Cross-sector Resilience – Phase 1 report

Report

Publication date: 16 April 2015

Civil Aviation Authority

FCA FINANCIAL CONDUCT AUTHORITY

Ofcom

ofgem Making a positive difference for energy consumers

OFWAT

ORR OFFICE OF RAIL REGULATION

About this document

The organisations comprising UKRN together provide regulatory oversight of the companies which own and operate much of the UK's national infrastructure. This infrastructure and the products and services it delivers are important, and sometimes vital, for the normal functioning of our day-to-day lives. The resilience of these infrastructures against a wide range of threats is therefore an important topic for regulators, Governments, and consumers.

This report sets out the results of the first phase of the UKRN Cross-sector Resilience project and our recommendations for further work in phase two. The project is focussed on finding ways for the regulators to tackle challenges to the resilience of UK's national infrastructure which have cross-sector implications. Most often, these shared challenges arise because multiple sectors face common threats (such as those from flooding or cyber-attack), or because of the interdependency created when the sectors rely on one another (such as the use of electricity by finance, telecoms and railway companies).

For further information on this work, please contact Ben Willis (ben.willis@ofcom.org.uk).

About UKRN

UKRN is a network formed by the UK's economic regulators:

- The Civil Aviation Authority (CAA)
- The Financial Conduct Authority (FCA) [1]
- Northern Ireland Authority for Utility Regulation (NIAUR)
- Office of Communications (Ofcom)
- Office of Gas and Electricity Markets (Ofgem)
- Water Services Regulation Authority (Ofwat)
- Office of Rail Regulation (ORR)
- The Payment Systems Regulator (PSR)

Monitor, the sector regulator for health, participates in the network and its projects as appropriate. The Water Industry Commission for Scotland (WICS) and Legal Services Board (LSB) are contributing members which generally participate in projects as observers.

Contributors to this document

- The Civil Aviation Authority (CAA)
- The Financial Conduct Authority (FCA)
- Office of Communications (Ofcom)
- Office of Gas and Electricity Markets (Ofgem)

[1] Although it has competition and consumer protection functions, the FCA is not classed by HM Government as an economic regulator

- Water Services Regulation Authority (Ofwat)
- Office of Rail Regulation (ORR)

For further information on this report contact Ben Willis, Head of Technology Intelligence at Ofcom: Ben.Willis@ofcom.org.uk

Table of contents

1. Executive Summary 4
2. Background and purpose of the UKRN's resilience work 7
3. Threats to resilience 10
4. Role of the regulators 12
5. Cross-sector resilience issues 16
6. Phase 2 work – recommendations & further options 21

1. Executive Summary

1.1. The organisations comprising UKRN together provide regulatory oversight of the companies which own and operate much of the UK's national infrastructure. This infrastructure and the products and services it delivers are important, and sometimes vital, for the normal functioning of our day-to-day lives. The resilience of these infrastructures against a wide range of threats is therefore an important topic for regulators, Government, and consumers.

1.2. The UKRN Cross-sector Resilience project is focussed on finding ways for the regulators to tackle challenges to the resilience of the UK's national infrastructure which have cross-sector implications. Most often, these shared challenges arise because multiple sectors face common threats (such as those from flooding or cyber-attack), or because of the interdependency created when the sectors rely on one another (such as the use of electricity by finance, telecoms and railway companies).

1.3. We are undertaking this project in two phases and this report sets out the results of the first of these. The objective was to provide background and context for the work that will follow in the next phase. We have investigated how resilience, and in particular cross-sector resilience, works across the different sectors represented in UKRN. This report sets out the roles and responsibilities of the various parties involved including companies, government and the regulators. It then goes on to discuss cross-sector resilience issues in more detail. Finally, we recommend work that could be undertaken during phase two to best deliver the overall objectives of the project.

Summary of findings

1.4. The split of responsibilities between relevant stakeholders for ensuring resilience varies across the sectors. Figure 1 provides a high level summary of the main elements of the role of the participating regulators in relation to resilience.

Figure 1: Summary of resilience roles

Resilience Role	CAA	FCA	Ofcom	Ofgem	Ofwat	ORR
Resilience duties?	Yes	Yes	Yes	Yes	Yes	Yes
Including cross-sector resilience?	Not explicitly, but implicit in general resilience	Not explicitly, but implicit in general resilience	Not explicitly, but implicit in general resilience	Not explicitly, but implicit in general resilience	Not explicitly, but implicit in general resilience	Not explicitly, but implicit in general resilience
Issued general rules/guidance on measures/ outcomes?	Yes	Yes – general rules & guidance	Yes – general guidance	Yes – e.g. via price control incentives	Yes – via price review	Yes – via price control
Involved in setting or agreeing specific measures or outcomes	Yes	Yes – review current practice and request changes	No – although may require changes as part of enforcement	Yes – e.g. via price control incentives	Yes – via price review. Moving to outcome based	Yes – via price control

1.5. It is clear that resilience planning is a significant issue in all the sectors and there is a large amount of existing activity underway. Government retains key responsibilities in relation to the overall national response to resilience emergencies and is the leading source of expertise on certain types of threat. Although all the regulators have duties related to resilience, the detail and maturity of these varies greatly, as does the range of powers available to discharge them. It is also clear that none of us have specific cross-sector resilience duties and the extent to which we can address this aspect under our general resilience work varies.

Recommended work in phase 2 of this project

Cross-sector resilience

1.6. We use the term cross-sector resilience here to mean the extent to which each sector regulated by a UKRN member is resilient to problems in the other sectors. The interdependence between sectors is a complex topic which has been studied extensively. Many frameworks and models exist to help understand, plan for, and reduce the risks that are presented. As regulators we recognise this is an important area and one in which we have varying roles to play within the broader public policy context set by Government.

1.7. Two of the sectors which are most often cited as providing some of the most important inputs for other sectors are energy and telecoms. In Phase 2 we are planning to look in more detail at an example of a resilience dependency between these sectors – the use of electricity by telecoms.

1.8. The resilience of mobile networks to power disruption is one particular area likely to attract increasing interest over time. We have seen people and businesses placing more and more demands and reliance on these networks, which themselves have a critical need for electricity to function.

1.9. The intention of this work is to inform any subsequent policy debate on this and similar cross-sector resilience issues. We will consider the current levels of reliance of telecoms on grid distributed power and the range and effectiveness of existing measures to limit the impact of any interruptions. We will go on to consider how the expectations of reliability might shift in the future and whether the current protection measures are likely to be sufficient. Finally we will consider what options might be available if there was a future policy decision to effect a significant change in the level of power resilience.

How can we increase collaboration in cross-sector incident planning and response?

1.10. Our initial work has suggested a number of areas where further collaboration between the UKRN regulators would be beneficial. We note that the main responsibility for resilience is with the companies investing in and operating relevant infrastructure. Our work has not focussed on whether the current resilience at this level is appropriate, as this is for the individual regulators to determine given differences in their duties and the sectors. Instead, the incident planning and response improvements below are areas in which we as regulators have the potential to improve cross-sector resilience by improved collaboration. We propose the items below for development in phase two of our work as those most likely to be of benefit.

- **Cross-regulator emergency plan (CREP)**. We will explore the benefits of introducing a regularly reviewed and exercised framework to facilitate communication and cooperation between the regulators during major incidents affecting infrastructure resilience. It would sit alongside existing mechanisms such as COBR's[2] high level crisis management, ad-hoc bilateral contact between regulators and sector-specific crisis management communication plans. The objective is to establish a more formal arrangement for direct regulator-to-regulator contact to maximise information sharing and ensure a coordinated response to major incidents with cross-sector impact.

- **Shared approach to assessing the state of regulated companies' cyber security**. Working with Government and its agencies as appropriate, we will collaborate to determine how UKRN members can best contribute to the assessment of cyber security within our sectors. Subject to any information sharing constraints being addressed, this will draw on the experience of the UKRN members that are most active in this area and will be beneficial in reducing duplication of effort and ensuring the outputs are comparable and of high quality.

- **Joint exercise coordination**. Consistently involving stakeholders from other sectors in resilience and emergency planning exercises can help to identify and better prepare for the impact of interdependencies. This work will establish a framework to ensure regulators are well informed about the range of exercises being planned and share this information with relevant stakeholders in their sectors to maximise opportunities for involvement.

1.11. We plan to publish a final phase 2 report during August 2015. This will contain detail on the work items above. We anticipate that exercise coordination can come into effect immediately following this. The cross-sector emergency plan will take some time to integrate into existing major incident plans, but we expect that regular testing would start before the end of 2015. The timing of cyber security assessment activity varies by sector, however we expect that when completed our work will be immediately beneficial to those involved in the process.

[2] Cabinet Office Briefing Rooms – Central Government's crisis management facilities which are activated during major emergencies to coordinate response and effective decision making.

2. Background and purpose of the UKRN's resilience work

2.1. The primary objective of the Cross-sector Resilience project is to identify and implement appropriate joint responses to resilience risks which are relevant across multiple sectors represented in UKRN.

Resilience in the regulated sectors

2.2. Resilience is a large and complex topic, the handling of which varies considerably across the infrastructure sectors. Resilience can be defined as the extent to which a system can maintain its normal function while suffering challenges or stress. Across the sectors covered by UKRN, the range of "normal function", in other words the useful services offered by the sectors, varies widely. The range of challenges the sectors face is also diverse, and changes over time. In situations where the challenges become so great that normal operation cannot be maintained, some services have minimum service levels that they must not fall below, but other do not. For example, in the water sector, the Security and Emergency Measures Direction (SEMD) provides for minimum service levels (10 to 20 litres of drinking water per person per day) that offer some protection to consumers against the total loss of services in order to protect public health.

2.3. The levels of resilience achieved by a sector are of great importance to a wide range of stakeholders beyond just the sector regulator. The companies providing the services, along with their customers, have the most obvious and immediate interest. Government departments and agencies will also have a broad range of interests in the performance of services across the sectors.

2.4. Each sector has a lead Government department with overall responsibility for its resilience. Other organisations will also be involved to varying degrees, such as the national Governments, Home Office, Cabinet Office, Department for Communities and Local Government (DCLG), and the Centre for the Protection of National Infrastructure (CPNI).

2.5. Most sectors have one or more groups dealing with resilience issues from planning to coordinating major incident response and recovery. These groups will typically involve a mix of Government, regulator and industry participants. In the finance sector, its complex and interconnected nature give rise to six significant groups:

- Securities Industry Business Continuity Management Group (SIBCMG)
- Retail Banks Business Continuity Group (RBBCG)
- Insurance Sector Business Continuity Group (ISBCG)
- Association of Foreign Banks (AFB)
- Cross Markets Business Continuity Group (CMBCG)
- Cross Markets Operational Resilience Group (CMORG)

2.6. The Energy Emergencies Executive Committee (E3C) has representatives from the Department of Energy and Climate Change (DECC), Ofgem, electricity and gas companies, Health and Safety Executive (HSE) and trade associations. It is responsible for the development and implementation of downstream emergency arrangements and approves and regularly exercises the National Emergency Plans (NEP) for Electricity and Gas.

2.7. The National Security and Emergency Working Group (NSEWG) is the resilience group focused on the water and sewerage sector. The group is chaired by the Department for Environment, Food and Rural Affairs (Defra) and meets every six months to discuss national security and emergency planning issues which affect the water industry.

2.8. The Sustainable Rail Programme (SRP) coordinates climate change and extreme weather resilience matters across the rail industry. ORR, along with the Department for Transport (DfT) and Transport Scotland (TS) are active participants in the SRP and influence and govern its activities.

2.9. The Electronic Communications Resilience and Response Group (EC-RRG) is an industry-led group comprising the main infrastructure-owning communications providers plus representatives from five UK Government departments, the Governments of Scotland, Wales and Northern Ireland, CPNI, and Ofcom.

2.10. In some cases, the infrastructure and services for which UKRN members provide regulatory oversight form part of the UK's Critical National Infrastructure[3] (CNI). The resilience of this infrastructure is particularly important as failure can lead to severe economic or social consequences, or loss of life. The Government leads on CNI resilience with lead Government departments responsible for identifying which assets should be classified as CNI and asset owners responsible for ensuring that they are resilient (based on advice from CPNI).

2.11. Achieving high levels of resilience can be very expensive. For many services, a certain level of resilience is expected by all customers and is therefore built in as a matter of course. Sometimes, certain customers will demand, and be willing to pay for, higher levels of resilience. In some cases, the level of resilience desired by Government, for example to properly safeguard national security, may be higher again and would lead to more expensive products than would be available in a purely commercial market.

2.12. Balancing these sorts of factors means that regulating resilience is complex. The split of responsibilities between the relevant parties varies widely between and even within sectors, depending on the exact infrastructure and service under consideration.

UKRN cross-sector resilience project

2.13. Due to the complexities set out above, the resilience arrangements in each sector are quite different. We decided early on that the UKRN was not a good vehicle for considering whether the level of resilience in each sector is currently at the appropriate level. There are many discussions about this going on already between the relevant parties in each sector, and they should continue at this sector-by-sector level. For the purposes of our work, we have assumed that the resilience arrangements and outcomes in each sector are already the correct ones, or at least if they are not, that they will be adjusted via existing mechanisms.

2.14. This work has focussed instead on the areas where joint action by the sector regulators that makeup UKRN can have an impact. We have concluded this is most likely to be the case where the resilience

[3] http://www.cpni.gov.uk/about/cni/

issues are cross-sector in nature, i.e. spanning multiple sectors represented in UKRN. In practice, this includes two main types of issue:

- **common risks** – resilience risks which may be faced by stakeholders in more than one sector. This could be due to a common threat, such as cyber-attack or severe weather events. Alternatively, it could be due to a common vulnerability, such as the use of computing systems which rely on a common software component; and

- **interdependencies between sectors** – the use of services in one sector that have been provided by another. Examples here would include the use of the rail network to transport supplies needed to maintain telecoms networks or the use of electricity to power the computers used by finance companies.

Purpose of this document

2.15. We are tackling this project in two phases. The first phase involved gathering information from all the participating regulators on resilience in their sector and then identifying gaps where further work within UKRN can offer improvements to the current levels of cross-sector resilience. This document sets out our conclusions from this first phase.

2.16. In phase two we will undertake the identified work with the objective of delivering the outcomes suggested in the recommendations section of this document.

3. Threats to resilience

3.1. Although the specific threats that face each sector differ, there are some common themes. At the highest level, threats can usually be grouped into a small number of categories such as[4]:

- human errors;
- system failures;
- natural phenomena; and
- malicious actions.

3.2. Underneath these categories, there are wide range of threats which can affect the operation of infrastructure. The list below gives some examples of those which might negatively impact the performance of a regulated sector and which we have been considering in our work. It should be noted that this list is neither exhaustive nor necessarily mutually exclusive.

- Weather – e.g. heavy rain leading to flooding
- Climate change – leading to severe weather, flooding, landslip etc.
- Volcanic eruption – e.g. leading to widespread ash clouds
- Space weather – e.g. solar flares
- Fire or explosion
- Terrorist attack
- Illness – e.g. pandemic flu in workforce
- Physical damage – accidental or deliberate
- Equipment failure – hardware or software
- Cyber-attack

3.3. This list does not include the loss of inputs which are delivered by other sectors, for examples power cuts, or failures of financial systems. These are cross-sector issues which we consider later.

Achieving resilient infrastructure

3.4. Securing resilience involves a range of activities. One framework for this given in the Cabinet Office guide "Keeping the Country Running: Natural Hazards & Infrastructure"[5] is reproduced below, although there are many others.

[4] From European Network Information and Security Agency (ENISA) "Guideline on Threats and Assets" - https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets
[5] https://www.gov.uk/government/publications/keeping-the-country-running-natural-hazards-and-infrastructure

Figure 2: The components of infrastructure resilience

Source: Cabinet Office

3.5. Within this framework, resistance is the ability of the infrastructure to successfully fend off a threat. Reliability describes the ability to continue operating, perhaps at a reduced level, even when a threat has caused some change to normal operating conditions. Systems with redundancy will be able to switch to back-ups when elements of their normal infrastructure have been affected. Finally, when a threat has affected a system's operation by overcoming the previous three protections, an effective response and recovery plan will return it to normal.

3.6. As noted in the previous section, the need for services to remain affordable means there is a practical limit on how much can be invested in resilience. The available budget needs to be directed in the most cost effective way. A common way to do this is to follow a risk based approach. This involves developing an understanding of the vulnerabilities of a particular piece of infrastructure and then considering the threats associated with that infrastructure to produce a list of the various risks to which there is exposure. Starting with the most serious, plans are developed to reduce the potential impact of each risk down to an acceptable level, as cost effectively as possible. Such a process needs to be continually refreshed as the risks will change over time.

3.7. Like all approaches to improving resilience, this will not reduce the risk to zero. Even with an unlimited budget this is unlikely to be a realistic expectation because it is usually impossible to predict all the possible threats and vulnerabilities that a system faces.

3.8. Companies in different sectors will focus on strengthening different components to improve their overall resilience. For example, adding redundancy may not be practical or economic for systems relying on particularly large or expensive physical assets. In other cases, redundancy might be available without any additional investment being needed, due to the ability of customers to switch to services provided by a completely different existing infrastructure in the event of failure. Where very complex infrastructure is involved it may be so difficult to identify and address all possible vulnerabilities that obtaining a sufficiently high level of resistance or reliability is essentially impossible. In such situations, the most effective investment to improve resilience may be in response and recovery.

4. Role of the regulators

4.1. Just as the elements involved in achieving resilience will vary sector to sector, so does the extent and nature of the regulators' involvement. In some cases the regulator has little or no formal involvement in directing the resilience of individual companies, as has been the case in the water sector until recently[6]. Elsewhere, such as in the communications and energy sectors, there is a high level requirement for companies to maintain appropriate levels of resilience, which is overseen by the regulator. In the financial sector the regulations are more detailed, for example requiring resilience arrangements to be regularly updated and tested.

4.2. In the energy sector, Ofgem sets allowances for network operators to fund their capital and operating expenditure activities. Companies are expected to ensure their networks are resilient and ensure that customers do not experience supply problems as part of their normal operation. Network companies provide annual reports which capture, amongst other items, the number and duration of power cuts. Based on these, Ofgem may adjust the companies' allowances via incentive schemes. In exceptional cases, Ofgem may investigate loss of supply incidents. An example of this is a review of the power cuts experienced by customers following the December 2013 storms.

4.3. To provide appropriate services to customers, companies in the water sector must manage, maintain and develop their assets and resources in accordance with the income allowed them from customers' bills. The role of the sector in managing the resilience of these assets and consequently services is not specifically defined in detailed terms. It is not desirable to dictate a 'one size fits all' approach to resilience as the geographic locations, conditions and asset bases provide different specific challenges. However, Ofwat intervenes on specific issues if required, such as issuing guidance on the resilience of critical infrastructure in the context of current and future climate change in its last water sector price review in 2009. Companies produced plans for output based solutions that generally involved specific capital projects such as flood defence schemes and new water supply grids to improve service resilience. Ofwat bases its monitoring of performance on data in companies' annual Risk and Compliance Reports.

4.4. The current water price review for the period 2015 to 2020 is taking a new approach by focussing on the desired outcomes, namely the continuity and resilience of services. This less prescriptive approach will allow companies to achieve their higher level objectives in a way that best meets their operational approach, resources and importantly customers' wishes with an emphasis on innovation and efficiency[7]. Companies are aware of their resulting obligation to understand their asset base and its vulnerabilities, assess risks, plan and implement solutions to mitigate those risks in a prioritised framework.

4.5. ORR does not set resilience targets for the rail sector, but it does review relevant performance and requires any identified improvements to be made. For example, the requirements placed on Network Rail for the period 2014-2019 include the obligation to produce, by September 2014, improved climate change and extreme weather resilience plans for all its routes as existing plans were not considered sufficiently robust. The requirements also set out specific asset management issues that need to be

[6] The Water Act 2014 introduced a new primary duty to secure the long-term resilience in the water industry
[7] 'Resilience – outcomes focused regulation – Principles for resilience planning', Ofwat, May 2012

considered by Network Rail and committed ORR to reviewing these policies throughout the control period.

4.6. There are a number of rules which place obligations on firms in the finance sector to take appropriate and reasonable steps to maintain the resilience of their regulated activities. The FCA considers that firms are responsible for the implementation of appropriate plans for operational resilience and supervises them accordingly. It may undertake 'deep dives' with supervisory colleagues to undertake detailed and comprehensive reviews of firms' resilience arrangements to confirm they are suitable and in accordance with the rules set out within the FCA Handbook. These assessments are not made strictly against standards, but will refer to internationally accepted standards of good practice such as ISO22301, ISO27001 and the Business Continuity Institute's Good Practice Guidelines. The FCA has a wide range of regulatory tools available should a firm fail to meet the requirements placed upon it, including fines or revocation of authorisation to operate in extreme cases.

4.7. In the communications sector, Ofcom does not approve or monitor investments in resilience. There are however high level obligations on companies to take appropriate measures to maintain reliable networks and services. Regularly updated guidance[8] is published for the relevant companies, which gives risk-based management of resilience as the expected starting point. Ofcom has the power to take enforcement action, including information gathering and auditing, requiring companies to take corrective actions, and issuing fines, if it determines obligations are not being met.

Incident reporting

4.8. In some sectors, but not all, there are regulatory requirements for companies to report incidents affecting the resilience of their infrastructure. In finance, companies must disclose anything of which the regulator would reasonably expect notice. The FCA considers that notification of any crystallised events resulting in material operational disruption to a firm's regulated activities are captured under this requirement, and would expect to be informed. In communications, companies have to inform Ofcom of reductions in availability which have a significant impact on a network. In energy, companies must report any events which have a significant impact on consumers to Ofgem. In the rail sector, incidents which affect safety must be reported to ORR.

4.9. New European legislation may introduce a significant change to the resilience role of most UKRN members over the next few years. The proposed European Network and Information Security Directive addresses the key role that electronic communication and computer networks now play in all infrastructure sectors. It is expected to introduce new resilience and reporting obligations in relation to what are commonly known as "cyber" incidents. The current draft sets out a scheme similar to that already in place for the communications sector, having been included in the 2009 communications Framework Directive[9]. The new Directive would extend these arrangements, including reporting, to all the sectors covered by UKRN, with the exception of water.

[8] http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/

[9] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC

Incident response

4.10. The role of regulators in responding to and recovering from incidents affecting resilience also varies. In the case of the FCA, it takes an active role in managing incidents with firms under its regulation and does so under its Interruption Response Framework which ensures fair and consistent handling. For incidents with a systematic impact, the FCA works with the Bank of England and HM Treasury under the Authorities Response Framework (ARF). If required, the Finance Gold crisis command group would be formed as the next level above the ARF, and would feed into COBR[10].

4.11. The CAA maintains and exercises a crisis management plan setting out how to respond in an efficient and effective way to support Government, industry and consumers to mitigate the impacts of major aviation events or significant business disruption within the CAA. The CAA's role in a crisis will depend on its nature, but may include:

- communicating with the public and the media regarding the crisis and the role that the Civil Aviation Authority is playing;
- supporting the Aircraft Accident Investigation Branch (AAIB) and Department for Transport (DfT) in the investigation of an aviation accident;
- repatriating passengers following an Air Travel Organisers' Licensing (ATOL) failure or on request from the DfT;
- supporting the DfT in implementing revised aviation security arrangements;
- restricting airspace in conjunction with the National Air Traffic Services (NATS);
- reviewing regulations and institutions in response to a crisis; and
- supporting or leading the prosecution of individuals and / or companies if required.

4.12. In other sectors, the regulator may have less of a formal role in managing the incident itself. For example, Ofwat does not have any formal emergency incident response role within its sector. However, it does monitor the effectiveness of companies' responses and recovery from incidents based on self-reporting plus direct and indirect customer contact information. Where it believes a company has not acted accordingly in its response, having considered the scale and impact of the event, it will investigate matters that fall under its jurisdiction and take enforcement action if necessary.

4.13. Similarly, Ofcom's duties don't extend to managing live incidents. However there are arrangements in place to plan for and coordinate the response to major incidents in which the industry, Government and Ofcom participate. This includes the National Emergency Alert for Telecoms (NEAT) process which is invoked for incidents affecting multiple communications companies. If appropriate, this process feeds into any higher crisis management layers such as Telecoms Gold command and COBR, usually via the Department of Business Innovation and Skills (BIS) in its role as lead Government department for telecoms resilience.

[10] Cabinet Office Briefing Room – the dedicated central government crisis management facilities used to coordinate the response to major incidents.

4.14. In the energy sector, the National Emergency Plan (NEP) outlines the procedures to follow in the event of a supply emergency. DECC may decide that a Joint Response Team (JRT) needs to be formed. The JRT may be formed of DECC, Ofgem and network operators, but the exact make-up of the team is decided by DECC.

Cross-sector resilience

4.15. The concept of cross-sector resilience is generally not mentioned in regulatory duties or powers. However, it is clear that none of the infrastructure sectors exist in isolation and all rely on other sectors for inputs essential to their continued operation. They are also all exposed to some common threats such as cyber-attack. As such, no sector can afford to think about its own resilience without considering the resilience of others. This also means that the general approach to resilience discussed above will naturally take into account cross-sector resilience issues to some extent.

Role of Government

4.16. Government's involvement in resilience, and cross-sector resilience in particular, is essential. Individual regulators have deep expertise on their sector, and depending on the exact nature of their duties this is likely to include resilience issues. However, the relevant Government agencies are often the authority on many relevant threats, especially those that are common across the sectors, such as natural phenomena, and those which come from malicious actions such as terrorism and cyber-attack.

4.17. The relatively narrow focus on its own sector that the legislation requires each regulator to take generally means that any interventions have to be justified in the context of that sector alone. The prevailing level of resilience achieved by the services in any sector is the result of a complex balancing of often competing factors such as affordability, geographic availability, environmental impact, innovation, competition, international competitiveness and reliability. Where there is a case for a different balance, for example in support of a broader national interest outside the regulator's scope, Government plays a key role in enabling, or even requiring, the regulator to act accordingly.

4.18. Government currently performs this function in several different ways. In some cases these issues are discussed in cross-sector fora such as those discussed in the previous section. In others, Government may take more direct action, such as formally directing or issuing guidance to regulators, or by introducing new legislation.

4.19. By way of example, the Water Act 2014 has given Ofwat a new duty to secure the long term resilience of supply and sewerage systems in the face of climate change, population growth and demand changes. More generally, the Secretary of State for Defra gives guidance to Ofwat on what elements of Government policy it must have regard to when implementing its regulatory responsibilities. This guidance is outlined the Strategic Policy Statement to Ofwat (2013).

5. Cross-sector resilience issues

5.1. Cross-sector resilience can be seen in terms of the inputs to a sector and its outputs to other sectors. Relying on general resilience activity tends to mean the inputs side is addressed. Companies consider the risks to the inputs they rely on from other regulated sectors just as they do for any other inputs. If an input from another sector is particularly critical, a risk-based approach to managing resilience should automatically prioritise work to protect it or find other mitigations in the event of its loss.

5.2. On the output side, all companies are focussed on the reliability of the services they provide as part of the normal course of business. However, relying on their general approach to resilience may not fully account for the particular needs of customers when they are part of other infrastructure sectors. Of course, provided one end of this output-input relationship is being appropriately specified, there should be no issues. It could be argued that if a company in one infrastructure sector is purchasing services from another sector, it is responsible for ensuring it specifies a sufficiently resilient product to meet its needs. However, there are a number of reasons why this process may not always work perfectly in practice. One of the objectives of the current work is to consider ways the sector regulators can contribute to improving the status quo.

5.3. Outside this UKRN work, cross-sector infrastructure resilience is already an area of increasing focus. One manifestation of this is the Cabinet Office's Infrastructure Security and Resilience Industry Forum. The forum is intended to foster stronger cooperation between Government, regulators and infrastructure owners and operators. It has been running for several years, and has grown during that time to become an important vehicle for stakeholders to share resilience information and experience.

Common risks

5.4. Common risks are those risks which can disrupt the resilience of infrastructure operators in more than one sector. Such risks could arise due to a common threat which can affect multiple infrastructures, albeit perhaps in different ways. Examples include the threat from cyber-attack and from severe weather events. While the particular damage they do to the infrastructure in different sectors may be very different, common threats are defined as those which have the potential to disrupt the services offered by any sector.

5.5. In some cases, the vulnerabilities will be common across the sectors, not just the threats. Examples could include telecoms and electricity cables occupying the same underground duct, or companies in different sectors using the same computer systems, or housing those systems in the same data centre building. In these cases, it is not just that the same threat may cause failures in different sectors; the failure modes will also be the same.

5.6. There are obvious benefits to knowledge transfer between the sectors in order to better address common risks such as these. It is likely that some sectors will have more experience than others in relation particular risks and information sharing can lead to resilience improvements that are quicker and less expensive than they would otherwise have been. Of course, even where risks are common, the differences between the sectors, such as the technical, operational, economic and regulatory frameworks, may mean some knowledge is not directly transferable.

5.7. As discussed earlier, the sector regulator may not be expert in a particular common threat, with leadership in this respect more likely to come from Government or industry stakeholders. The

regulator's role may therefore be one of coordination, backed up as appropriate by enforcement action or changes in the regulatory regime.

5.8. One example of this response to a common threat is that of climate change. The Environment Agency's (EA) Climate Ready service runs the Infrastructure Operators Adaptation Forum, which is attended by sector regulators as well as the companies operating the UK's main infrastructures. The objective of this forum is to facilitate cross-sector sharing of information and experiences of overcoming the challenges from long term climate change.

5.9. Other examples of cross-sector working come from the Government's objective to improve resilience to cyber threats under the 2011 National Cyber Security Strategy. The Cyber Security Information Sharing Partnership[11] (CISP) is joint initiative between industry and Government to share cyber threat and vulnerability information. The pilot of this scheme during 2013 involved 160 companies from sectors including finance, energy and telecoms. It is now operational and open to UK companies of any size which operate relevant networks.

5.10. Another cyber example is the summit held between ministers, senior officials and sector regulators in February 2014, which considered approaches to strengthening the cyber security of the UK's essential services. A joint Communiqué from the event recognised the importance of protecting infrastructure from cyber risks and set out a number of actions that would be pursued to achieve this.

Interdependency between sectors

5.11. The companies operating infrastructure in the regulated sectors will make extensive use of the services provided by one another. In some cases the resilience of these services will be vitally important to the reliability of the sector's own outputs. Looking broadly enough at each sector, it is likely that at least one service from every other sector will be used somewhere. However, the services most commonly cited as vital inputs come from the electricity sector, followed by telecoms.

5.12. The risks presented by these interdependencies have long been understood to be significant. Without sufficient resilience, it is theoretically possible for a problem in one sector to cascade across many others, affecting much of the UK's national infrastructure. As a result, many studies and much academic work have been undertaken, often involved with trying to predict and plan around otherwise unforeseen dependencies. Recent examples include Infrastructure interdependency analysis: Requirements, and capabilities and strategy[12] produced for CPNI in 2009, the Interdependency Planning and Management Framework[13] produced for Infrastructure UK in 2012, and Infrastructure Interdependencies Timelines[14], produced by Engineering the Future in 2013.

5.13. There are also a range of practical activities underway aimed at better understanding and managing the risks of cross-sector dependency. Most sectors have fora responsible for emergency planning, often feeding into the National Emergency Plan for that sector. To take the communications sector's group[15]

[11] https://www.cisp.org.uk/
[12] http://www.csr.city.ac.uk/projects/cetifs/d418v13_public.pdf
[13] http://www.bristol.ac.uk/eng-systems-centre/research/researchhighlights/interdependencyplanning.html
[14] http://www.engineeringthefuture.co.uk/government/pdf/EtF_Infra_Interdep_Report.pdf
[15] Electronic Communications – Resilience and Response Group - (EC-RRG)

as an example, interdependence with other sectors is often an agenda topic, with representatives from other sectors invited to meetings to participate in relevant discussions. Emergency plans are also regularly exercised, often based on scenarios involving the loss of services provided by another sector. In the larger exercises, such as Government-led Tier 1 exercises, participants from multiple sectors will be directly involved.

5.14. The Greater London Authority's project Anytown is running an ongoing series of workshops with experts from across the infrastructure sectors, and across the UK, to map the cross-sector impacts of infrastructure failure.

5.15. There are also sector-specific examples. In the finance sector, HM Treasury has run a pilot project involving FCA among others from Government and industry, aiming to assess the operational resilience of the telecoms systems which support the finance sector CNI. Regulators will also meet bilaterally where required to discuss specific issues that arise between their sectors.

Example – Winter storms and cross-sector dependency

A common root cause of disruption to the services offered by many of the regulated sectors is severe weather events. Beyond the direct impacts of the weather itself, there are a range of subsequent problems that can challenge the resilience of infrastructure, including cross-sector dependency. A recent high profile example was the series of at least 12 major storms during the winter of 2013/14 which caused widespread flooding and disruption across much of the UK.

Storms can directly affect services such as rail and aviation due to the immediate safety concerns, for example due to high winds or heavy snowfall. During the winter storms we saw the alteration and cancellation of rail services and the cancellation of services from several UK airports. Severe weather also frequently damages infrastructure and this can have a longer term impact on services while repair work is undertaken, with the railway line damage near Dawlish being a particularly high profile example.

Flooding is often a further source of infrastructure damage following major storms and can also hamper repair efforts, increasing the duration of "routine" failures unrelated to the weather, as well as those directly caused by it. One widely reported example from the winter storms was the threat of flooding to the Kenley water treatment works, although in the event normal operation was maintained at the site. In the telecoms sector, flood water caused damage at Winchester telephone exchange and threatened many other sites.

Beyond these direct impacts on particular sectors, severe weather events can also be the trigger for service problems involving cross-sector dependency. For example, the power outages caused by storms can create additional challenges for other sectors even in areas where their own infrastructure is not directly affected. As result of snow storms in Northern Ireland in March 2013, some customers in Antrim and Belfast had their water supply disrupted due to power interruptions at pumping stations. The same storms also left some telephone exchanges in the region without power for extended periods leading to a reliance on emergency generators. Factors complicating the repair of damaged infrastructure, such as floodwaters, or in this case snow, can result in power restoration taking several days. The same factors can hamper efforts to deploy and refuel emergency back-up generators, causing further service outages.

Interdependency example – electricity and telecoms

5.16. This example considers some of the implications of the interdependencies between the two sectors most commonly cited as being vitally important, both for each other and also for the other infrastructure sectors.

5.17. Telecoms relies heavily on electricity for its ongoing operation. It is used to power and cool networking equipment, the continuous operation of which is an essential part of telecoms service provision. Looking in the other direction, the electricity sector also relies heavily, and increasingly, on telecoms. While electricity generation and distribution can in principle continue without telecoms, many operational practices use it extensively.

5.18. Installing redundant infrastructure which is geographically separate is an important resilience tool used in telecoms to deal with power cuts. However, to protect local elements of the network, or to protect against geographically widespread power cuts, this approach may not be practical or economic. The main options available to telecoms operators when essential equipment is affected by a power cut are to arrange for supply from an alternative provider, store electricity for emergency use, or generate it from another energy source.

5.19. It is common for data centres, widely used in the telecoms and finance sectors, to have a combination of battery storage to maintain supply during short term power cuts and local generation for longer term interruptions. Generators, powered by diesel or gas, typically allow for several days of operation, with indefinite operation possible if the fuel supply can be maintained.

5.20. Such arrangements are expensive to install and maintain. They are therefore more likely to be used in situations where a large volume or value of services would be affected by a power cut. In telecoms, central sites handling the switching of telephone calls or the routing of data for hundreds of thousands or millions of customers are likely to have back-up power arrangements such as these, or alternatively be able to have their function taken over seamlessly by a geographically diverse site.

5.21. In fixed telecoms, BT's local exchanges have also been built to be resilient to the loss of mains power, so typically have battery and generator back-up. Customers' own wired telephones can also be powered from this back-up capability. This means that traditional fixed telephony services will typically continue operating for extended periods during power cuts.

5.22. The situation for fixed broadband services is more complicated, particularly with the increasingly important superfast services which typically require mains power at street cabinets as well as exchanges. The practical difficulties, and costs, of accommodating large batteries or generators at such small and numerous sites means the duration of power cut that can be accommodated is lower. In any case, depending on the geographic extent of the power cut, the customer's own equipment (router, computer) may not be working so the resilience of the local network cannot be considered in isolation.

5.23. The nearest equivalent to the telephone exchange in a mobile telephone network is the basestation. They are more numerous than exchanges and usually occupy much less physical space. They might be built as a mast and equipment cabinet in the corner of a field, or the equipment might be housed in vacant space somewhere in an urban building which hosts the antenna on its roof. The practicalities and economics of providing similar power back-up arrangements may be unfavourable as a result.

5.24. The impact of the loss of one basestation due to power outage is also different from the loss of an exchange, where all customers connected to it will typically lose service. In mobile networks, the coverage footprint of basestations will overlap so depending on the geographic extent of the power cut, service for a given customer may not be affected, or affected only to a limited extent. Additionally, the ability of customers to use any available mobile network to make emergency calls further increases

the chances that a signal from a still functioning basestation can be obtained for the most important calls.

5.25. These considerations have led to mobile network operators typically providing less back-up power for local infrastructure than was traditionally the case for fixed voice networks. While key basestations may have back-up power that will last for several hours, many others will have minimal back-up, perhaps only sufficient to ensure a graceful shut down of the equipment. Mobile operators will typically deploy portable generation equipment if required but there are obviously limitations to this approach in the event of widespread or prolonged outages.

5.26. Mobile communications is often cited by stakeholders in other infrastructure sectors as one of the most important cross-sector dependencies. This is because it is often used for the management of engineering workforces, particularly important when dealing with an emergency. So in the example of a power cut, any subsequent loss of mobile communications as a result could hamper efforts to deploy engineers to fix the power problem. This is an example of a cross-sector interdependency that has the potential to amplify the severity of the initial resilience issue.

5.27. Potential mitigations to the above risk might include a communication system for power engineers that is more resilient to power failure, or increasing the level of back-up power at mobile basestations. Both of these solutions are likely to be very expensive. Currently, it appears that such issues occur rarely. However, if over time they become more common, or the risk of them happening becomes increasingly unacceptable, Government may determine the current cost/reliability balance needs to change.

6. Phase 2 work – recommendations & further options

6.1. In producing the above summary of resilience across the infrastructure sectors, we have taken note of gaps which could potentially be eased by action led by UKRN members. These observations form the basis for the further work we set out in this section.

6.2. The first item we propose to consider further in phase 2 of the project is related to cross-sector resilience. We will examine the particular example of the reliance of telecoms networks on grid distributed electricity and the potential implications for the resilience of the sector.

6.3. The second group of work items all relate to enhancing collaboration between UKRN members to improve preparation for, or response to, cross-sector resilience incidents.

6.4. Finally, we have also set out some additional items which have been identified by our work to date, but which we feel may be of less value, or less likely to be deliverable in a reasonable timeframe. We are not proposing to take these forward at this time.

Cross-sector resilience

6.5. The resilience of the services offered by the sectors which UKRN members regulate is of national importance because they support so much of our normal daily and economic life. However, beyond their importance to other users, the services offered by one sector are also used by others. This creates the concept of cross-sector resilience – to what extent are each of our sectors resilient to problems in the others. The interdependence between sectors is a complex topic which has been studied extensively. Many frameworks and models exist to help understand, plan for, and reduce the risks that are presented. As regulators we recognise this is an important area and one in which we have varying roles to play within the broader public policy context set by Government.

6.6. Two of the sectors which are most often cited as providing some of the most important inputs for other sectors are energy and telecoms. In Phase 2 we are planning to look in more detail at an example of a resilience dependency between these sectors – the use of electricity by telecoms.

6.7. Section 5 of this report already touches on this issue in its brief discussion of mobile telecoms networks and their resilience to the failure of grid distributed power. Despite the clear dependency of one sector on another in this case, in practice we see relatively few widespread outages of mobile networks caused by power loss. This suggests that the likelihood of this cross-sector dependency causing a major incident is low. However, it is certainly not zero - previous resilience exercises have shown it is possible to generate plausible scenarios under which it could happen, and if it did the impact would be very significant.

6.8. The resilience of mobile networks to power disruption is likely to become of increasing interest over time. We have seen people and businesses placing more and more demands and reliance on these networks, which themselves have a critical need for electricity to function.

6.9. The intention of this work is to inform any subsequent policy debate on this and similar cross-sector resilience issues. We will consider the current levels of reliance of telecoms on grid distributed power and the range and effectiveness of existing measures to limit the impact of any interruptions. We will go on to consider how the expectations of reliability might shift in the future and whether the current

protection measures are likely to be sufficient. Finally we will consider what options might be available if there was a future policy decision to effect a significant change in the level of power resilience.

How can we increase collaboration in cross-sector incident planning and response?

Cross-regulator emergency plan (CREP)

6.10. Regulators currently communicate and coordinate activity during major incidents through established channels such as COBR, for the most serious national incidents, and we use bi-lateral arrangements with each other on an ad-hoc basis if the situation requires it for lesser incidents. We want to explore whether there would be additional benefit in developing a more formal framework setting out how we will communicate directly with one another during incidents affecting two or more of our sectors. Such a framework could operate as an adjunct to the existing arrangements in place within each regulator for dealing with major incidents, where it makes sense to do so.

6.11. The framework would include thresholds for triggering its use. When these were met, it would set out protocols for how communication would take place. To give an example of a similar framework which is used by stakeholders within the telecoms sector during major incidents, this sets outs things such as:

- contact lists for representatives of each organisation and regular updating procedures;
- multiple methods to alert participations of the framework's activation;
- diverse platforms for hosting a conference call and/or using the Cabinet Office's Resilience Direct extranet web portal;
- protocols for the chair and participants on the conference call;
- templates for information shared on Resilience Direct; and
- regular testing and process review procedures.

6.12. The framework would be intended to serve several purposes useful in the context of dealing with a major incident. Firstly, and perhaps most importantly, it would provide a platform to allow information sharing between affected regulators. For example, during a prolonged flood, it may be useful to the telecoms industry to understand the likely order and timing of mains power restoration across any affected areas. Having a shared view of the incident is also beneficial to the regulators directly in ensuring any messages they release to the public or media are accurate and consistent. It may also facilitate resource sharing between the regulators, or other stakeholders within the sectors, where this is appropriate. However it would not replicate or replace the emergency procedures that regulated businesses themselves are responsible for maintaining for the purposes of crisis coordination.

Shared method for assessing the state of regulated companies' cyber security

6.13. For companies in the sectors we regulate, cyber-attacks are already a high profile source of security incidents. They also have the potential to cause resilience problems across the sectors and are therefore within the scope of this project.

6.14. In February 2014, the Secretary for Business, Innovation and Skills, Vince Cable, hosted a meeting on cyber security which was attended by the majority of UKRN members. The joint Communiqué issued following the meeting[16] committed participants to a number of actions. One of these in particular, to assess the state of cyber security across each sector, potentially lends itself to a coordinated approach between relevant UKRN members. Sharing experience and knowledge between the regulators involved in these assessments will be beneficial in reducing any duplication of effort and ensuring the outputs are comparable and of a high quality.

6.15. There is a considerable amount of work already underway in relation to cyber security, and our work will be mindful of this. For example, as part of the UK's national cyber security strategy[17], government agencies such as CPNI are already undertaking various cyber security assessments, particularly in relation to CNI companies. Some UKRN members have already undertaken cyber security assessments or been involved with assessments led by government agencies. For example, the FCA, working with the Bank of England and Her Majesty's Treasury, has developed CBEST, a framework for testing the resilience of critical financial assets to cyber-attack[18]. This followed a consultation with the sector to understand the current levels threat intelligence, cyber security and testing.

6.16. We will work with the relevant government agencies to understand the areas where additional assessment activity by the regulators will be most beneficial. We will also share our knowledge and experience of how this work can best be achieved. The work would also act as a focal point for any other joint activity on cyber security issues.

Joint exercise coordination

6.17. An essential part of improving resilience is performing regular exercises to test the response arrangements that are in place. In many cases, resilience exercises in one sector have benefited from the involvement of other sectors, and such activity can be used to improve plans to deal with interdependencies. For example, Exercises Long shadow in 2007 and White noise in 2009 tested the country's response to widespread power and telecoms failure respectively, and involved many organisations from across the infrastructure sectors.

6.18. Despite the examples of good cross-sector collaboration in some previous exercises, there is currently no clear mechanism for information about forthcoming exercises to be shared. It is therefore possible that opportunities for cross-sector involvement will be missed. Regulators are well placed to help address this, by regularly gathering and sharing exercise information with other regulators, and the companies in their own sector.

Further options

6.19. As well as the items set out above for further study in phase 2, our work to date has also identified other areas which could be considered. We do not currently have any plans to pursue these further because we have prioritised the earlier items as those likely to offer most value or to be deliverable in a reasonable timeframe.

---

[16] https://www.gov.uk/government/publications/communique-strengthening-the-cyber-security-of-our-essential-services
[17] https://www.gov.uk/government/publications/cyber-security-strategy
[18] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

- **A guide to infrastructure resilience for cross-sector users.** It will always be true that the infrastructure sectors rely on each other to varying degrees and that however resilient the services offered by each sector become, they will sometimes fail. Despite the many studies and frameworks that have been produced, these realities mean cross-sector interdependency problems will continue to occur. The more the sectors understand of one another's resilience strengths and weaknesses, the better they can plan their own resilience measures.

  Such a guide would explain each sector's approach to resilience and set out the key information and recommendations that users in the other infrastructure sectors should be aware of. Industry involvement would be necessary, ideally drawing on expertise and existing material from the sectors' emergency planning groups. Although we have decided not to pursue the development of a guide in Phase 2, it may be useful to revisit this at some future point if interest in cross-sector resilience continues to grow.

- **Joint preparation for the European NIS Directive.** A new European Directive covering Network and Information Security (NIS) is currently being developed. If it continues to final publication, which currently appears quite likely, it is expected to introduce new security and resilience obligations on companies in most infrastructure sectors within the next two or three years. This would have a significant impact on the resilience planning and incident reporting in most UKRN-regulated sectors.

  If they come into force, the requirements in the draft Directive would not be entirely new. Some aspects, in particular the reporting of major resilience incidents, are similar to those in an existing Directive which has applied to the communications sector since 2011. Other aspects, such as any requirement to take appropriate steps to maintain the service and resilience of services are likely to overlap with existing regulatory requirements in some sectors.

  It is currently too early to determine exactly how the NIS Directive will be implemented in the UK. It may be for example that the sector regulators will not be directly involved in the incident reporting process. However, it seems unlikely that the UKRN members would not be involved in implementing the Directive at all. Therefore, having a platform for sharing information and experience between us might be useful. This work would consider how this could best be achieved which will depend how the Directive develops. If the impact on the regulators is limited, it may be that an existing forum for discussing security or resilience matters can be used. Alternatively a dedicated new group may be warranted if more work is required.

- **A cross-regulator emergency planning group**. Such a group would sit alongside the proposed cross-regulator emergency plan (CREP), and mirror the various resilience planning groups that exist in each sector. We are of the view that the existing UKRN structure is currently sufficient to fulfil this role. UKRN is an ideal vehicle to develop and maintain the CREP and this work should encompass all the areas on which cross-regulator resilience cooperation is currently beneficial. If any new items emerge, a new UKRN project and/or group can be established as needed.

- **Regular attendance of resilience planning groups in other sectors**. It is clearly beneficial for regulators to maintain a good knowledge of the resilience arrangements in other sectors. However, attending sector-specific groups may not always be appropriate, and there is evidence of ad hoc attendance occurring already when specific issues suggest it. On balance therefore we feel the current arrangements are sufficient.

- **Regulators to attend all relevant cross-sector resilience groups and follow-up as required**. There are a number of groups dealing with cross-sector resilience issues, such as the Cabinet Office's Infrastructure Security and Resilience Industry Forum. Regulators already regularly attend these and also follow-up directly with each other as required, so no further action seems to be needed at this time.

- **Detailed risk assessment and mitigation costing for each sector**. This is a broad description which could encompass a range of activities such as identifying and prioritising residual risks, determining whether and how they could be further reduced and how much this would cost, and assessing emerging risks. We are of the view that these sorts of activities are best undertaken sector-by-sector as required by the particular circumstances each faces. They are also already reflected in the Sector Resilience Plans. We therefore do not see significant benefit in UKRN involvement.