were built over a 100 years ago when compared with dams built in the last 20 years. Dams must meet certain technical requirements to ensure safe, effective and economical operation and the design and construction of all dams must comply with those requirements.

Embankment dams are the most common because they are constructed of materials, either earth or rock, or a combination of both, which are plentiful in the area where the dam is to be built.

Most dams have a number of features associated with them including a spillway, outlet works and control facilities.

The outlet works and control facilities often involve a drawoff tower within the reservoir with valves and pipes which allow water to be taken for example to supply water, to draw the reservoir down to provide flood storage or to release water to the stream/river for river regulation.

The spillway is the overflow facility at the dam to prevent the reservoir becoming too full. At a concrete dam the water can be passed over part of the concrete dam but at an embankment dam it must be safely passed around the dam in a spillway, usually made of reinforced concrete.

A scour facility is often provided at the bottom of the reservoir controlled by valves which allow the reservoir to be emptied, particularly if there is an emergency.

Although the likelihood of failure is very small the consequence of the failure of some dams can be large. As a result, after failures in the 1800s and in 1925, reservoir safety legislation was developed and our current legislation is the Reservoirs Act 1975, which ensures that all dams with a capacity greater than 25,000m³ are inspected and examined frequently. All dams subject to the Act will be very carefully inspected by an Inspecting Engineer at least once every 10 years, and examined by a Supervising Engineer at least once a year. It is best practice for owners of dams, certainly in public ownership or used for water supply and where the consequence of failure is high, to provide members of their staff who would visit the dam, usually at least 3 times per week to look for signs of distress.

The likelihood of the failure of a dam is very low but as part of an emergency preparedness scheme techniques are now available to mathematically model the way in which a dam might fail and also to study how the water released would then flow down a valley below the dam. Analyses carried out to date have illustrated that the effects of the failure of a dam may stretch for many kilometres, in certain instances as many as 30-40 kilometres from a dam.

Information from inundation mapping, as it is known, enables emergency planners to see how quickly the water will move, and what damage is done. This allows the development of plans to evacuate and take people to safety. Obviously when the population is some way from a dam then that population can be warned and evacuated before the effects of the dam breach are felt.

In many countries throughout the world these inundation plans are made available to the public living in the vicinity of dams and used to develop emergency and evacuation plans, which are then given to those who might be affected. They are often rehearsed for high consequence dams – dams where the consequence of failure is high.

When inspecting a dam an Inspecting Engineer is required to assess the dam's condition and also its safety against a number of engineering 'guidance notes' and standards. An engineer will make a visual assessment of the dam and its associated features (its spillway, valve tower, tunnel, pipework etc) and look for signs of distress which might include leakages or seepages, cracking of both the dam and its associated features, evidence of movement (i.e. bulges, depressions or slips in the face of the dam), and perhaps deterioration of materials – softening, spalling, cracking, crazing etc. In addition he would carry out technical assessments of the dam's ability to withstand seismic events and flood events.

The seismic assessment is based on the type of dam and the consequence of failure and enables an engineer to decide an appropriate level of seismic analysis to adopt to be able to demonstrate the dam is safe under seismic loading. Because the UK is not a highly seismic region, very little or (more often than not) no seismic analysis is deemed necessary.

In the case of floods, an Engineering Guide suggests the 'design flood' that a dam must be able to safely withstand based on the consequence of failure. For a dam where loss of life can be foreseen the design standard becomes the 10,000 year event or the PMF, the Probable Maximum Flood, where the return period might be of the order of 30,000 or even a million years – the worst storm that could be imagined.

The system of reservoir safety in the UK has developed from the late 1800s and continues to develop. The great benefit of the UK system compared with others around the world is that it places responsibility for safety on the owner of the structure and the assessment of safety on the shoulders of an individual, the Inspecting Engineer. The UK has not followed a highly prescriptive assessment of safety based on codes of practice which would be inappropriate in some areas, but recent events have highlighted a need to move our legislation to a risk/consequence based approach.

It is considered that the UK continues to be one of the best safety regimes in the world by allowing appropriately qualified engineers, who take individual responsibility, to use their judgement and supporting information to assess reservoir safety.