techUK

THE UK'S CORE DIGITAL INFRASTRUCTURE: DATA CENTRES

CLIMATE CHANGE ADAPTATION AND RESILIENCE

Voluntary submission to DEFRA on behalf of the ICT (information, communications and technology) sector under the Adaptation Reporting Power (second round of reporting) as defined by the 2008 Climate Change Act

Abstract

This submission explores the climate change readiness of the UK's data centre sector, plus informal observations on fixed line and mobile communications. This report explains the main features of our core digital infrastructure – data centres, fixed line telephony and mobile telephony - and how they fit together. It records the information sources that we are using to assess climate change risks and it highlights the main threats that present challenges to the operation of our digital infrastructure and to the delivery of services that depend upon it. It sets out some of the approaches that we already deploy within the sector to identify, manage and mitigate those risks. The report then reviews several recent climate change related incidents that resulted in interruptions to service, considers what we have learned from these and what actions are being taken. Finally it explores several areas that require further scrutiny to ascertain whether they represent potential vulnerabilities and suggests where there is scope for action. This report does not pretend to provide a complete picture of our readiness for climate change risks: it is the first step in an iterative process.

December 2016

Contents

0 Executive Summary

Introduction and scope

This is a voluntary report submitted under the Adaptation Reporting Power. It explores the resilience of our digital infrastructure to climate change risks. Because the communications sector has already reported under ARP this submission focuses primarily on data centres, but includes observations on fixed line and mobile communications. Because we are reporting as an industry association representing dozens of operators, rather than an individual infrastructure provider, we are not party to individual corporate risk plans so the report provides a general overview of the state of play. It is a first submission in what we anticipate to be an ongoing process.

Climate change adaptation is about being resilient to the risks posed by a changing climate. It is therefore different from climate change mitigation, which seeks to minimise emissions and reduce global warming. Adaptation is therefore about coping with climate change rather than preventing it.

What is our core digital infrastructure?

Our core digital infrastructure is not a single system but multiple systems and networks that interoperate. The three main constituents are fixed line telecommunications (made up of the high capacity and highly resilient core network plus the access network which runs from the exchanges to tens of millions of individual customer premises), mobile telecommunications (that interacts with the core network but provides customer coverage through a cellular network) and data centres (that manage, transmit, process and store data for government, businesses, individuals and academia). Satellite and broadcast communications also play important roles in digital infrastructure.

How will the climate change and how do we find out about climate change risks?

Climate change risks relevant to our digital infrastructure are primarily flooding from increased winter rainfall, changes to humidity and temperature and high winds. UKCP09 (UK Climate Projections) include probabilistic scenarios for rainfall, temperature and humidity that are relevant for future planning and standards development within the sector, although it is not clear that these are widely used by operators. The Environment Agency's Flood Risk Maps provide localised flood risk information and are extensively used by operators, advisors, investors and consultants to inform decision making, especially choice of location and design. They are also revisited during the operational stage to meet bid requirements, for insurance renewals and to comply with availability standards, but regular review is not systematic across the industry. The extent to which the sector is aware of, and uses, other EA data such as surface water modelling is variable.

What is special about digital infrastructure in this context?

ICT infrastructure has some unique characteristics that make it relatively resilient to climate change: asset life is relatively short so more resilient assets can be deployed as part of the natural replacement cycle, there is more built-in redundancy in IT infrastructures, and technology development is fast and often able to innovate around threats. On the other hand the sector is highly dependent on energy and we are increasingly dependent on ICT for our economic and social wellbeing. The multiple interoperable systems that make up ICT infrastructures confer advantages in terms of redundancy and overlap but they are also complex. Not all interdependencies are known and rapid changes in technology may expose the sector to new and unexpected vulnerabilities.

What are climate change threats?
Climate change threats include coastal, fluvial and pluvial flooding, increased severity and frequency of storms, lightning, high winds and heavy rain, increased average summer temperature and winter humidity, increased speed of temperature and humidity change, and drought.

How will they impact our infrastructure?
Physical impacts include flooding of buildings, ducting and other assets; water, silt and salt damage, scour of cabling and foundations, subsidence to buildings and masts, problems of access for engineers and staff, disruption to fleet operations, cable heave from uprooted trees, higher costs of cooling, shorter asset life, reduced reliability, fractured ducts, reduced signal strength and higher operating costs. Non-physical impacts include reputational damage, failure to meet customer SLAs (service level agreements), failure to meet regulatory objectives, high customer call volumes, impacts on staff wellbeing and unbudgeted costs.

How do we deal with climate change risks?
Climate change risks are handled as just one of a myriad of business risks facing the sector, and we consider this to be an appropriate approach. Data centres compete on the basis of resilience: resilience tends to be matched to criticality and to price. Specialist data centre availability classes under the EN50600 series of standards reflect this. Data centres work to a range of generic risk standards such as ISO 31000 and ISO 22301. Operators adopt formal risk management tools and processes. Scenario planning for emergencies is common.

At build and design stage, flood is at the top of the list of risk factors when choosing a location for data centres; although there is no agreed risk threshold, industry practitioners generally seek a risk below 1 in 1000. This is, however balanced with other factors and emphasis is on managing and mitigating the risk rather than working to inflexible thresholds. Operational risk management is not limited to physical protection and data centres may be mirrored to ensure a continuously available backup. Power availability is key and batteries provide instantaneous power in the event of a grid outage, with diesel generators for longer outages. Similar approaches are taken by communications providers for core network functions. In addition the sector follows recognised industry standards for masts and towers – BS8100, BSEN1991-1-4, BS EN1993 and PLG07.

What have we learned from recent events?
The UK's digital infrastructure has to date been relatively resilient to severe weather. While there have been isolated incidents and localised interruptions in service, the sector has not suffered the scale of problems encountered by other utilities, such as those experienced during the 2007 floods, which left tens of thousands of people without water and electricity. This is no reason for complacency. The sector has learned lessons and implemented changes following recent events including loss of communications services in York and Leeds in 2015 due to flooding in a telephone exchange and a dedicated data centre. However, the most serious events were abroad: Hurricane Sandy impacted data centres in New York and New Jersey, and the sector has also learned from Japan where prior planning ensured that Japanese data centres escaped serious damage from the 2011 tsunami. Improvements have been implemented to fuel storage, switchgear protection, communications and emergency access arrangements.

What are the barriers to building adaptive capacity?

Building adaptive capacity does not come cheap, but cost is not the only barrier. There are interdependencies with other infrastructures: the sector relies heavily on electricity and to a lesser extent on transport - for regular operations, emergency access and generator replenishment in times of power outage, and on water. It is also vulnerable to failures in physical "pinch points" like bridges that carry multiple utilities – communications, electricity and water. Within ICT there are critical sub-sector dependencies : data centres cannot function without communications and vice versa. The complexity of our digital infrastructure can sometimes make it difficult to understand and identify these interdependencies.

Other internal barriers include a mixed picture on awareness of relevant sources of information, and understanding climate change risk. External barriers include a disproportionate focus on protecting physical assets rather than on continuity of service delivery. For communications providers regulatory approaches that hamper efforts to improve resilience (such as the conditions of the fixed line Universal Service Obligation or the emphasis on competition over price for mobile operators) and the failure to enforce planning policy in flood zones can be unhelpful.

Which areas need further investigation?

Looking ahead, we are taking action at sector level to improve resilience. There are areas that need further work. There is (fortunately!) a very limited evidence base to inform future actions, we need more data on how often operators re-examine flood risks; interdependencies are not fully understood and some regulatory approaches could have unintended consequences on resilience.

What else will we be doing?

So we will monitor any publicly reported events and share learning outcomes, raise awareness of the nature of climate change risks, the information available, and how it should be used. We will alert the industry to relevant standards and develop recommendations for operators to review flood risk regularly. We will continue to engage with external stakeholders and regulators.

Our recommendations

Others can help us build adaptive capacity. We therefore recommend

i. A preferred or default UKCP scenario to encourage infrastructure operators to use the same reference points for strategic planning and standards development.
ii. A broader focus on service delivery rather than asset protection.
iii. A more robust approach to flood plain development that is at odds with Environment Agency advice e.g. responsibility retained by developers or limited obligations for infrastructure operators in those zones.
iv. Scope for the provision of condition reports on bridges that carry multiple utilities and other single points of failure in our physical infrastructure.
v. A review of regulatory provisions of the USO for fixed line telephony, especially for new properties located in flood zones.
vi. Scrutiny of the current regulatory focus on customer prices for mobile services in terms of its potential impact on resilience.

Contact: Emma Fryer, Associate Director, techUK: emma.fryer@techuk.org

1 Introduction and scope of report

Section summary: *In this section we define climate change adaptation and differentiate it from mitigation. We outline the scope of this report and its limitations. We also explain that while this submission relates to the Adaptation Reporting Power, it is nevertheless voluntary, our first attempt to explore a specific set of risks in isolation and is iterative rather than comprehensive.*

1.1 What is climate change adaptation?

Adaptation[1] assumes that climate change will happen and is already happening, and focuses on being resilient to the impacts. This differentiates it from climate change mitigation, which seeks ways to minimise climate change by reducing carbon and other GHG (Greenhouse Gas) emissions, or by sequestering carbon. Mitigation is therefore about trying to *prevent* climate change and adaptation is about *coping* with it when it happens.

In this context, adaptation means continuing to enjoy our current quality of life in a changed climate by ensuring that the complex support systems that we rely on can still function adequately when climate change risks are realised. We have to make sure they are resilient to things like flooding, sustained high temperatures and rapid fluctuations in temperature or humidity in the same way that we try to make them resilient to other forms of interference such as theft, vandalism or terrorism. Adaptation does not mean we have to live in caves and eat bugs.

Our lives depend on a complex array of interconnected physical infrastructures – energy, transport, communications, water, etc. If our infrastructure is compromised then so too is our economic and social activity. So, successful adaptation in the modern world depends on building infrastructure resilience.

1.2 Scope of this report

For the purposes of this report we have taken a simplistic view of our core digital infrastructure and represented it as three main constituents: the data centres in which our digital data is processed, managed and stored, the fixed line telecommunications network and mobile telecommunications networks. We have not covered broadcast or satellite on this occasion but since they comprise important elements of our digital infrastructure they will be included in our next report.

Since the communications sector has reported previously under ARP (in 2011), this report is primarily intended to cover the data centre sub-sector of the ICT sector, which has not yet reported. That said, ICT comprises a combination of systems and networks of which data centres are an integral part. We therefore had the choice of reporting exclusively on the data centre sector and declaring a heavy cross-sector interdependency with communications or to provide some generic information on those sectors as an interim measure. We have chosen the latter on the basis that this seemed the most constructive and pragmatic approach but the information included here is only an informal representation of our understanding of these other sub-sectors. For a formal assessment of climate change readiness we refer to OfCom's Report "Climate Change Adaptation:

[1] Formal definitions vary.

Impact on our Functions, submitted September 2011" in response to the Secretary of State's Direction.

As a trade association reporting on behalf of dozens of operators, we do not have insight into individual risk assessments or corporate contingency planning – nor should we. However, we do have a general understanding of the state of play. This report to some extent exploratory and at this stage we do not expect to be in a position to provide a comprehensive assessment of relevant risks, propose specific risk thresholds and standards or provide a full catalogue of mitigation actions specific to this agenda. Moreover we cannot comment on sites designated CNI (Critical National Infrastructure) because we are not party to information on how those sites manage resilience.

Our initial objectives are to explain our core digital infrastructure, to explore it in the context of climate change risks, to present some indicators of the general state of readiness, to identify areas where greater scrutiny is needed and to stimulate discussion within the ICT sector itself on how these risks should be managed looking ahead.

This report is voluntary, this is the first time we have examined the sector through this lens, this is our first report and is therefore likely to pose at least as many questions as it answers. It should be viewed as the first step in an iterative process and indeed it is already clear that this exercise has initiated a new conversation within the sector.

2 Definitions: What makes up our core digital infrastructure?

Section summary: *This chapter provides a non-technical overview of the three main components of our digital infrastructure: data centres, fixed line communications and mobile communications in turn. Not everyone is familiar with digital infrastructure so there is quite a bit of explanation here that can be skipped if you are conversant with these technologies. In truth it is rather artificial to separate fixed and mobile communications because technological convergence means that in reality they are interconnected parts of a single digital system.*

2.1 Data Centres

For the purposes of this report, our core digital infrastructure comprises three main components: fixed line telecommunications, mobile telecommunications and data centres. The fixed line and mobile networks are independent but interconnected. Both networks rely on data centres for managing, storing and processing data, but data centres do not just facilitate communications services. They also provide the core digital infrastructure underpinning the IT functions of businesses, government, academia and social networks. If we want to live connected lives then we need data centres. If we want to bank, shop or socialise online then we need data centres. If the UK wants to be a net exporter of digital services, then we need data centres.

So what does a data centre do, exactly? In terms of function, data centres store, manage, process, receive and transmit digital data at scale within secure, specialised, resilient buildings. A data centre consolidates any number of separate IT functions within a single operating unit, delivering economies of scale, improved performance and efficiency.

In terms of the physical asset, a data centre is a building (or self contained unit within a building) used to house computing equipment such as servers along with associated components such as telecommunications, network and storage systems. A data centre is equipped with a guaranteed power supply and high bandwidth connectivity. Resilience is critical so redundancy (duplication) of networks, power and other infrastructure is common to ensure continuity. Building management controls such as air conditioning maintain the environmental conditions for the equipment within a specified envelope of temperature and humidity, and security systems ensure that the facility and its data remain secure. In plain English a data centre is a building filled with lots of computers talking to lots of other computers elsewhere.[2]

There are around 500 data centres in the UK. Roughly a third of these are colocation (commercial) facilities, operated by specialist data centre service providers like Equinix, Pulsant, Digital Realty, Global Switch, Virtus, etc. the rest are known as enterprise, which loosely means "in house". Some of these support ICT service providers (like IBM, BT, Atos, Fujitsu, HPE) and the rest underpin corporate IT functions for all sorts of organisations like universities, banks and supermarkets.

Twenty years ago there were no data centres – or at least none as we know them today. That's probably because there wasn't enough digital data to create a requirement for specialist facilities in which to house and process it, and the data that existed did not underpin enough critical

[2] For more detail see "Er What is a Data Centre?"

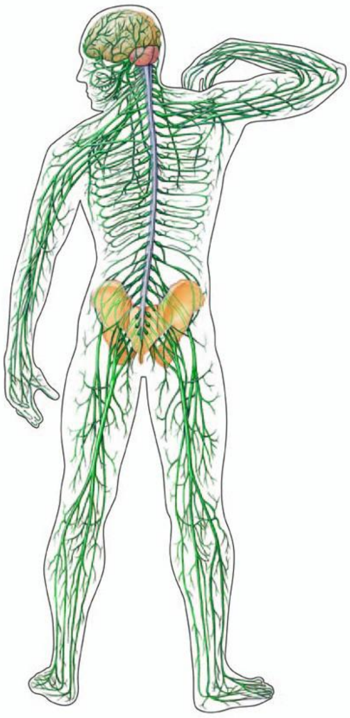
government, business or social functions to make protecting it such a key priority.   More and more of our everyday processes, including government services, business processes, shopping and socialising rely on computing to function. So the growth of data centres is the result of our increasing reliance on computing and on digital technology generally.

The growth in data centres is also the result of changes in the way that we handle our computing – our increasing tendency to consolidate IT resource in purpose built facilities rather than keeping it on individual company premises in server rooms and cupboards (known as “distributed IT”).

2.2 Telecommunications: fixed line communications infrastructure

All telecommunications involve the movement of information in the form of electromagnetic energy, from a transmitter, via a transmission medium, to a receiver. The energy can take the form of electrical signals transmitted along wires, radio signals transmitted through space or light signals transmitted down glass, or fibre-optic cable. Telecommunications, in contrast to broadcast and most other utilities, are bi-or multi-directional and are important enough to economic and domestic activity to be classed as CNI (Critical National Infrastructure)[3].

Our fixed line telecommunications infrastructure comprises a bewildering array of assets that vary by age and life expectancy, by vulnerability and criticality. Messages are transmitted between customers via the core network or via local nodes (communications nodes and exchanges) and the architecture resembles a tree with messages moving via trunk and branches to leaves, or a nervous system where messages move between brain, nodes and peripheries (see image).



Simplistically, it can be seen as two parts – the core network (central high volume trunking and data centres) and the access network (from the exchanges to the customers).

The Core Network

The core public network, or PSTN (Public Switched Telephone Network) in the UK is operated by BT, except Hull, operated by KCOM (Previously Kingston Communications). It comprises around 5,000 telephone exchanges, about 350 buildings and a high bandwidth transmission network, most commonly of bundled fibre optic cables, enclosed either within specialist earthenware ducting, or more recently, plastic tubes. These same tubes may carry network infrastructure for other telecoms providers who have their own core networks and/or lease capacity from BT.   Historically, voice messages were transmitted through a trunk and branch network.   Voice transmission has now been replaced by data and voice signals are converted into an

[3] For a clear description of the network, its history and characteristics, see the EC-RRG group publication on protecting communications: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62279/telecommunications-sector-intro.pdf

IP (Internet protocol) stream then routed through big “soft switches” through a voice gateway into a managed network. Data traffic is actively managed and the same data stream can take one or several routes to its destination, splitting and joining up again later. This allows the network to make best use of available capacity and minimise latency (delay to signals).

Data transmission works in a similar way, using the IP network and relying on powerful servers to provide the data switching capability. The majority of data transactions are small ones – checking availability of a book or buying a hat or renewing a tax disc involve downloading a web page or two after which the download ceases. However, video streaming and offerings like iPlayer require continuous availability of high bandwidth communications. The growth in large size file transfer requires more and more network capacity and drives up costs.

The core network has to perform a number of different functions with high levels of reliability and resilience, underpinned by service level agreements (SLAs) with customers (e.g. other telecoms services providers). These networks are managed from highly resilient sites with duplicated fibre connections, duplicated power supply, back-up generators, duplicated servers and even whole data centres, extra capacity, additional soft switches and duplicated locations for routing.

The access network

The access network is operated by Openreach. It is the part of our fixed lined telephony network that stretches from the local exchange to the customer’s premises (a distance that can vary from 10m to 17km but is on average 5km) usually via an underground cable in a duct or sometimes just trenched in the ground. Multiple cables start from the exchange and peel off to cabinets along the route. A 200 pair cable may go down to a 10 pair cable by the time it arrives at the final cabinet, from which cables fan out underground or via telegraph poles to individual premises. There is one pair for each customer. No power is needed locally to use a fixed phone at home as the service is power fed from the exchange battery down the pair from the exchange. Cordless phones need their own power source (hence their unsuitability for 999 service when the power is off locally).

Cabinets and cabinet architecture

A first generation cabinet

There are around 90,000 cabinets and most homes are within 1km of a cabinet. Sometimes in rural areas an aerial cable is carried via poles. Physical assets range in age from brand new to over 100 years old as some of the architecture is unchanged since the beginning of telephony service.

Recent changes to access network architecture with the introduction of second generation (superfast) broadband have implications for resilience.

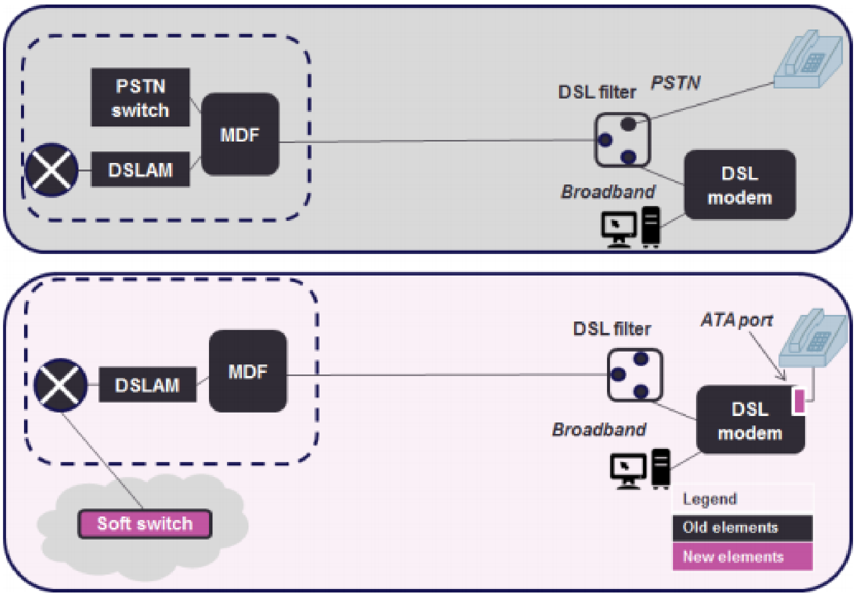
First generation broadband (ADSL or asymmetric digital subscriber loop) did not require changes to infrastructure because the broadband shared the copper pair with telephony by the application of a filter. Second generation (superfast) broadband involved a marked change in the architecture. New cabinets installed near to existing ones take optical fibre from the exchange (FTTC or Fibre to the Cabinet), usually drawn through existing ducting and have Digital Subscriber Line Access

Multiplexers (DSLAMs). These are powered locally from the street mains supply and have battery backup.

A second generation (superfast) cabinet

The DSLAMs are connected to the customer's existing telephony pair in the adjacent cabinet via a copper tail cable and the broadband service is carried to the customer's home on the existing telephony pair. The telephony is still carried in the same way as before. However this time local power is needed for the broadband modem.

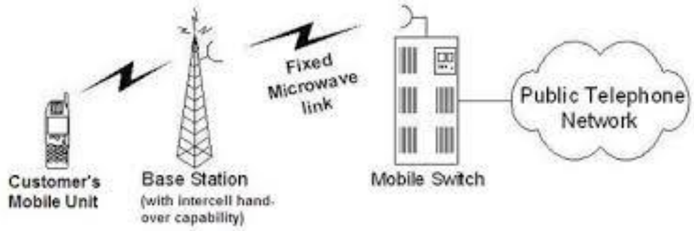
So there are two important considerations for second generation broadband; the (FTTC) continues to depend on both cabinets and is essentially a hybrid. Where fibre extends to the home (FTTH) this is not the case and it does not depend on the cabinet. However, for the next generation of architecture, power is needed at customer premises and landline phones will no longer be powered from the cabinet or exchange. This will be an important factor in resilience planning.



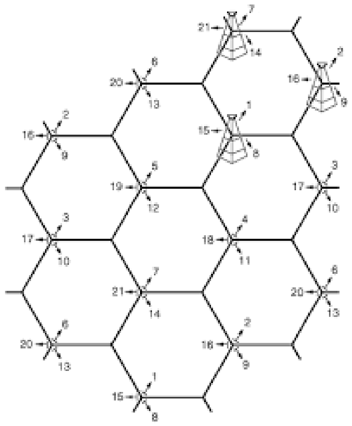
Schematic diagram showing the difference in architecture as the PSTN (public switched telecoms network) is gradually superseded. By around 2025 we expect the PSTN to be switched off. Careful consideration should be given regarding the implications of this major infrastructure change on resilience.

2.3 Mobile communications infrastructure

Calls using the mobile network involve at least one wireless link. A mobile device receives wireless signals from a base station, which may receive signals wirelessly from a local exchange. Switches at this exchange will transfer the signal into a fixed line network, which may be a private network belonging to the mobile operator or the public telephone network (PSTN) operated by the incumbent fixed line telecoms provider. The mobile system will automatically choose the optimum route to make the connection depending on traffic, availability, and cost.



So a call to a mobile phone from a landline phone travels via a fixed line to the nearest exchange then, depending on where the mobile user is, can travel over the public network to a mobile exchange near the user, or via a private fixed line (usually fibre) belonging to the mobile operator and thence via the mobile exchange. The mobile user pays the incumbent for traffic using the public network, so provided that the mobile operator has sufficient capacity, routing will tend to minimise use of the public network. However, the core public network has far greater capacity with plenty of redundancy.



Our mobile communications architecture is based on a cellular model rather like a honeycomb, except the cells may vary in size depending on user density. This differs markedly from the much more dendritic fixed line network (see above).

A mobile base station (the building at the bottom) with mast

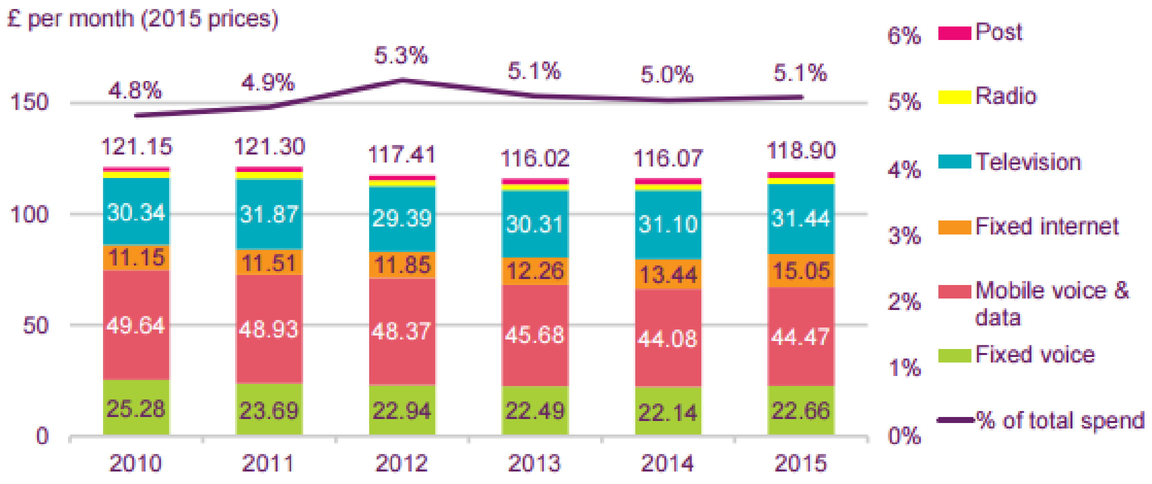
Each cell is serviced by a base station but there should be overlap between cells and if connectivity is lost in one particular cell, messages can be transmitted via other cells – a bit like Chinese Chequers. This is the theory although in practice this is not always the case, especially in rural areas where a single mast may be shared by multiple operators and therefore can present a potential single point of failure. In general, though, the cellular structure is an efficient way of providing resilience although there is much less redundancy (spare capacity) in the system than in the fixed line network.

Relevant market developments

The mobile communications network is enabled by radio masts connecting base stations and other elements of the network. Early on in network history, operators were under pressure to share masts (through the 1969 Town and Country Planning Act, although this did not become an issue until 1985 when operators began to roll out their own networks). Most were reluctant because in the early days of mobile telephone services, coverage was the primary USP. In recent years, coverage became less of an issue as the USP developed into a more complex combination of services and offerings. In addition, the high capital cost, maintenance obligations and the burdensome compliance and planning requirements related to the installation of new masts provide compelling incentives to share. Independent mast providers like WIG and Arqiva provide shared infrastructure as their business model. However, coverage is still a very live issue and currently, pressure is growing for operators to compete once more on coverage.

Some observers also remark that the highly competitive nature of the UK's mobile telephony market is another factor; margins for mobile operators in the UK are severely reduced and as a result infrastructure provision may be minimised in some areas because incentives for investment are limited by market conditions. For evidence of this see the two charts below. The first provides statistics on consumer spend on communications, which has been largely flat for the last 5 years despite the fact that consumption has exploded during the same period. The second chart provides data on delivery rates and consumption over the same period. Both are sourced from Ofcom.

Figure 1.2 Average household spend on communications services



Mobile and fixed stats from 2010-16	2010	2016
Coverage of broadband at 2Mbit/s	86%	c100%
Coverage of superfast broadband – 30Mbit/s	58%	90+%
3G premises coverage by all operators	72%	88%
4G Coverage by all operators	0%	55%
Average fixed download sync speed	7.5 Mbit/s	28 Mbit/s
Average monthly data usage per residential connection	17GB	82GB
Average mobile monthly data usage per SIM	0.24 GB	0.87GB

While competition has reduced prices it may not have served the consumer well in terms of provision and reliability. There are obvious implications for climate change resilience, which we will revisit.

3 Identifying relevant climate change risks

Section summary: *In this section we review the UK Climate Projections and identify the impacts most relevant to ICT infrastructures. We reproduce UK maps showing probabilistic models for the two most important climate change impacts: increased seasonal precipitation and increases in summer temperatures and we explain which scenarios we have chosen and why. We make observations about the data provided by the EA and the extent to which the sector makes use of it.*

3.1 Climate projections for the UK

We have made use of the UK Climate Projections as our source of information on the changes we are likely to experience in weather patterns as a result of climate change. As is made clear by UKCP these are probabilistic models and a range of scenarios are presented for different time periods, different emissions levels and different probabilities. The predictions also vary significantly by UK region. Although the UK's data centre estate tends to be clustered around connectivity and customers, the mobile network and fixed line network cover the whole of the UK, so a UK-wide model has been used.

We have adopted the 50 year projections, the medium emissions scenario and central probability as our framework. In general, we can expect:

- Hotter summers: mean temperatures to increase by up to 4.2°C, mean daily maximum temperature to increase by up to 5.4°C, increase in the number of very hot days
- Drier summers: more frequent ten day periods without rain, amount of summer precipitation reduced by up to 40%
- Warmer winters – higher average temperatures, mean daily minimum temperature to increase by up to 2.1°C, reduction in the number of frost days.
- Wetter winters: precipitation in winter increase by up to 33% especially on the Western side of the UK, increase in precipitation on wettest days up to 25%
- No obvious change in annual rainfall but a significant change in distribution of precipitation between summer (lower) and winter (higher)
- Sea level rise: between 12 and 76cm to 2095 before land movements are taken into account (±10cm). Seasonal mean and extreme waves are projected to increase by up to 1m in some areas (though decreasing in other areas). Projected increases in storm surge heights are expected to be small.
- While an increased incidence of storms and extreme weather events is generally considered likely it has not been possible to model this.

Specific issues relevant to ICT include (but are not restricted to) longer sustained periods of hot weather, greater temperature extremes, higher humidity, more rapid changes in temperature and humidity, greater incidences of pluvial, fluvial and coastal flooding[4], changes to precipitation

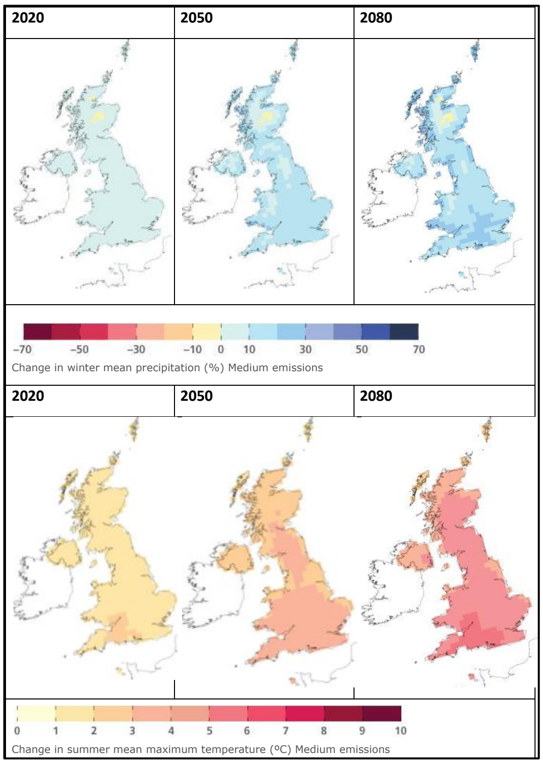
[4] Pluvial flooding comes from heavy, prolonged, or highly concentrated rainfall when the surface water simply has nowhere to go. It is exacerbated by impermeable surfaces which is why in many places planning permission is needed to pave driveways. Fluvial flooding is from rivers and streams which cannot contain the flow levels and burst banks. Coastal flooding occurs from any, or a combination of, very high tides, a strong onshore wind and sea level rise. Pluvial flooding is the hardest to predict, but tends to be shortest-lived.

patterns including an expectation of heavier downpours and larger droplet size, higher wind speeds and increased likelihood of lightning strike.

Changes of particular concern for ICT infrastructures are increased winter precipitation with associated risk of flooding (fixed line access networks and data centres) changes in mean summer temperatures with associated impacts on sustained high temperatures, temperature and humidity variations (exchanges and data centres). The UKCP09 maps for these are reproduced below.

UKCP09 probabilistic climate projections for the UK

(Scenario chosen: Medium emissions scenario, central estimate, 50% probability)
Source: **http://ukclimateprojections.metoffice.gov.uk/21731**


2020
2050
2080
−70
−50
−30
−10
0
10
30
50
70
Change in winter mean precipitation (%) Medium emissions
2020
2050
2080
0
1
2
3
4
5
6
7
8
9
10
Change in summer mean maximum temperature (ºC) Medium emissions

Rationale for choice of impacts
The impacts we have chosen to illustrate in detail are increased winter precipitation and increased mean summer temperatures since these present the most serious risks to our infrastructure, as demonstrated by recent incidents. A cursory review of publicly reported incidents makes it clear that winter flooding has posed the vast majority of the weather related problems that the sector has had to address, and that this has primarily affected local communications infrastructure (including local exchanges and network sites). To date however, we have struggled to find evidence of weather related incidents attributable to climate change that have compromised our core communications networks or commercial (colocation) data centres in the UK in the last ten years.

Rationale for choice of model
We have chosen the medium emissions scenario and also the central estimate because we view this as most probable and also because this appears to be the most common combination chosen by other infrastructure providers with whom we compare notes, it provides a common basis on which to compare resilience strategies, which would be more difficult had we all chosen different scenarios.

Observations
Unless there are reasons why this might adversely affect adaptation planning, we suggest that government recommend a standard combination of scenarios. Although we know that operators make extensive use of Environment Agency flood risk mapping (see below) we do not have evidence that they are making systematic use of these probabilistic scenarios to inform standards development or future planning (see below). Further work is needed to assess to what extent this information informs relevant decision making processes within the sector.

3.2 Environment Agency Data relevant to sector resilience

The Environment Agency is responsible for fluvial and coastal flooding, and has been mapping, modelling and managing flood risk for many years. The EA also responds to flood incidents, liaises with other stakeholders to improve resilience and comments on development proposals. The EA also does some surface water modelling. The EA is a primary source of flood risk data for insurers, solicitors (doing conveyancing), developers, consultants and the public. Data is location specific but not property specific. The EA provides advice on how that data should be used and its strengths and limitations. Information includes:

- Historic flood data (over 11,000 records) and historic flood event outlines
- GIS based risk of flooding from rivers and sea, free of charge and accessed through the Geo Store / Data share website. It shows probability of flooding from rivers and sea on a 50x50m grid in four probability bandings: High: 3.3% (1 in 30 year), medium: 1% to 3.3% (1 in 30 year to 1 in 100 year), Low: 1% to 0.1% (1 in 100 year to 1 in 1000 year) and Very Low: below 0.1%. Properties at higher risk than 1 in 75 years are also identified.
- Flood maps for planning which show details of flood risk taking defences into account and in a worst case scenario without defences. In high risk areas more detailed information and scenario modelling is available via local offices.
- The EA monitors condition of flood defences and takes this into account in modelling.
- Since December 2013 the EA has also published surface water maps which include direction of flow, velocity and depth. Bandings are based on the same probabilities as the Risk of Flood maps.
- Live flood warnings and alerts.

3.3 How are we making use of available data?

As an industry association we have socialised our members with relevant information sources through our Risk Radar series of workshops and associated briefings but anecdotal evidence suggests that not all operators are making use of the full suite of data available. The sector also appears to make only limited use of the probabilistic modelling of medium to long term changes to the UK's climate provided by UKCIP. Operators tend to focus on environment agency Risk of Flood mapping and modelling which they make extensive use of. The "blue" Risk of Flood / flood zone maps are very familiar across the sector and are used by developers, investors, insurers, purchasers and customers as well as operators. There is particular emphasis on the use of this data to direct choice of location and at planning, design and development stage.

We have questioned the data centre sector about the frequency with which this information, particularly the Risk of Flood mapping, is revisited. This seems to be very variable: some operators revisit this risk as part of their resilience planning. Others are required to do so by their insurers who request that flood risk is revisited annually. This information is generally required by default if a facility is being sold or if new investment is sought and it is also frequently seen as a requirement for bid proposals especially for large contracts or for contracts for large organisations. Standards used within the sector also require regular reappraisal of these risks (see EN 50600 and ISO 31000 below). That said, we do not yet have evidence that this data is revisited systematically by all operators. This is an area that we have identified as requiring further work and we will revisit it later.

4 Impacts of climate change on ICT infrastructure

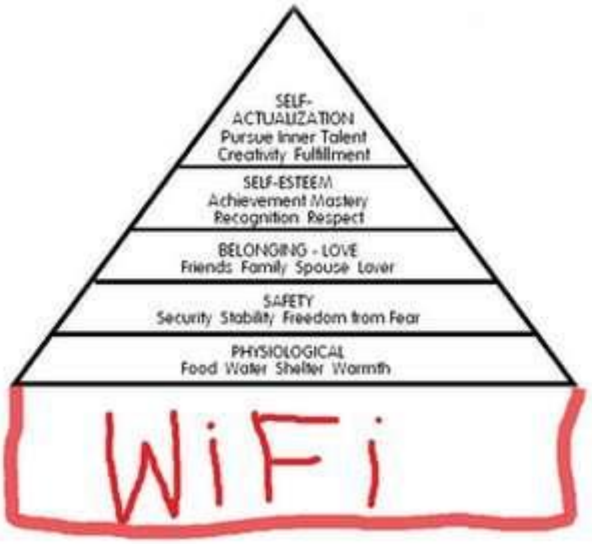
4.1 General observations on the nature of ICT infrastructure

ICT infrastructure underpins the digital economy. However virtual an application or activity may be, it still relies on physical infrastructure. The cloud is not a cloud; it is a data centre with high bandwidth connectivity. ICT infrastructure differs from other physical infrastructures in several ways. In terms of adaptation and resilience, ICT has a number of advantages that make it able to respond rapidly to changing requirements and robust to disruption. These include:

- Relatively short asset life: ICT infrastructure assets tend to have shorter lifetimes than those of other infrastructures. Communications infrastructure assets, however, have very variable life expectancies.
- Rapid pace of technological development and innovation gives the sector an inherent advantage in responding to change.
- The fact that ICT infrastructure comprises multiple systems interoperating – fixed line networks, mobile, satellite and broadcast, so there is natural redundancy.
- The sector competes on availability and continuity of service: resilience is part of a data centre's DNA.
- Built-in redundancy: ICT infrastructures tend to have built-in redundancy because digital services can be delivered using a variety of means: these include multiple fixed line routes, plus modular or cellular routes, plus a range of wireless alternatives using different parts of the radiofrequency spectrum.
- The tendency to consolidate and outsource IT function – for instance in purpose built data centres. These are designed for exceptional levels of resilience that cannot be achieved in normal business premises.
- The ability to innovate around problems or challenges is a particular characteristic of this sector.
- ICT is less dependent on other sectors than other infrastructures (ICT is dependent on 7 other sectors, transport on 16, energy on 17)[5]

On the other hand, ICT infrastructures have some disadvantages:

- ICT is highly dependent on the energy sector as ICT functions require electricity. As the digital economy develops, other infrastructures will become increasingly dependent on ICT and these mutual interdependencies increase the risk of cascade failures.
- Individuals and businesses are highly dependent on ICT and as a result any disruption to ICT enabled services has a significant impact. The internet meme pictured here represents a digital age interpretation of Maslow's Hierarchy of Needs. It may be tongue in


SELF-ACTUALIZATION
Pursue Inner Talent Creativity Fulfillment
SELF-ESTEEM
Achievement Mastery Recognition Respect
BELONGING - LOVE
Friends Family Spouse Lover
SAFETY
Security Stability Freedom from Fear
PHYSIOLOGICAL
Food Water Shelter Warmth
WiFi

[5] AEA 2009

cheek but it underlines our heavy reliance on connectivity.

- Complexity: the ICT sector is highly complex in terms of technology, the asset base and the sheer number of stakeholders across the business ecosystem. This means that interactions and sub-sector interdependencies may not always be obvious and some interdependencies may be indirect.

4.2 Changing vulnerabilities

- ICT infrastructures change rapidly and as such present a moving target in terms of vulnerability. A new asset may present an entirely new set of vulnerabilities. Within fixed line communications the asset base is changing dramatically from copper wire to fibre to the cabinet. The retention of copper between cabinet and home will result in a hybrid network that will retain some of its old characteristics and acquire some new ones.
- Copper and fibre have different vulnerabilities, depending on the type of risk. A copper cabinet, once flooded, is more likely to recover after drying out but a fibre cabinet is more likely to suffer catastrophic damage due to failure of the electronic circuitry inherent in a fibre solution. FTTC will therefore have different vulnerabilities to FTTH.
- The distribution of assets is changing due to demographic changes. Customers dictate where services have to be rolled out. As mentioned above, if those locations are high risk then the assets too will be high risk and steps have to be taken to make them less vulnerable.
- Our dependence on ICT and communications assets has dramatically increased. ICT is now pervasive. Fixed line assets now underpin business, government services, online shopping, flexible working, social networking and banking to name a few: we are now a network-enabled society heavily dependent on broadband connectivity
- Interdependence between different infrastructures are changing and the level of interdependency is growing rapidly - e.g. as smart grid is rolled out the energy distribution infrastructure will be increasingly dependent on ICT. So ICT is dependent on energy which is increasingly dependent on ICT, and so on. These circular vulnerabilities need scrutiny.
- Climate change mitigation activities also have an impact on the level of resilience. The move away from fossil fuels towards increased renewables will introduce new vulnerabilities to energy supply in the UK. We are aware that the RESNET project explored this topic but not what its findings were.
- With global connectivity expanding all the time, digital data is probably the most mobile commodity on earth, so some of the UK's ICT capability is located abroad.
- Developments in technology for servers and other hardware mean that newer equipment has higher tolerances for variations in temperature and humidity and the envelope for reliable operation is growing. Official standards produced by ASHRAE (see below) set the thresholds.

4.3 Physical impacts

See table 1 below for a summary of the impacts of climate change on ICT infrastructure

Table 1: Impacts	Data Centres	Fixed Line Telecoms	Mobile Telecoms
Coastal flooding erosion, inundation by salt water, increase in salt spray	Flooding of exposed infrastructure, damage to cabling, scour damage to foundations, subsidence, cabling exposed or damaged, salt damage to materials. Problems with emergency access for engineers.	Flooding of exposed infrastructure, damage to cabling, scour damage to foundations, subsidence, cabling exposed or damaged, salt damage to materials and equipment. Problems with staff access and safety.	Flooding and salt water damage to expose infrastructure – cabling and underground ducting and cabling. (Masts and base stations usually positioned on high ground but base stations may occasionally be flooded. Problems with staff access and safety.
Fluvial flooding (erosion, inundation by fresh water, silt and sewage deposit)	Flooding, silt and sewage, water ingress and/or damage to heavy plant and switchgear, erosion and scour of cabling and buildings. Problems with emergency access for engineers.	Scour of cabling, flooding of ducting, underground cables, cabinets and access points. Water damage to assets, silt damage, disruption to fleet operations. Problems with fleet operation and emergency access.	Flooding of ducting, water damage to cabling and hardware, scour damage to buildings, exposed cabling. Occasional flooding to base stations, silt and sewage deposit. Problems with fleet operation and emergency access.
Pluvial flooding (flash floods, inundation of localised area	Flooding of facilities. Heavy plant and switchgear disabled, damage to cabling, water damage to other hardware. Problems with emergency access for engineers.	Water damage and flooding to exchanges, cabinets, ducts, exposed infrastructure below and above ground. Disruption to fleet operation and emergency crew access.	Flooding and water damage in exchanges, ducts, exposed infrastructure below and above ground. Disruption to fleet operation and emergency crew access.
More rain, Heavier rain, larger droplets	Not significant, no known incidences	Greater penetration into cabinets, damage to connection points such as tops of poles. Higher groundwater may change shear strength of substrate and reduce pole stability.	Mobile signal can be affected by rain (rain shading). Mainly a problem above 10GHz. Connectivity may be reduced. Possible penetration into exposed base stations. Higher groundwater may change shear strength of substrate and reduce mast stability.
Sustained high summer temperatures	Poor working conditions for staff. Some legacy sites may struggle to maintain required temperature or avoid hot spots. May compromise some activity if cooling cannot be maintained. Cooling costs may increase for other facilities.	Maintaining safe working conditions in exchanges etc. Component failure, ICT equipment failure, especially legacy kit (NB: Newer equipment has higher temperature and humidity tolerances)	Maintaining safe working conditions in exchanges, component and equipment failure in base stations.
Increased rapidity of temp change	Higher HVAC (Heating, Ventilation, Air Conditioning) costs. Stress on components and hardware	Stress on components and hardware. Shorter in-service life.	Stress on components and hardware. Shorter in-service life.
increased humidity	More active humidity management required. higher risk of damage to hardware, may affect reliability and life expectancy.	Damage to exposed assets. Shorter in-service life.	Damage to components and ICT hardware and supporting equipment. Can speed up degradation and affect reliability
increased storminess - wind and lightning	Not significant unless power, comms or transport links affected- second tier effects.	Cable heave (tree roots, etc.) scour, aerial parts of network at risk – poles particularly and wires.	Cable heave, cables exposed from scour, aerial parts exposed, tower and masts subject to damage, microwave dishes displaced or misaligned
Drought	Access to cooling water for water cooled facilities. Subsidence	Subsidence of fixed assets, fractured ducts.	Subsidence, fractured ducts.

4.4 Other impacts

Climate change impacts are not limited to asset failure. Each asset failure generates a number of secondary impacts, on operations, on customers, on staff, on reputation and on cost. The more significant the failure, the greater the ripple effect. Within the industry resilience tends to mean the ability to deliver service and meet service level agreements. For instance data centres can be graded according to standardised availability classes and this availability is a measure of that data centre, in terms of its core functionality – power, security, connectivity, etc., being available to enable its customers to provide services to their customers and their customers to provide services to their customers and so on. Data centres and communications operators are all service providers and so most of the following points will be true across the whole ICT infrastructure.

- Impacts on customer service: Failing to provide guaranteed services to customers is the thing that keeps data centre operators awake at night. Failure to meet customer SLAs (service level agreements) is another major concern, for instance failing to keep the operating environment within the agreed limits of temperature and humidity.

- Cascade impacts: Communications and digital infrastructures underpin most economic activity and so an interruption in service has significant consequences for business activity. Consequent costs for a large bank unable to complete any transactions or the potential impact of air traffic control being suspended are examples. Commercial colocation providers compete to a large extent on their ability to provide a continuously available service that supports their customers' business continuity, and that of their customers' customers.

- Reputational damage: UK data centres tend to be focused on business customers whereas communications providers are focused on both business and consumer markets. Whilst, therefore communications providers tend to be household names in a way that data centre operators are not, reputational damage is a major issue for both. The failure to provide a customer with a service critical to their business continuity would be deemed very damaging to an operator.

- Costs: Climate change risks can result in significant unbudgeted costs. These could perhaps be categorised as acute or chronic. Acute cost would include responding to incidents and doing remedial work following breaches, or repairing storm or flood damage to physical assets. Chronic costs include additional costs for environmental management controls. For example, cooling data centres is expensive and while modern data centres use free air cooling, extra cooling will add cost. For widely spread infrastructures like the access network, ensuring readiness for wide scale flooding or a long period of exceptional rain, as was seen in 2012, is extremely costly: while equipment can be stored, having enough trained staff for all contingencies, or bringing enough human resource online in times of need, are extremely challenging.

- Pressure on fault reporting: When teams are particularly stretched, companies will experience high volumes of calls to helplines and fault reporting.

- Working conditions, staff wellbeing and safety: during flooding staff they may have to do long hours of overtime and sleep in improvised accommodation on site or work in difficult conditions.

- Resources diverted from scheduled activities: When resources, especially staff, have to be deployed in emergency, this often has a knock-on effect on scheduled work, which may be delayed.

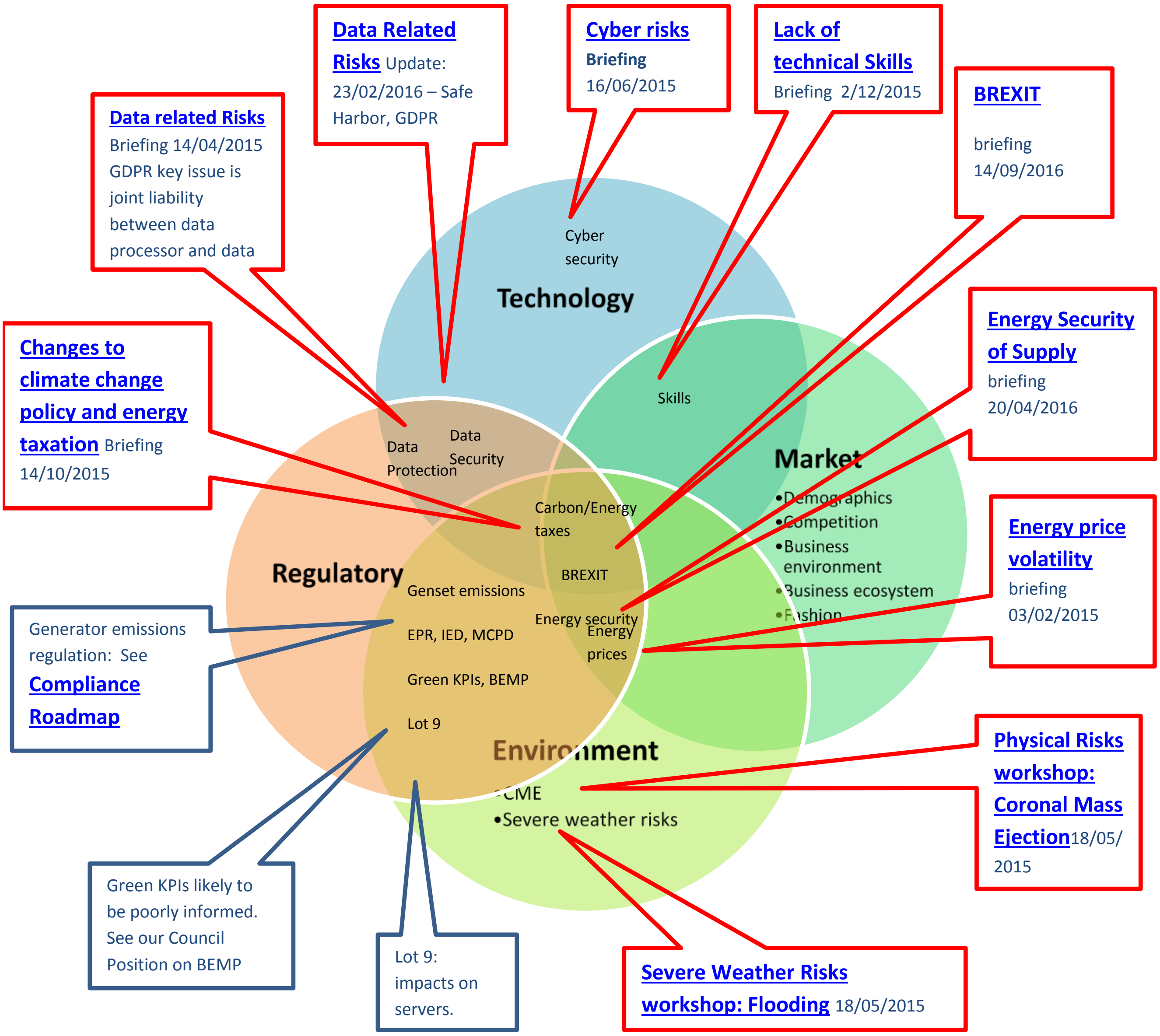
- Difficulty in meeting regulatory obligations: in sectors regulated by Ofcom (mobile and fixed line telecoms) operators may be subject to incompatible obligations. Price constraints, the obligation to connect properties (other than those deemed hard to reach) irrespective of whether they are in flood zones, and a regulatory obligation to provide resilience are likely to prove mutually exclusive. In some cases the Universal Service Obligation (See Annexe i) for fixed line may limit an operator's ability to manage risk cost effectively.

5 How do we manage climate change risks in digital infrastructure?

Section summary: *In this section we explain why climate change is classed as a business risk just like any other. This is a tricky section for us because unlike most organisations submitting ARP reports, we are writing on behalf of dozens of providers. Risks are managed at organisation level rather than at sector level and we are not party to individual corporate risk planning strategies. So we can provide generalisations but what we say will not be true in all instances. We look at the kind of practices that are adopted and explore the role of industry standards and other formal tools.*

5.1 Climate Change is a Business Risk

Climate change is a business risk and sits within the wider risk landscape. The illustration is from our Risk Radar series of briefings for data centres



Data Related Risks Update: 23/02/2016 – Safe Harbor, GDPR

Cyber risks Briefing 16/06/2015

Lack of technical Skills Briefing 2/12/2015

Data related Risks Briefing 14/04/2015 GDPR key issue is joint liability between data processor and data

BREXIT briefing 14/09/2016

Changes to climate change policy and energy taxation Briefing 14/10/2015

Energy Security of Supply briefing 20/04/2016

Energy price volatility briefing 03/02/2015

Generator emissions regulation: See **Compliance Roadmap**

Physical Risks workshop: Coronal Mass Ejection18/05/2015

Green KPIs likely to be poorly informed. See our Council Position on BEMP

Lot 9: impacts on servers.

Severe Weather Risks workshop: Flooding 18/05/2015

5.2 Managing climate change risk in data centres

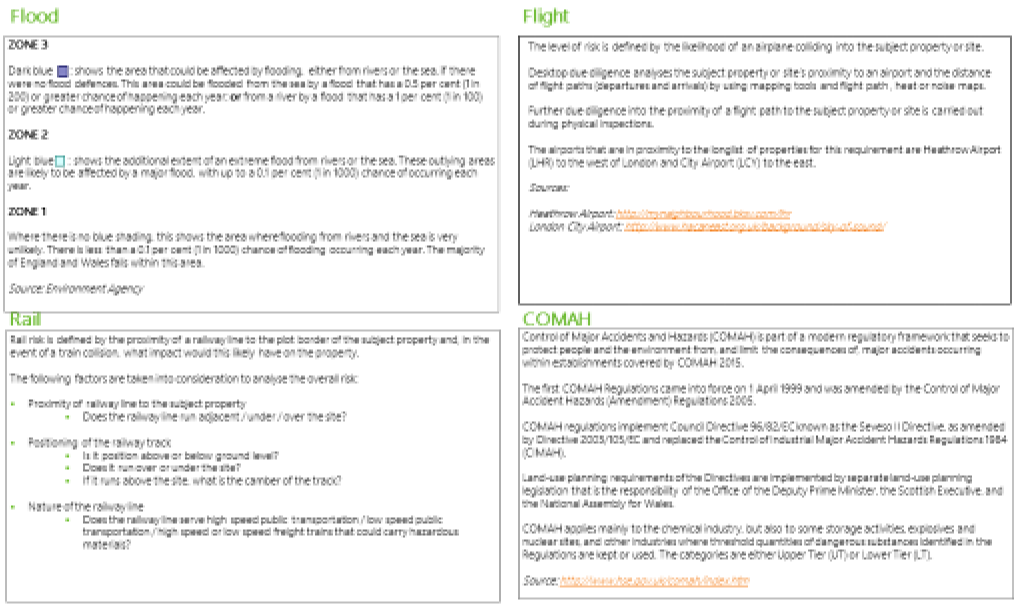
As with all other types of infrastructure, risk is managed at two stages: build stage and operational stage. Because data centres are relatively recent features in the UK landscape, and the sector is growing rapidly to service the digital economy including the rapid digitisation of government services, business processes and social activity, data centre infrastructure are growing. Most other infrastructures are dominated by legacy systems that have to be adapted and retrofitted. Our ICT infrastructure does depend on legacy systems but there is also a lot of new build. This presents an opportunity to ensure that new capacity is appropriately protected from emerging risks like climate change.

Build stage

Data centre buildings are designed for a life of about 50 years, the mechanical and engineering plant is designed for perhaps 25 years, other hard infrastructure like cabling may have a design life of 10-15 years, and the IT that is the productive part of the data centre business may have a design life of 18 months. These figures are indicative only: the main point is that design has to accommodate wide variations in in-service life expectancy of physical assets.

Flood risk is at the top of the list of geographic factors that data centre operators take into account when choosing a location. Although there are no formal published standards for this, advisors, brokers and consultants give very consistent advice, that a location with a flood risk above 1 in 1000 is undesirable. See below a typical risk analysis relating to site selection.

Sample site search risk analysis



Flood

ZONE 3

Dark blue ▨ : shows the area that could be affected by flooding, either from rivers or the sea, if there were no flood defences. This area could be flooded from the sea by a flood that has a 0.5 per cent (1 in 200) or greater chance of happening each year, or from a river by a flood that has a 1 per cent (1 in 100) or greater chance of happening each year.

ZONE 2

Light blue □ : shows the additional extent of an extreme flood from rivers or the sea. These outlying areas are likely to be affected by a major flood, with up to a 0.1 per cent (1 in 1000) chance of occurring each year.

ZONE 1

Where there is no blue shading, this shows the area where flooding from rivers and the sea is very unlikely. There is less than a 0.1 per cent (1 in 1000) chance of flooding occurring each year. The majority of England and Wales falls within this area.

Source: Environment Agency

Flight

The level of risk is defined by the likelihood of an airplane colliding into the subject property or site.

Desktop due diligence analyses the subject property or site's proximity to an airport and the distance of flight paths (departures and arrivals) by using mapping tools and flight path , heat or noise maps.

Further due diligence into the proximity of a flight path to the subject property or site is carried out during physical inspections.

The airports that are in proximity to the longlist of properties for this requirement are Heathrow Airport (LHR) to the west of London and City Airport (LCY) to the east.

Sources:

Heathrow Airport: [illegible]
London City Airport: http://www.hacaneast.org.uk/background/city-of-sound/

Rail

Rail risk is defined by the proximity of a railway line to the plot border of the subject property and, in the event of a train collision, what impact would this likely have on the property.

The following factors are taken into consideration to analyse the overall risk:

- Proximity of railway line to the subject property
    - Does the railway line run adjacent / under / over the site?
- Positioning of the railway track
    - Is it position above or below ground level?
    - Does it run over or under the site?
    - If it runs above the site, what is the camber of the track?
- Nature of the railway line
    - Does the railway line serve high speed public transportation / low speed public transportation / high speed or low speed freight trains that could carry hazardous materials?

COMAH

Control of Major Accidents and Hazards (COMAH) is part of a modern regulatory framework that seeks to protect people and the environment from, and limit the consequences of, major accidents occurring within establishments covered by COMAH 2015.

The first COMAH Regulations came into force on 1 April 1999 and was amended by the Control of Major Accident Hazards (Amendment) Regulations 2005.

COMAH regulations implement Council Directive 96/82/EC known as the Seveso II Directive, as amended by Directive 2003/105/EC and replaced the Control of Industrial Major Accident Hazards Regulations 1984 (CIMAH).

Land-use planning requirements of the Directives are implemented by separate land-use planning legislation that is the responsibility of the Office of the Deputy Prime Minister, the Scottish Executive, and the National Assembly for Wales.

COMAH applies mainly to the chemical industry, but also to some storage activities, explosives and nuclear sites, and other industries where threshold quantities of dangerous substances identified in the Regulations are kept or used. The categories are either Upper Tier (UT) or Lower Tier (LT).

Source: http://www.hse.gov.uk/comah/index.htm

However, risk is only one of several location factors for data centres. Others include power and connectivity. It is often tricky to meet all requirements and in some cases a slightly higher flood risk might be deemed acceptable provided that this risk is understood and mitigated.

While data centre operators within our membership make use of up-to-date flood mapping information from the Environment Agency regarding fluvial flooding and coastal flooding, we are not yet convinced that the sector at large is as aware of, or using effectively, all the information sources at hand. We have yet to establish what proportion of operators or consultants are making use of the newer datasets on pluvial and surface water flooding. Since data centres are generally located in urban areas where the percentage of impermeable surface materials may be high, this suggests that we could do more to raise awareness of the full range of information sources available to the industry. We will revisit this later.

Data centre operations rely on power and connectivity (very high bandwidth communications) so they are designed for failures in provision of both services. Data centres use UPS (uninterrupted power supplies) to ensure continuous power to the facility, in conjunction with batteries, flywheels and generators. These deal with instantaneous loss of supply and longer term outages. Data centres are often built incrementally with new data halls being fitted out in response to customer demand. Stand-by power is generally increased in line with the site power demand as that increases and is not necessarily a reflection of the power provisioning of the site. This is an important distinction: power provisioning is the maximum instantaneous power supply to that site and operators tend to over-provision sites in order to future proof their activity. So many sites operate well below the maximum power provisioned and generator backup function is matched to the maximum power that a site is likely to consume based on its current level of activity and not the maximum power that can be supplied. So, simplistically, the power backup is matched to the function of the site, not to the capacity of the site.

Generators can theoretically work when immersed, provided that the fuel supply, air intake and exhaust are clear. This has important implications for emergency planning: a flooded site can remain operational in the event of a mains failure. Emergency plans will include a move to generator power before the electricity has been isolated to ensure a managed transition rather than an emergency response.

Not all data centres need highly resilient power. Some do not perform mission critical functions so all they need in the event of power failure is enough back up supply to shut down safely without data loss. This is reflected in the design which would not include generators. Standby power would be provided in the form of batteries that are kept fully charged. These will be a familiar sight in server rooms within office premises. Most organisations split their provision and may keep externally facing activity via third party colocation or cloud providers whilst maintaining more mundane office functions in house. It is increasingly common, with the growth in cloud offerings and the flexibility of pay-as-you-go cloud provision, for companies to outsource their IT function in this way.

Operational

As mentioned above, data centre operators compete on resilience with the ultimate objective of avoiding any outages – or achieving “0% downtime”. Increasing resilience does add cost, so the more resilient a data centre is, the more expensive it is to operate and the charges to customers usually reflect this. Whilst all operators aim at 0% downtime, there is nevertheless a market for resilience that loosely (but by no means universally) reflects the criticality of the data that is being managed or the value of the services that are being provided. So downtime for a batch processing or social media site would have a less significant impact than downtime for transactional activity for a large bank, or for air traffic control.

Operational resilience is achieved in a number of ways and is not limited to physical protection. Hot standby and warm standby were discussed above and are applied in data centres although the terminology varies. Hot standby involves mirrored facilities less than about 30km apart which can be synchronised live and where functionality can be moved across pretty much seamlessly. Other mirrored facilities ("mirrored" means that activity is duplicated between two sites) may be further apart. Operators set their own criteria: for instance one operator requires its mirrored sites to be about 100 miles apart, others might look at the infrastructure and locate the back-up facility on a different part of the electricity transmission or distribution network. In general data centres have access to disaster recovery facilities that are ready to receive an entire operation if it suffers partial or catastrophic failure. Some operators provide disaster recovery as a commercial service to third parties.

Standards and risk management tools (data centre specific)

Although the sector does not have a bespoke standard for climate change resilience, relevant standards and best practices exist, and are widely referred to, within the sector.

EN 50600 TR Availability Classes

The EN 50600 series is a set of data centre standards developed by international standards body CENELEC. CENELEC is internationally recognised, vendor agnostic, not for profit and peer reviewed. The EN 50600 series is made up of multiple components. EN 50600-1 covers general requirements and availability classes. EN 50600-2-2 focuses on power supply and distribution. EN 50600 2-3 is focused on environmental controls. Others deal with telecommunications and security. The following extract from "Data Centre Assessment vs Certification" explains this in more detail:

- EN 50600-2-2 defines four levels (1 to 4) for the design availability of the power supply and distribution system of the data centre;
- EN 50600-2-3 defines four levels (1 to 4) for the design availability of the environmental control system of the data centre;
- EN 50600-2-4 defines four levels (1 to 4) for the design availability of the telecommunications cabling systems of the data centre;
- EN 50600-1 defines the overall availability level of a data centre based on the lowest level of three infrastructures detailed above.
- EN 50600-2-5 defines requirements for the maintenance of physical security of data centre spaces independent of the infrastructure level.

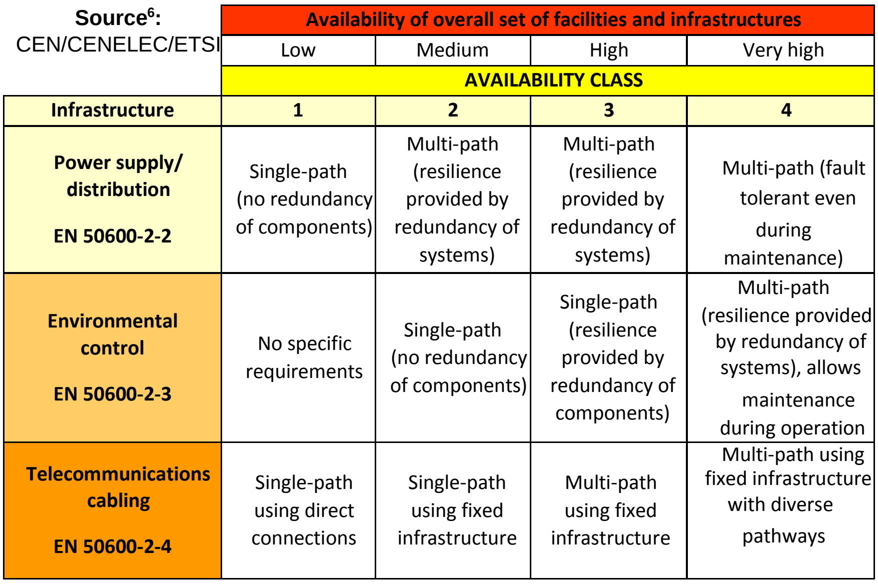
In this way EN 50600-1, -2-2, -2-3, -2-4 and -2-5 provide a comprehensive framework for assessment of the design availability of a data centre. They are supported by EN 50600-2-1 and EN 50600-3-1 for building construction and operation respectively but these are currently treated as subsidiary to availability objectives.

Availability classes

Availability (*A*)	Common reference	Downtime (based on a 365 year)
90 %	1-nine	36,5 days
99%	2-nines	3.65 days
99.9% (3-nines)	3-nines	8,76 hours
99.99% (4-nines)	4-nines	52,6 minutes
99.999% (5-nines)	5-nines	5,3 minutes
99.9999% (6-nines)	6-nines	31,5 seconds

While not focused exclusively on climate change risks, the resilience of a data centre facility is assessed against four classes of availability (see figures). Within the industry, data centre availability tends to be described in terms of a percentage. So it is common to see descriptions of 99.999% (or "five nines" availability – see figure. What this means is that the data centre is designed and operated to ensure an absolute maximum of 5 minutes of down time in a year. Generally it has none. The EN 50600 series assesses the availability of the data centre infrastructure as opposed to the availability of the data centre function and this is an important distinction that has recently been clarified. More detail is supplied in Annexe IV.

A data centre with Class I availability would probably have a single power supply, a single communications connection and enough battery power to allow it to shut down safely in the event of a power cut. A class 4 facility would have three separate sources of power – most likely two separate grid supplies and one generator or vice versa. In terms of communications there would be diverse routed fibre backbones with multiples paths to devices enabled to receive multiple inputs (See chart).



Source[6]: CEN/CENELEC/ETSI	Availability of overall set of facilities and infrastructures			
	Low	Medium	High	Very high
	AVAILABILITY CLASS			
Infrastructure	**1**	**2**	**3**	**4**
Power supply/ distribution **EN 50600-2-2**	Single-path (no redundancy of components)	Multi-path (resilience provided by redundancy of systems)	Multi-path (resilience provided by redundancy of systems)	Multi-path (fault tolerant even during maintenance)
Environmental control **EN 50600-2-3**	No specific requirements	Single-path (no redundancy of components)	Single-path (resilience provided by redundancy of components)	Multi-path (resilience provided by redundancy of systems), allows maintenance during operation
Telecommunications cabling **EN 50600-2-4**	Single-path using direct connections	Single-path using fixed infrastructure	Multi-path using fixed infrastructure	Multi-path using fixed infrastructure with diverse pathways

The objective of EN 50600 is not to be too prescriptive in terms of requirements. So it does not set a risk threshold for data centres or require, for instance that no data centres are located in flood zones. There might be very good reasons for locating a data centre where the flood risk is slightly higher than is desirable. Instead, it focuses on mitigating and managing those risks. The standard also covers ongoing risk management and EN 50600-3-1 requires operators to have management procedures in place that ensure the risk assessment is ongoing. This is very important and we will revisit this point.

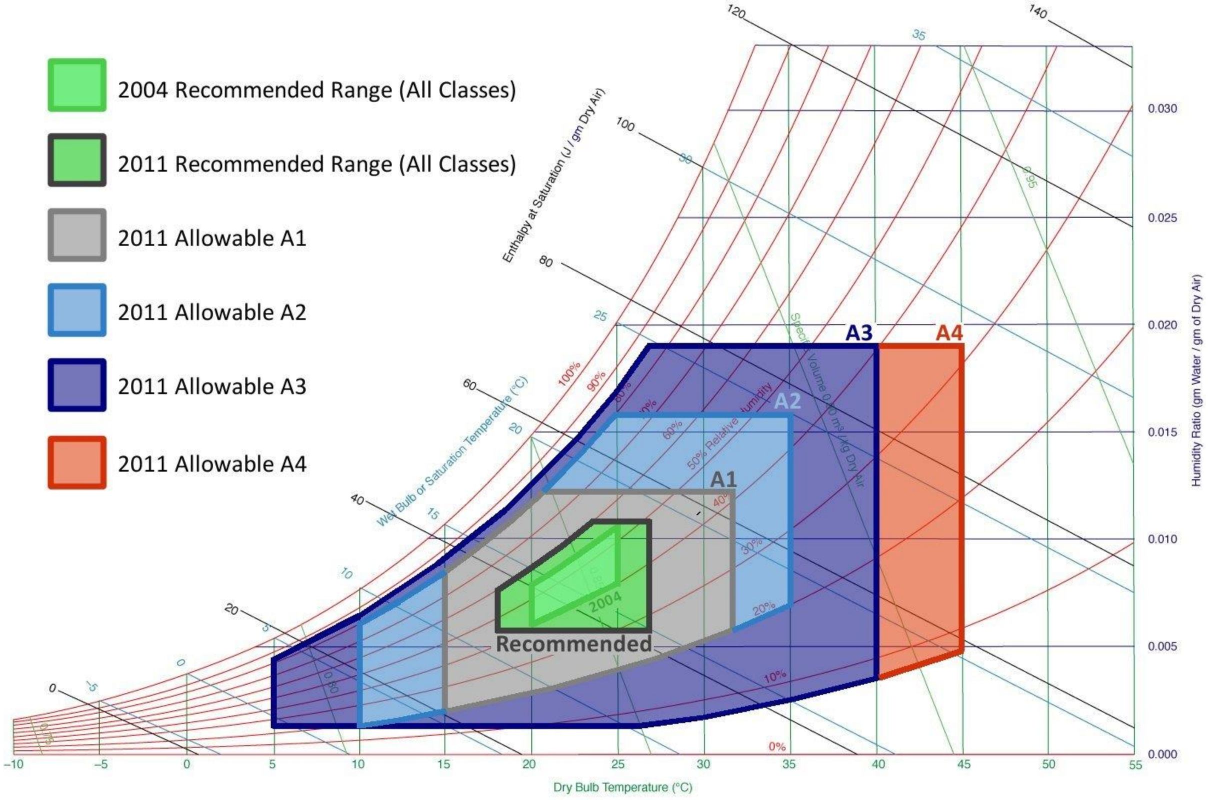
The 50600 series is widely recognised within the industry and although the standards were developed relatively recently and are still being rolled out, adoption is growing rapidly. There is

[6] Extracted from Review of Standardisation Activities: Energy Management and Viability of Data Centres basted on the edition 3 report of the CEN/CENELEC / ETSI coordination group on green data centres.

currently no certification process for this series but that does not mean that a data centre cannot be assessed against this standard or that the EN50600 standard cannot be used as part of the certification process against another standard such as ISO 9001, for which certification does exist.

ASHRAE

ASHRAE (the American Society of Heating, Refrigeration and Air Conditioning Engineers) standards relate to ICT equipment rather than infrastructure but they are important in an adaptation and resilience context because they define temperature and humidity boundaries for reliable operation of servers. In 2004 ASHRAE defined a common set of guidelines for operating conditions in data centres that would not invalidate the warranties provided by server manufacturers.   In 2004 the original envelope proposed was 20°C to 25°C (68-77F). In 2008 the range expanded from 18°C to 27°C (64.4-80.6F). In 2011 the envelope was challenged again and allowable operating ranges as wide as 5° to 45°C (41 to 113 F) have been considered (see the ASHRAE Psychrometric Chart below).



Source: ASHRAE/Don Beatty Associates

Uptime Institute Tier Rating

Primarily aimed at the design stage, but now with an operational option, the Uptime Institute's Tier rating system grades data centre resilience from Tier 1 (low) to 4 (high)[7].   It is not an appropriate standard or even a proxy standard for climate change resilience and is therefore not useful in this

[7] This tier rating should not be confused with tier ratings for data centre markets. A Tier 1 market means one of the prime data centre clusters. Europe's four tier 1 markets are London, Frankfurt, Paris and Amsterdam.

capacity. Observers remark that it is a costly commercial standard primarily designed for the US market and is focused more on internal aspects than on external risks that the facility might be exposed to. It therefore excludes fundamental resilience measures like ensuring security of power supply.

Generic industry standards

ISO 31000 is widely used within the data centre sector but is a generic family of standards relating to risk management (codified by the International Organization for Standardization). The purpose of **ISO 31000** is to provide principles and generic guidelines on risk management. There is no certification process, this is guidance only.

ISO 22301

ISO 22301 is another generic standard not specific to data centres but widely used within the industry and increasingly being specified in tender requirements and bids. Again it is codified by the International Organisation for Standardisation and is effectively the internationally recognised standard for business continuity. There is a certification process so operators are audited against it by accredited external auditors.

Sarbanes Oxley, TIA ANSI 942 and BICSI ANSI 002 2014

Wide reference is made within the UK to other information sources and good practice guides focused on resilience and risk. These include Sarbanes Oxley, a regulatory requirement for US operators and a useful source of information, TIA ANSI[8] 942 and BICSI ANSI 002 2014. These are US good practice guides that are used widely in the UK and relate to all forms of physical risk. Although they come from a communications/cabling source they cover all aspects of data centres from design to operation. There is no certification process.

Risk management tools

We are not party to the risk management tools deployed by individual operators nor to their corporate risk management strategies but we can comment on standard practice:

Operators deploy formal risk management tools and methodologies and a sample methodology is included below. This is a common approach applied to multiple risks. The key objective is to develop understanding of the nature of the risks (e.g. type and severity of adverse weather and what impact these will have on the various elements of the site and key supporting utility/transport infrastructure). The next step is to provide senior management with a quantified understanding of the key issues, enabling them to make informed decisions about the risk levels they are willing to accept and what risk reduction/mitigation activity they need to invest in.

For the risks that are to be treated, a risk treatment plan would be developed. The risk treatment plan would normally show

1) the absolute risk level or score with no mitigation,

[8] TIA = Telecommunications Industry Association, ANSI = American National Standards Institute

2) the current level with existing controls,

3) the residual level that would be achieved when lanned improvements have been implemented. This enables senior management to periodically review/chase progress in overall risk reduction.

Sample Risk Assessment Methodology

When reviewing risk in the context of the requirements of the business, the following criteria shall be applied. Risk reviews shall be conducted by individual(s) who have appropriate knowledge and understanding of the risk / control being assessed.

Risk Scoring

Risk shall be calculated and scored by the multiplication of business impact x probability that a threat may cause the risk to materialise and will be scored as follows:

Business Impact

Impact Level	Description
5 Catastrophic	Potentially catastrophic impact upon long term business due to the non-renewal of contract and reputational damage within industry
4 Major	Major impact, immediate action required to prevent long term prospects of company being adversely affected
3 Significant	Significant impact which requires active involvement of senior staff to contain
2 Moderate	Moderate impact which can be effectively managed
1 Insignificant	Insignificant

Probability (or likelihood)

Level	Description	Indicative Frequency
5	Almost Certain (Very High)	1 in 10 years
4	Likely (High)	1 in 30 years
3	Possible (Medium)	1 in 100 years
2	Unlikely (Low)	1 in 200 years
1	Rare (Very Low)	1 in 1000 years

Risk Scoring Matrix

This Matrix is used to determine “RAG” ratings associated with risk scores generated during the risk assessment.

Impact	5 🟩	10 🟧	15 🟧	20 🟥	25 🟥
	4 🟩	8 🟩	12 🟧	16 🟥	20 🟥
	3 🟩	6 🟩	9 🟩	12 🟧	15 🟧
	2 🟩	4 🟩	6 🟩	8 🟩	10 🟧
	1 🟩	2 🟩	3 🟩	4 🟩	5 🟩
	Likelihood				

Risk Tolerance

All risks with a score of 10 or higher require treatment or formal acceptance. Risks achieving a score of less than 10 will be managed via the general operational management process of continual improvement.

Risk Acceptance Authority

Risks identified as ‘Red’ or ‘Amber’ in the Risk Treatment Plan (RTP) may only be accepted following a formal review by the Board. Risks identified as ‘Green’ in the RTP will be managed via the process of continual improvement of business as usual controls.

Emergency response planning

Individual corporate flood response plans are confidential but we have attached a list of the main elements of a sample emergency flood response plan that would be suitable for a London data centres. See Annexe iii.

We also include a sample resilience and risk scenario plan from a commercial operator providing services to government and a flood risk plan for a large commercial docklands facility. See Annexe ii.

Emergency scenario planning

While we are not party to individual corporate initiatives, operators engage in emergency planning and drills to demonstrate their capability to deliver continuous service. See the link for a sample scenario: http://archwayresilience.com/resilience-exercises

What are other people doing?

There is plenty to be learned from operators elsewhere. Comparisons have sometimes been made with the approach to protecting similar technical real estate in the Netherlands. The largest Dutch data centre park, near Schiphol, is below sea level but behind at least three physical lines of defence and data centre activity is located at or above first floor level, at 3M+. The approach of limiting ground floor activity could be applied more widely in the UK to new builds but would be problematic to apply to legacy facilities.

The Dutch “multiple lines of defence” approach has at times been compared with the Thames Barrier which has been described (erroneously) as a SPOF. Some misconceptions need to be laid to rest here. The Thames Barrier operates as three independent sections and each has three separate power sources. If an entire section failed the barrier would still perform its function of restricting water flow at times of peak movement. The barrier is not intended to be a dam.

5.3 Managing climate change risk in the fixed line telecoms network

Core network

Our core fixed line network is operated by a number of providers. The PSTN – Public Switched Telecoms Network – is operated by the incumbent provider, BT, across the UK with the exception of Hull. Other providers like Virgin Media, Vodafone, Level3 etc. operate private networks. We are not party to individual corporate risk and continuity plans but we can make some general observations. The core network is highly resilient with substantial redundancy and is comparable to the transmission network for electricity. Formal risk management tools are applied as part of an ongoing process. Risks are managed both proactively and reactively. Substantial resources are committed to research and R&D in terms of modelling, mapping, asset resilience and fault volume reduction.   BT and KCOM are the points of contact for detailed information.

Access network

The fixed line access network covers the whole of the UK. In terms of risk the access network in communications is comparable to the distribution network for electricity. The infrastructure is more vulnerable but easier to repair; ducts (and less often, poles) rather than pylons, cabinets rather than exchanges) and a given asset serves fewer people. In our view, which is in line with that expressed by the Pitt Review following the 2007 floods, it is not possible to protect the entire access network all the time from all climate change related risks and it would be counter-productive to attempt it.

Openreach operates the access network and is therefore the point of contact for information on the way climate change risks are managed within this network.

5.4 Managing climate change risk in the mobile telecoms network

NB: It is important to note at this stage that we have not conducted an extensive survey or made a systematic analysis. We have asked stakeholders and technical experts both within and outside the industry for their opinions. So far, views are very consistent.

The climate change risks to our mobile telephony network are (primarily) wind damage to towers and antennae, potential flooding or storm damage to base stations, heat in base stations and damage to underground cables through heave, slip, scour or flooding (water ingress).

Interdependencies include access to fixed line networks infrastructure, data centres and electricity. Flooding severe enough to affect transport will obviously prevent engineers reaching affected assets, particularly if they are in isolated locations.

We will look first at the design and build stage and then at the operational stage. There are obviously overlaps.

Design and Build

The most vulnerable parts of the mobile communications infrastructure are the towers, or masts (see Box 1). They carry the antennas for the compound, cupboard or building at the bottom, generally known as the base station (see above).

Mobile towers are usually made of steel latticework which is semi-permeable to air flow and performs well in high winds. There are around 27,000 towers in the UK, averaging around 17m in height. Most are built to about 15m. Elsewhere in Europe they tend to be built about 10m higher.

At the design and build stage a range of standards is applicable to construction and maintenance of towers. These are:

- BS8100 – Pts 1, 3&4 – Lattice Towers & Masts – Codes of Practice for Loading, design etc.
- BS EN1991-1-4 (Eurocode 1) – Actions on Structures PLUS National Annex
- BS EN1993(Eurocode 3) – Design of Steel Structures PLUS National Annex
- PLG07 (Monopoles)

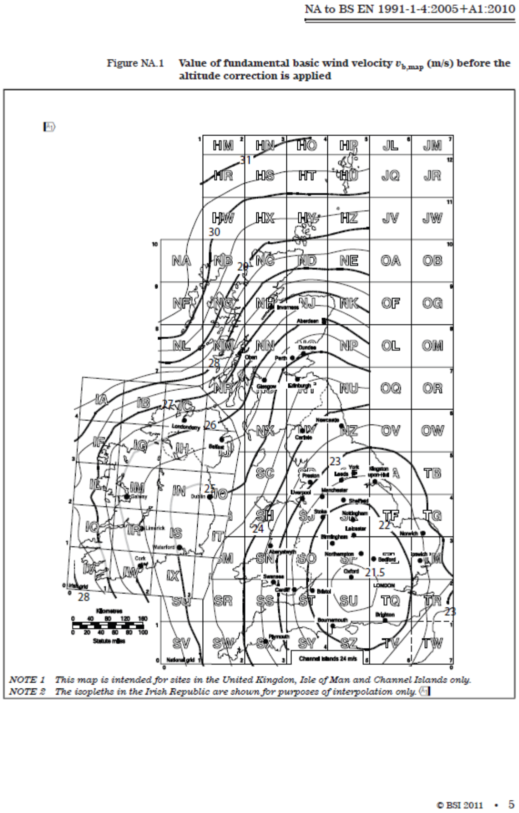
Industry respondees to our request for information observe that the Eurocodes are not fully tested and implemented and that therefore the *de facto* industry approach within the UK is to use the more recent loading data from the Eurocodes (which is more accurate because the data sample it is built from is much larger and more recent than that for BS8100 which was sampled in 1986) but refer to the superseded BS8100 to complete the analysis. The ice data in BS8100 is the same as in EN1993. The Annexes are periodically updated and re-issued as changes are made to the data.

In terms of analysis and practical application, the raw data is interpolated for the site location factored for altitude, season, orography and a multitude of other factors before being run through the calculations. In both cases the probability thresholds used for calculations and return rates is 0.02 or 1 in 50 years.

Box 1: Masts and Towers

Most towers are built by independent companies or consortia and most are shared. 1/3 are owned by a joint venture MBNE – Mobile Broadband Network Ltd, of Three and EE. About 1/3 are owned by PPIT, made up of O2 and Vodafone. Independent operators include Arqiva who have about 6000 towers and WIG, Wireless infrastructure Group, who have around 2000. Arqiva and WIG provide towers for their customers to use on a shared basis with on average about three operators per tower. Although mobile network operators (MNOs) provide the bulk of the demand there are hundreds of other wireless users who make up the rest of the customer base. These include power utilities, and power companies (some of whom operate their own private radio networks) RNLI, Maritime and Coastguard Agency and there are other forms of fixed wireless access that provide a substitute for broadband and CJV. Backhaul from masts is either by fibre or microwave links, currently about half and half. Speaking very roughly, mast service life is around 30-40 years.

Arqiva also operate the TV and radio broadcasting networks, using around 1100 masts, around 50 of which are very large structures at around 300m/1000ft. Many of the rest are repeater sites. Many masts are shared and carry microwave dishes to deliver backhaul for mobile phone companies.

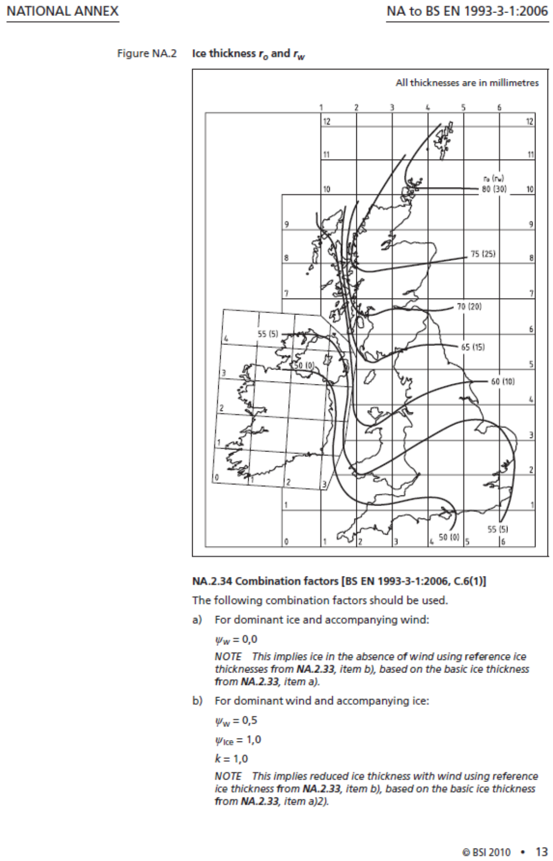


NA to BS EN 1991-1-4:2005+A1:2010

Figure NA.1 Value of fundamental basic wind velocity $v_{b,map}$ (m/s) before the altitude correction is applied

NOTE 1 This map is intended for sites in the United Kingdom, Isle of Man and Channel Islands only.
NOTE 2 The isopleths in the Irish Republic are shown for purposes of interpolation only.

© BSI 2011 • 5



NATIONAL ANNEX NA to BS EN 1993-3-1:2006

Figure NA.2 Ice thickness r_o and r_w

All thicknesses are in millimetres
r_o (r_w)
80 (30)
75 (25)
70 (20)
65 (15)
60 (10)
55 (5)
50 (0)
50 (0)
55 (5)

NA.2.34 Combination factors [BS EN 1993-3-1:2006, C.6(1)]

The following combination factors should be used.

a) For dominant ice and accompanying wind:

$\psi_W = 0,0$

*NOTE This implies ice in the absence of wind using reference ice thicknesses from **NA.2.33**, item b), based on the basic ice thickness from **NA.2.33**, item a).*

b) For dominant wind and accompanying ice:

$\psi_W = 0,5$

$\psi_{Ice} = 1,0$

$k = 1,0$

*NOTE This implies reduced ice thickness with wind using reference ice thickness from **NA.2.33**, item b), based on the basic ice thickness from **NA.2.33**, item a)2).*

© BSI 2010 • 13

Incidents caused by high wind: : The most significant wind related incident was back in the 1960s when the Emley Moor Transmitter, a tubular steel broadcasting mast supported by stay wires, became iced up and fell in high winds. The engineering design had not accommodated the weight of the ice combined with the force of the wind. That was considered to be an extreme event but the replacement structure is concrete, to appease local anxieties. TV signal was restored to 2.5 million people within 4 days.

Wreckage: (photo: Gerald England, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=7479129)

New transmitter (photo Arqiva)

Lightning: All towers have lightning conductors and incidents of lightning damage to antennas seem, from anecdotal evidence, to be very rare. The only vulnerabilities identified relating to lightning were due to copper theft from towers when the conducting metal was stripped off by thieves. Changes in rules over metal recycling have improved matters.

Heat and humidity: The base stations are generally not air conditioned and therefore some are vulnerable to sustained high temperatures that may cause equipment or components to fail. Air conditioning may be retrofitted but equipment is also being manufactured to withstand much greater variations in humidity and temperature[9] and so in some cases the natural refresh cycle for equipment will reduce, but not eliminate, this risk.

Operational Risk Management

In term of managing risk when the system is operational, anecdotal evidence suggests that approaches vary and there is less consistency in terms of standards and processes that we see at build or installation. Airwave (now owned by Motorola) provides a dedicated network for the emergency services and is considered informally to have the most “gold plated” system because emergency services connectivity demands a high level of infrastructure investment, especially in resilience. This system will be migrating from Airwave onto EE’s 4G network in 2017. EE is in the process of implementing upgrades to the network to improve resilience, for instance installing alternative emergency power supplies at base stations.

Commercial providers who offer services to operators and other wireless infrastructure users appear to take a proactive and systematic approach to managing these risks. Rather like commercial data centres, where resilience is the product, for independent mast providers a functioning mast is the primary product, so this is to be expected. Elsewhere in the network there will be instances where climate change related risks are managed more reactively. As mentioned earlier, regulatory pressure seems to be a root cause: competition has been driven very strongly around affordability and prices for consumers rather than around quality of supply, which means that margins are so low that the infrastructure will, of necessity, be very efficient and have little built-in redundancy.

A sample approach from a commercial provider might be instructive here. *“Our towers tend to be between 25m and 35m and they are all under review. Each time we add another operator* [to a shared tower] *we do a structural survey and assess the tower against predicted wind speed and work out what structure rating to give it – red amber or green. If it is red or amber we put in place mast strengthening such as extra braces at key points on the mast. Generally we find that we can affordably strengthen the towers.”*

“Mast function is weather dependent and to model extreme events we use existing wind speed forecasts, corrected for conditions and location. So it will be common to have gusts of 100mph in the Highlands. The other wind impact is that the microwave dishes are blown out of position so they are

[9] For example, ASHRAE standards for servers set temperature and humidity envelopes for reliable operation of ICT equipment, underpinned by manufacturers. The current standard generally being applied is ASHRAE 2011. There are more recent standards but it is not generally cost effective to apply them in all environments.

effectively misaligned and off-course which means that relay function can be lost. Sometimes it can be tricky to detect when this has happened and trace the fault to the correct source."

"The whole network is power dependent and in general the mobile network does not have power backup at the masts. The requirements are different for emergency service connectivity [as mentioned above]. *Those that do may have diesel generators or batteries but those only have a limited operating window and if transport links are broken and nobody can reach the generator to refuel it then the mast cannot operate."*

Rain shade to mobile signals
Rain can affect the quality of mobile signals, especially in rural or hard to reach areas where covereage is lower. Rain shade is currently not a significant problem and the issue is largely designed out by increasing the power at the point of transmission to ensure that any dips in signal due to rain do not interrupt services. We anticipate that before long, smarter technology will be able to predict incidents or threatened incidents where rain shade is likely to reduce signal and augment signal power in a much more bespoke manner. Rain shade can affect higher frequency signals – above 10Ghz - and so this has to be a consideration in future planning.

Network interdependencies

The mobile networks depend on the higher capacity public fixed line network for at least some degree of routing. In theory, it should be possible to re-route communication traffic in the case of mast or base station failures but in some cases there is limited information even within operators regarding mobile traffic routing. So in theory if a single exchange floods there is scope for impacts on mobile networks. Identifying which hubs are responsible for high concentrations of traffic is now a priority so that we can identify potential SPOFs and interdependencies. Other shared assets are more transparent and include comms rooms and data centres where broadcast, telecommunications and hosting functions may all run in the same facility.

Resilient digital systems such as broadcasting may operate "warm standby" or "hot standby" and this approach is also common in data centres. The Crystal Palace antenna is considered to be a critical asset because it serves around 10 million people. Therefore, besides having robust alternative power in its own right, there is a mirrored site in Croydon on hot standby all the time.

Some networks provide a fall-back mode, where if necessary, the mast can talk to the handset directly without having to rely on the core network, and if the mast is lost handsets can communicate with each other without going via the mast. It is recognised that fall-back with reduced functionality is preferable than nothing in an emergency.

6 Learning from climate change incidents and proxies

***Section summary:** This chapter examines three case studies. In two cases severe weather affected data centre or communications operations and in the third a tsunami provided a useful proxy for an extreme weather event. Each event is described and the lessons from it are discussed. While the US case study involved some severe interruptions to commercial data centre services and the UK case study involved interruptions to communications provision, we are not yet aware of any commercial (colocation) data centres in the UK being compromised or having to interrupt or suspend service delivery due severe weather.*

6.1 United States

The US is the world's largest data centre market. New York is a major data centre cluster, though smaller than London. New York and New Jersey data centres were badly affected by Hurricane Sandy. A number of painful lessons were learned. This is what happened.

When Hurricane Sandy hit New York on 29th October 2012, utility power supplies were cut and in many cases were not restored until 2nd November. During this time, data centre operators in affected areas were implementing their disaster recovery plans. There had been advance warning of the storm and companies had taken the opportunity to top up their generator fuel supplies and make other emergency preparations (pooling additional equipment, setting up temporary accommodation within the facilities and laying on food supplies for staff working overtime). Nevertheless a number of data centres in New York and New Jersey were very badly affected by the storm and some were compromised, leading to serious consequences for their customers (i.e. the many businesses that ran their IT functions from these facilities).

Lessons learned

- Closer collaboration between landlords and operators was needed to ensure that incentives are aligned. Complex leasing arrangements in which data centre operators may not own, manage or control the buildings in which their facilities are housed can -and did- cause problems.
- In the past, emergency fuel stores had been at the top of buildings but after 9/11 this was discontinued and fuel was stored at lower levels, often in basements. This created severe problems for a number of operators - their generators worked fine but their fuel supplies or the pumping gear were under water – as in some cases was the switching gear.
- Communication is key: one operator that lost power to 5 of its 8 data centres for a number of days maintained multiple channels of communication, keeping customer abreast of all developments. This improved trust and provided customers with the information they needed to decide whether and when to implement their own disaster recovery plans.
- The speed of recovery was largely dictated by the rate at which water could be pumped out of flooded systems so the availability and proximity of heavy plant was key. This was also a lesson from Japan (see below).

6.2 York and Leeds, December 2015

Unprecedented flooding occurred to communications infrastructures in York and Leeds in December 2015 and was widely covered by the press.

The last month of 2015 saw 14 rivers across the north recording their highest ever flows, and 194 Environment Agency gauges registered their highest river levels on record. This culminated in severe flooding over the Christmas weekend which affected the UK and Yorkshire in particular. Thousands of homes were flooded or went without power after sub-stations failed, bridges were washed away and roads were blocked. York and Leeds were badly affected and communications infrastructure was damaged by floods in both cities.

In Leeds the River Aire rose from its normal level of 0.9m to an unprecedented 2.95m, which flooded the Kirkstall Road area of Leeds and affected a Vodafone network site. Customers in the area suffered from intermittent voice and data services. Vodafone observed *“water ingressed our main Transmission sites in that area to a level estimated at between 620mm and 650mm. Our main site has standby generator provision and DC battery back up but due to the water ingress causing water damage to the main incoming switchgear and also some of the DC battery systems some of our systems failed during the incident. Upon failure of these systems we deployed resource to the site but local Emergency services would not allow access until the following day. Once access was granted we were able to undertake assessment of the damage and commence the recovery process of both the damaged Switchgear and DC power systems as well as the clean up process”.*

The site also serviced the North Yorkshire Police’s non-emergency 101 phone line which was out of action for three hours at the height of the floods. Calls had to be re-routed via an alternative number which was in place for a further five days. Local crime commissioners suggested that flood resilience should be a factor in the forthcoming procurement when awarding the new contract for the 101/111 numbers.

BT’s York exchange was also flooded over the same Christmas weekend. This affected landline services, including broadband in the local area. 999 calls for North Yorkshire also had to be re-routed due to loss of functionality at the exchange but no emergency calls were missed as a result. The exchange had never flooded before and was not considered to be at risk. It had a full suite of back up generators plus batteries but the volume of water caused first the mains power and the generators to fail, leaving only the short term reserve batteries. Once engineers reached the site the recovery work could start: after pumping out more than 1.8 million litres of flood water they worked round the clock and restored the majority of phone and broadband services in less than 36 hours.

North Yorkshire Police’s internal radio network was also under pressure: with flooding affecting several sites, bespoke provider Airwave deployed emergency response vehicles to provide a mobile base so that emergency services could communicate with each other. Airwave deployed a specialist team to work directly with the emergency services to minimise the impact and keep the network operational. Once they gained access to their affected sites they were able to restore normal service. West Yorkshire’s police services were unaffected.

Lessons learned

- In all instances transport links were affected to the extent that engineers and other specialist teams were unable to reach facilities. This meant that they could not start pumping water out or get to the generators, or repair switchgear.
- While initial concerns were that a single physical facility supported multiple operations (a SPOF), this was not the case and the floods were severe enough to affect three separate and independent networks at the same time.
- Regular flood risk reassessments would be appropriate given the fact that flood zones are expanding.
- Operators could consider installing / upgrading physical protection for sites, especially for switchgear and generators.

Follow up

- Following the incident a full risk assessment was immediately undertaken by BT to identify how to protect the York exchange from future flooding of this scale.
- BT has also engaged directly with Government via the Electronic Communications Resilience and Response Group (EC-RRG) to ensure that lessons from these incidents are applied more widely.
- Vodafone has been working closely with the Environment Agency and the Cabinet Office as part of the National Flood Resilience Review and has carried out a comprehensive assessment of their infrastructure's resilience against the new flood maps developed by the Environment Agency.
- Based on this assessment, Vodafone has been working on a programme to deliver the remedial works required to reduce the risk of flooding. These works have varied from putting in place temporary defences to developing full flood prevention schemes. Specifically at Leeds, Vodafone has spent over £1 million improving the site's resilience to flooding, including building a flood wall around its perimeter. These works are now complete.
- Vodafone has also worked closely with the emergency services to ensure effective access and egress to sites, so that engineers can get on site more effectively during incidents.

6.3 Japanese Tsunami, 2011 (proxy event)

On 11 March 2011 an earthquake of magnitude 9 occurred about 70km off the East coast of Japan. In turn it caused a tsunami in excess of 10m and in places up to 40m high along the length of the coast. In addition to catastrophic damage to coastal infrastructure and the loss of at least 15,000 lives, one of the four nuclear power stations along this stretch of coast was seriously damaged, leading to a leak of radioactive material. Although earthquakes and tsunamis are not climate change related incidents, the challenges they present to infrastructure provide a useful proxy for an event like a 1 in 1000 year flood or storm surge. Second order impacts included a very significant reduction in power generating capacity as nuclear and thermal power stations stopped generating or were taken offline. There were also critical shortages of fuel, semiconductors and power cables. Despite the scale of the catastrophe, there was no critical damage to Japanese data centres. The reasons for this primarily related to the quality of planning and preparation and included the following;

- Japanese data centres are required by law to be earthquake-proof. M&E and racks are firmly bolted to buildings

- No major commercial data centres are located in areas of coastline (tsunami) risk
- There is a high level of readiness – regular drills etc. and data centres have their own emergency task force which was deployed the same day as the earthquake
- There was a high level of certainty that an earthquake would occur (so the threat is real and the issue of preparing for uncertain threats does not occur)
- Education and licensing ensure a high level of skill, training and readiness.
- Shift patterns were established within 24 hours of the earthquake.
- Good quality of dialogue with government together with evidence based arguments gave data centres priority for power supply and refuelling where power was not available.
- Customer announcements made within promptly so they could make their own plans.

Lessons learned

- Tools worked variably and not always as expected: Twitter and Facebook and web message boards and satellite phones worked well. Tools that did not work were fixed line and mobile phones, SMS and email which experienced line or antenna damage, call saturation or long delivery delay.
- It is vital to communicate proactively to prevent overwhelming levels of enquiry by customers
- Careful planning is needed to manage the workload of engineers to avoid exhaustion
- Service level guarantees need to be improved to ensure fuel re-supply
- Approaches for dealing with long term power outages could be improved

Commentary

This case study demonstrates an extraordinary level of infrastructure resilience. Although not all the findings are relevant to climate change scenarios, this example demonstrates how resilience can be achieved when a) the threat is real (i.e. the risk is certain so the investment decision is straightforward and b) operators can choose where to locate assets. Other aspects of this case applicable to climate change scenarios include proactive – and prompt – outbound communications to prevent overwhelming numbers of incoming calls – this was also a lesson from Hurricane Sandy. Education and training, drills and emergency shift scheduling for engineers might be relevant to some scenarios.

7 Barriers to building adaptive capacity

Section summary: *This section explores some of the barriers to improving resilience in the ICT sector. Dependence on other infrastructure providers or on the supply chain are addressed first. We then review a number of the common barriers to building adaptive capacity that have been cited by infrastructure providers through fora like the Infrastructure Operators Adaptation Forum (IOAF). We divide these into two: barriers that are internal and could primarily be addressed by sector level initiatives and those that are external and largely beyond our control. We make observations from the perspective of the ICT sector on the impacts of those barriers.*

7.1 Interdependencies

There are two sets of interdependencies that we need to be aware of: interdependencies within the ICT sector – between the three constituent sub sectors, and interdependencies with other infrastructure sectors.

Internal (sub-sector) interdependencies

ICT is not a single infrastructure. It comprises a number of systems and networks that work together. This is one of its strengths. Some parts of the infrastructure can work independently such as large parts of our mobile and fixed line communications networks, where one may continue to work if the other is compromised (see section 5). Some are mutually dependent. A data centre cannot function without connectivity and much communications activity depends on data centres. The barriers here are not so much that sub-sector dependencies exist but in the difficulty of ensuring that we know what and where they are. This is one of the actions that we are taking forward as a result of this reporting exercise. techUK is also engaged with the ITRC (Infrastructure Transitions Research Consortium) which models complex infrastructure interdependencies for planning and resilience.

External (cross-sector) interdependencies

Understanding risks arising from interdependencies is always a concern: how do we assess risks in our supply chains and different approaches to risk assessment and management across different sectors? For ICT infrastructure the major interdependencies are energy and transport and to a lesser extent, water. Of these, energy is key, primarily in the form of grid power.
These risks are already prioritised in every aspect of design and operation of the core infrastructure. Moreover, large customers of data centre operators are unlikely to allow their data centre provider to present a single point of failure for their corporate operations: they generally have their own contingency plans and are rarely completely dependent on one facility. Smaller customers are more exposed in terms of business continuity.

Grid power

All our digital infrastructure depends on electricity. Data centres have dual independent power supplies and back up power in the form of batteries or rotary arm UPS and diesel generators (the batteries provide instantaneous power in the short term while the generators fire up). There will usually be fuel supply for at least 48 hours, often longer, plus a prioritised agreement for fuel deliveries in the case of a longer term outage.

Larger telephone exchanges have diesel back-up generators with fuel for at least 48 hours, usually longer in remote areas. They also have batteries for short term outages. We understand that some very remote exchanges and base stations have no mains power and are fuelled from generators with (typically) fuel replenishment needed every two weeks. These are unaffected by grid outages (see below). Smaller exchanges have battery backup typically for a minimum of 2 hours and the green cabinets (DSLAMs) have battery backup provision for a minimum of 1 hour.

At customer premises, fixed line telephones will continue to work during power outages whilst the DSLAMS are still on backup but cordless phones will not work at all because they use radio communications powered by domestic supply. The same applies to broadband and wireless routers which depend on a domestic power supply. Mobile phones will work while they retain charge and can be recharged from the car battery if domestic power is cut but these depend on network connectivity.

Transport

The sector relies on the transport infrastructure to get regular staff to and from facilities, to access affected sites in an emergency and to get fuel to sites in the event of a long power outage.

Regular operations: Operational and technical staff have to travel to work to run facilities and do regular maintenance or upgrades on communications networks and nodes. Disruption to transport networks will impact fleet deployment for scheduled activities and this may have knock-on effects on network resilience. If transport infrastructure is compromised this may also have an impact on customers: in commercial (colocation) data centres customers often look after their own IT equipment which is co-located with that of other customers. Although data centre functions are highly automated, there may be instances where business functionality could suffer if staff cannot reach the facility.

Emergency access: In the event of an emergency it is critical that engineers and emergency teams can reach affected sites. Flooding or damage to transport infrastructure that prevents vehicular access to affected premises will delay repairs because engineers cannot physically (or safely) attend those sites.

Communications providers, especially Openreach, (managing the fixed line access network) will often need to reach the local cabinet and/or customer premises in order to restore service. Fleet deployment will be affected and if roads are flooded, blocked or damaged engineers will not be able to reach affected locations to start recovery operations.

Generator fuel replenishment: In the event of prolonged power outages, fuel deliveries will need to be made at regular intervals and if transport infrastructure is severely disrupted, or fuel distribution is impeded further upstream, then sites cannot function. Fuel delivery was a problem after Hurricane Sandy, when roads were flooded and tankers were unable to reach affected premises. It is also a consideration for very remote base stations run by generator – they have to be accessible to be refuelled.

Pinch points in physical infrastructure (SPOFs)

Some parts of our physical infrastructure act as pinch points for a number of utilities. A single bridge may provide a conduit for multiple networks - water, communications and electricity leading to cascade failure if damaged. Infrastructure providers may not always be aware which physical assets are single points of failure for their, or other infrastructure, nor is there any systematic means of alerting them to the condition or vulnerability of these assets.

Water

Some data centres are water cooled and require high volumes of water. In theory, peak demand is likely to coincide with high summer temperatures and periods when water is in relatively short supply. However we are not aware of any instances in the UK where shortage of water (through drought or rationing) has affected data centre operations.

Cross-sector dependencies relating to ICT are very asymmetric. ICT is critically dependent on energy and all other dependencies are secondary. However, nearly all sectors are heavily dependent on ICT, including those providing other parts of our infrastructure.

7.2 Other internal barriers

Awareness: misunderstanding climate change risks: *difficulty in understanding the problem we are trying to address.*
Awareness of climate change risks is patchy. Conversations usually have to be preceded by definitions and explanations. The terms “climate change adaptation” or “climate change risks” are not meaningful to most data centre operators and many communications providers. Substituting the term “resilience to severe weather” produces an entirely different response. This is an area where we as industry association can take a lead to improve awareness within the sector.

Awareness: information barriers: *lack of awareness of the information available and how to access it, how to interpret it, and how to use it.*
Awareness varies between operators and between sub-sectors. This is an area where we as an industry association could help.

Cultural / behavioural barriers: *Convincing senior management / shareholders /customers that adaptation actions are required.*
This is a common issue where funds have to be thinly spread. It can be tricky where risks are uncertain and there is no evidence base of failures to galvanise investment in protective measures. This is less of a problem in data centres but in communications customer perceptions of cost are key.

Isolating climate change risks: *sometimes it is difficult to extract data from our own fault reporting and incident reporting processes.*

Approaches vary and most operators see no reason to isolate climate change risks from other risks or to handle them differently. For instance, although climate change risks are increasing, so are cyber threats and terrorism. Why single out one type of risk?

Evaluating risk: *how do we deal with the inherent uncertainty of climate change risks? How do we differentiate climate change risks from BAU weather risks?*
Data centres are highly risk averse so all risks are accommodated. It is more problematic for communications providers who may be under greater pressure to allocate funds to projects with more predictable outcomes.

Difficulty in setting risk thresholds: *how do we decide what level of risk is acceptable for a given asset? How do we know we are applying climate science to our assets appropriately?*
Risk thresholds vary depending on asset type. The risk threshold that tends to be used for commercial data centres is around 1 in 1000 although this is not prescribed by standards or regulation. Facilities choosing locations with higher risk factor generally find some means of mitigation. Large exchanges also work to a similar risk threshold or seek mitigation. Mobile masts standards tend to be operated with a 1 in 50 year incident in mind.

Difficulty in prioritising risks: *how do we choose which risks to mitigate?*
For the ICT sector this is relatively straightforward since flooding is the primary climate change risk and carries the most severe consequences. However, this is lower priority than managing dependency on power: the risk of failure in the electricity infrastructure is one of the top priorities for data centres and comms providers because the ICT infrastructure is so heavily dependent on electricity.

Cost benefit analysis: *problems of establishing a business case: how do we put relative values on costs of climate change vs. cost of improving resilience?*
This is an issue for communications providers who tend to be caught between the regulator who wants to keep prices low for consumer and the customer who might be sceptical about paying for an uncertain risk. Within data centres this is a more straightforward decision because resilience is a very high priority and all risks have to be factored in.

7.3 Other external barriers

Regulatory barriers: *Regulatory obligations on operators may compromise resilience or increase the cost of improving resilience.*
This is not a problem for data centres but is certainly an issue for communications providers. The strong regulatory focus on competition around low prices for consumers is a barrier to resilience in the mobile network and the universal service obligation requires the incumbent fixed line provider to connect and maintain connections to premises in flood zones provided they are not classed as "hard to reach".

Incompatible decision cycles: *how do we reconcile long term planning with shorter term investment cycles?*

This has not been reported as a particular problem for data centres. However, the communications regulator needs to accommodate longer term risks even if they are unlikely to be realised within next price review period.

Incompatibility between efficiency and resilience: *how do we reconcile efficient use of resources with the redundancy we need for greater resilience?*

This is probably true of our mobile infrastructure which is shared between operators and is very efficient. The corollary to this efficiency is that spare capacity will be low and there won't be much redundancy. This inevitably has an impact on resilience when parts of the network are damaged or unusable.

Public policy: *climate change adaptation not evident on public policy agenda.*

This is unlikely to be a factor for data centres where risk assessment is driven by sector requirements rather than public policy priorities. It may be more of an issue for communications providers who are regulated.

Planning and enforcement: *Planning policy is not always enforced at decision stage. EA input is not always accommodated in planning decisions.*

Inadequately enforced planning policy is a particular problem for the fixed line access network because development is still continuing in flood plains against the advice of the Environment Agency. These developments are unlikely to be classed as "hard to reach" which tends to apply to very rural or isolated premises, so there is an obligation under the Universal Service Provision to connect, and more problematically, to maintain the connection, to these developments. This inevitably makes it harder for risk to be managed cost effectively in this infrastructure.

Problems of restricted focus: *Focusing on assets exclusively rather than on service delivery – maintaining service delivery even when assets are compromised should take precedence over a pure focus on protecting assets.*

The ICT sector is a service sector and the core focus is on maintaining service and delivering against service level agreements (SLAs). It has been very evident, however, that government and regulators are focusing closely on physical assets at the expense of service delivery. It is true that the cloud is not a cloud – it is a data centre full of servers – but there are more ways to protect the services provided by that data centre than just protecting that physical asset.

Market and technology barriers: *uncertainties created by disruptive technology developments.*
Industry wide uncertainties regarding evolution of key markets such as energy mix and transport.

It is perhaps the ICT sector that creates the most uncertainties here. The increased reliance on ICT by all other sectors is an example.

8 Looking ahead: actions to improve sector resilience

Section summary: *This section sets out some areas where we could be better prepared as a sector for climate change risks. It then outlines what we can do as an industry association to ensure that we implement what we have learned from this exercise.*

8.1 Areas needing further investigation

While setting out the approaches to managing climate change risks in the industry, we have identified a number of areas where we think there are potential weaknesses. These are:

- Conceptual understanding of climate change adaptation
- Level of awareness of relevant information sources
- The extent of the evidence base needed to direct future initiatives
- The variable regularity with which flood risk is re-examined
- Reactive rather than proactive re-examination of flood risk
- Difficulty in identifying sub-sector interdependencies due to infrastructure complexity.
- External interdependencies, especially SPOFS and pinch points in physical infrastructure
- Regulatory pressures.

8.2 What we can and can't do

As an industry association we do not prescribe- or proscribe - particular approaches but we can guide and encourage. We have the capability to draw our members' attention to climate change risks and to sources of information that will help them understand and prepare for those risks. We can remind them that climate change risks are changing all the time and we can alert them to relevant industry standards. We can also produce recommendations and work with the sector to develop a better understanding of single points of failure. These are set out as actions below.

- Build the evidence base to inform future action: monitor any publicly reported incidents and identify the lessons that can be learned from them for wider application within the sector.
- Raise awareness of climate change risks within the industry and provide clear guidance to help operators differentiate climate change mitigation from climate change adaptation.
- Provide further guidance to members on the information sources they should be accessing and how they should be using them.
- Alert the sector to relevant standards.
- Develop simple recommendations for operators on reviewing flood risk proactively, on a regular basis, rather than at point of site selection or in response to a bid, insurance request or incident.
- Build closer relationships with stakeholders: insurers, academia, the supply chain and other infrastructure providers
- Initiate dialogue with relevant regulators to highlight areas in which regulatory requirements hamper adaptation and resilience.
- Lead an industry activity to review the reasons why SPOFs are frequently difficult to identify on a systematic basis, and explore the scope for improving our understanding and awareness of SPOFs in our digital infrastructure.

We will provide an update on progress against these actions in the next round of reporting.

8.3 Other recommendations

We have identified a number of actions that we as a sector need to take. However there are several areas where resilience could be improved with the help of external stakeholders. We therefore recommend:

i. A preferred or default UKCP09 scenario to encourage infrastructure operators to use the same reference points for strategic planning and standards development.
ii. A broader focus on service delivery rather than asset protection.
iii. A more robust approach to flood plain development that is at odds with Environment Agency advice e.g. responsibility retained by developers or limited obligations for infrastructure operators in those zones.
iv. Scope for the provision of condition reports on bridges that carry multiple utilities and other single points of failure in our physical infrastructure.
v. Regulatory provisions of the USO for fixed line telephony are reviewed, especially for new properties located in flood zones.
vi. The current regulatory focus on customer prices for mobile services is scrutinised in terms of its potential impact on resilience.

8.4 Further information

Contact:

Emma Fryer, Associate Director, techUK, Emma.fryer@techuk.org

More information on Data Centres

techUK data centre programme: http://www.techuk.org/focus/programmes/data-centres
Data Centres Council: The UK Council of Data Centre Operators (techUK Data Centres Council)
Data Centres for Tiny Tots

- **Er, what is a data centre?,**
- **Data Centres: Engine of Growth**
- **So What Have Data Centres Ever Done for Us?**
- **Data Centres: A Day in YOUR Life**
- **Data Centres and Power: Fact or Fiction,**

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. In 2015 the internet economy contributed 10% of the UK's GDP. 900 companies are members of techUK. Collectively they employ more than 800,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses. www.techuk.org

ANNEXES

Annexe 1: Universal Service Obligation for Fixed Line Communications

Annexe 2: Sample Statement of capability conformation

Annexe 3: Sample emergency flood risk plan

Annexe 4: Technical Annexe: Criteria for 50600 Availability Classes

Annexe I: Universal Service Obligation

What is the Universal Service Obligation?

Incumbent operators Kingston Communications (in Hull) and BT (for the rest of the UK) are obliged to provide a range of services including

- a phone line, on demand, almost anywhere in the UK, at speeds that allow internet access
- special low-cost schemes to help people on low incomes to afford a phone service
- enough public call boxes ('payphones') where they are needed; and
- special services for people with disabilities.

This is known as a Universal Service Obligation (USO) and was introduced in 1984 when BT and Kingston were privatised. The USO was revised in 2006. At this point Ofcom estimated that the cost of providing the USO was not disproportionate to the benefits and that therefore it did not present a significant cost burden.

However, things have changed since 2006. Climate change now has a prominent place in the business and policy agendas and carbon dioxide levels in the atmosphere have recently broached 400ppm for the first time since the Pliocene[10]. Climate change risks are now real risks and businesses and governments must accommodate them in strategic planning.

The USO does not appear to take into account additional costs presented by providing and maintaining this infrastructure under an adaptation scenario (essentially a scenario in which a number of climate change risks are realised). While the USO sets a threshold above which costs can be recouped for connecting hard-to-reach customers, properties in flood zones are not generally hard to reach but neverthelss may present much greater capex or opex costs. It would make sense for the USO, if it does not do so already, to differentiate provision requirements for very high risk properties (for example, properties that have been built in flood plains against the explicit advice of the EA). Moreover the USO focuses exclusively on the cost of supply (the one-off cost of connection) rather than on managing ongoing risk (the long term, open-ended costs of maintaining that connection). This may make it difficult for providers to manage these risks cost-effectively in some areas in the long term.

[10] Recording taken on 10 May 2013 at Mauna Loa by NOAA of 400.03ppm.

Annexe II: Sample statement of capability

Ark[1] Risk and Resilience Management (ARRM)

Statement of Capability and Conformance

1 ARRM System Overview

The ARRM System covers the whole enterprise (this includes suppliers and sub-contractors) and provides a single, holistic and integrated means by which the full spectrum of identifiable risks faced in all business environments can be managed efficiently and coherently. The Ark Enterprise **conforms to international standards of best practice** and responsibility by employing risk and resilience management processes in all aspects of its service delivery. **Risk management** embraces all business processes, activities and key outsourced services during business-as-usual periods. **Resilience management** covers the actions required at every level within the Ark Enterprise following a major disruption or undesirable incident, from response through to achieving a full recovery. The whole system is underpinned by a process of review and continual improvement.

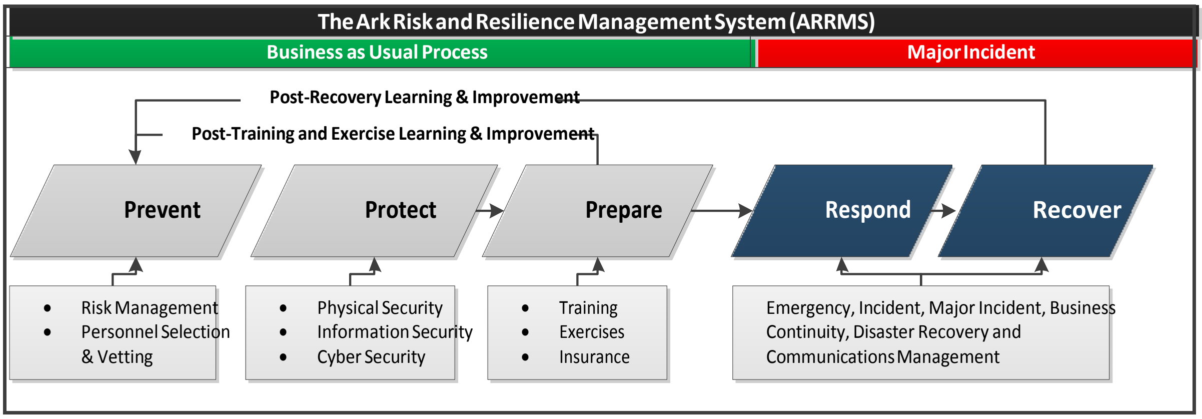

The Ark Risk and Resilience Management System (ARRMS)
Business as Usual Process
Major Incident
Post-Recovery Learning & Improvement
Post-Training and Exercise Learning & Improvement
Prevent
Protect
Prepare
Respond
Recover
Risk Management
Personnel Selection & Vetting
Physical Security
Information Security
Cyber Security
Training
Exercises
Insurance
Emergency, Incident, Major Incident, Business Continuity, Disaster Recovery and Communications Management

Figure 1 - The ARRM System

The enduring corporate and phase-specific aim & objectives are achieved in accordance with the direction of the Ark Senior Leadership Team (SLT). These are expressed in this Statement of Capability and Conformance.

2 Corporate Aim of the ARRM System

In order to secure and protect Ark's present and its future integrity, the ARRM System fulfils Ark's commitment to safeguarding our clients, people, reputation, investors, brand and assets by:

(a) Creating and protecting a safe environment where data and systems can be stored, managed and developed with confidence.

(b) Enabling risk to our clients, Ark and to other key stakeholders to be managed of a comprehensively and robustly.

(c) Demonstrating and communicating our resilience to reassure our key stakeholders and inspire client and public confidence in the business, its operations and its intentions.

(d) Acting decisively to influence the outcome of disruptive incidents, turning disruption into opportunity, in Ark's favour and in the best interests of our clients.

(e) Protecting critical services, revenue streams and enabling fast business recovery from an all- hazards perspective through employing comprehensive business continuity and IT disaster recovery management systems at all levels.

(f) Demanding high levels of compliance in responsible management and resilience from all of our key partners and suppliers.

(g) Following the principles of 'Plan-Do-Check-Act' to review and continually improve our systems in the light of developing best practice and lessons learned.

(h) Complying with ISO 22301:2012 to standards verified by external audit and aligning risk management systems with ISO 31000:2009.

3 Objectives of the ARRM System

3.1 Objectives – Prevent & Protect Phases[2]

In order to ensure that the organisation has taken every reasonable step to anticipate and mitigate all known risks, the SLT directs that the whole organisation will:

(a) Through effective risk management, continuously identify, manage and reduce uncertainties in order to:

(b) Protect and secure Ark, its clients and its stakeholders from suffering the adverse effects of disruptions when they occur and;

(c) Exploit the full spectrum of potential opportunities, thus benefitting the organisation, its clients and its stakeholders.

(d) Establish, maintain and continuously improve the risk management process in alignment with ISO 31000:2009 best practice (measured through compliance with ISO 9001:2015 to external audit standards).

(e) Reassure and promote the confidence of our clients and staff through proactive communication of our risk management practices, processes and achievements both internally and externally.

(f) Allocate management time and funds to ensure that the risk management element of the ARRM System is current, relevant and compliant through a process of revision and internal/external audit.

3.2 Objectives – 'Prepare' Phase

In order to maintain the highest level of preparedness during business-as-usual operations, the SLT directs that the whole organisation shall achieve the following objectives:

(a) Establish, maintain and continuously improve the business resilience element of the ARRM System in full compliance with the requirements of ISO 22301:2012, and shall remain externally certified to this standard.

(b) Allocate management time and resources to ensure that the business resilience element of the ARRM System is current, relevant and compliant through a process of revision and internal/external audit.

(c) Reassure and promote the confidence of our clients, staff, sub-contractors and suppliers through proactive communication of our business resilience practices, processes and achievements both internally and externally.

(d) Protect our service delivery by demanding the highest level of resilience in our supply chain.

(e) Ensure the highest continual level of preparedness through training, exercising and testing of systems at all levels.

3.3 Objectives 'Respond' Phase

The SLT directs that the whole organisation shall be capable of achieving the following objectives in response to a major disruption or undesirable event:

(a) Protect and safeguard our people, assets, facilities, systems and revenue streams in accordance with our duties as a responsible employer and service provider.

(b) Protect and safeguard the interests of our clients while minimising any disruption to that of their own service delivery.

(c) Restore our urgent and critical client services and supporting business functions within recovery time objectives determined through the Business Impact Analysis process).

(d) Maintain our capability for winning & managing new business.

(e) Maintain clear, timely and effective communications with internal and external stakeholders from the onset of an incident through to full recovery.

(f) Protect and, where possible, enhance our corporate reputation through rapid and efficient responses to business disruptions.

(g) Recover full business functions within recovery time objectives through comprehensive business continuity and IT disaster recovery arrangements at all levels.

[1] For these purposes "Ark" is "*Ark Data Centres Limited and the other UK subsidiaries of Ark Group Limited*"

[2] For phases see Figure 1.

Annexe III: Template for flood risk plan

0 Introduction

A flood emergency response plan should set out the preparations needed to respond to flood incidents (people and resources) and the procedures that should be implemented.   An effective flood plan will contain commercially sensitive information and important details relating to site security and therefore should remain confidential.

The plan should include the following

- Identification and appraisal of the flood hazard, including information sources
- Survey of building and categorisation of the flood risk affecting critical areas
- Preparation
- Emergency management structure
- Action plans for dealing with different categories of floods and the subsequent clear up
- Post event analysis

Supporting information should also be available:

Appendix A	Understanding local flood hazards (an example is included for London Docklands)
Appendix B	Key equipment and supplies that should be in place
Appendix C	Likely water damage to plant items that are affected by flood
Appendix D	Health & safety considerations in dealing with floods
Appendix E	Guidance on deployment of protective measures (sand bags and flood board

1.0 Understand and evaluate the flood hazard relevant to the location.

- Understand relevant flood types – coastal, fluvial, pluvial, plus tidal surge, surface water runoff, other local factors. (There is a large data centre cluster in London so Appendix A includes notes specific to tidal surges and flooding to the Thames basin).
- Familiarise staff with existing hard defences and other public flood protection. See Appendix A for notes on the Thames Barrier
- Ensure that relevant sources of information are being used (Met Office, Environment Agency, Water company, barrier/barrage/lock/weir controller, Energy provider)
- Ensure that the correct information is being accessed and used to inform decision making (Flood alerts, forecasting, advanced hazard warnings)
- Be aware of times where risk is higher / seasonal variations in risk
- Ensure that different flood scenarios have been explored and envisaged.

2.0 Building survey

A building survey should be conducted to record the location of critical plant with respect to potential water levels.

2.1 Annotated building elevation

- An annotated elevation, if necessary supported by an indicative plan, should be produced.
- A key reference level should be identified and the relative height of all plant /critical assets should be included on the elevation, plus information regarding access.
- External reference levels (e.g. for nearby water bodies) should be included.
- An inventory of critical plant at each level should be compiled.

SCALE or ANNOTATED DIAGRAM SHOWING BUILDING ELEVATION AND FLOOR LEVELS, VERTICAL LOCATION OF ALL KEY PLANT AND ANY RELEVANT KEY REFERENCE POINTS IS ESSENTIAL

2.2 Assessment of flood risk (for each floor/level):

- At what point above reference level would the level/floor be breached by flood water?
- How much water could accumulate and have to be pumped out (M^3/L)?

- Type and condition of external drainage to building – surface, gravity / pumped?
- Destination of drain water, priority rating of termination point for water
- (some pumping stations are considered priority and will be backed up by generator)

2.3 Survey of each floor level

- Floor height relative to key reference points.
- Indicate what kind of walling – block, partition etc.
- Access and emergency access
- Situation of plant: enclosed or open?
- Plinthed or frame mounted? Height of plinth /frame?
- Generators: indicate levels of Alternators, air intake, fuel intake, exhaust
- Oil storage: indicate level of filler nozzles, capacity and lowest likely capacity
- Existing water protection/ internal drainage
- Location of any specialist equipment
- Operator responsible for drain terminus (e.g. Thames Water).
- Operator responsible for HV switch room (i.e. energy supplier)

2.4 Plant to include in inventory

- UPS Batteries.
- DC System Batteries
- DC Battery Isolator Panel
- Transformers
- Electrical Distribution & Cabling
- MVA Generator(s)
- Fuel Tank/s
- HV Switch Room(s)
- UPS
- Static Switch(es)
- Transformer Incoming Panel(s)
- Generator Control Panel(s)
- Main Switch Panel(s)

3.0 Preparation

The facility and staff must be prepared so that the emergency flood response plan can be implemented instantly. This includes communicating the information to key people and the advance purchase of equipment and supplies.

3.1 Awareness of senior management

Senior management to board level should be made aware of the potential for flood hazard at the site/s and the existence of the Emergency Response Plan. They need to understand the risks of damage to assets, impact on customers and reputation. Most importantly, responsibility for implementing site shut down plans must be acknowledged.

3.2 Awareness of other key people

All members of the Flood Management Team must be fully briefed on this plan. Awareness of the conditions that can build up into a flood and the ability to proactively prepare are critical. The Flood Management Team will need to be familiar with the emergency equipment, and trained in its use. Training and awareness will also need to be maintained through the use of regular drills. Maintenance of emergency equipment also needs to be considered part of the day to day site operations management.

3.3 Site shut down briefing

A briefing on site shut down needs to be prepared including criteria for implementation and authorisations.

3.4 Equipment to purchase

Equipment identified in the plan (sample list in the appendices) will need to be purchased. An inventory should be prepared and the location of the equipment should be clearly communicated to staff.

3.5 Other preparations

Other site preparations should include flood boards, line markers on walls to indicate depth etc.

4.0 Management structure for incident response

A Flood Management Team should be established; all key staff needed to deal with the incident must be identified, and the list must be maintained to accommodate staff changes.

Home addresses should be included in case any staff are personally affected by flooding

5.0 Emergency response: staged action plans

Establish key reference points for implementing action plans. These could be Environment Agency flood or severe weather warnings, warnings from other sources (Thames Water, Thames Barrier, Met Office), water level measurements in adjacent water bodies (rivers, reservoirs, docks, etc.), rain gauge measurements, water levels in basement or car parks, etc. or known upstream risks.

Action plans should be staged on the basis of the degree to which circumstances are departing from key reference points and on the basis of impacts on assets and functionality as water level rises.   It is likely that operators will have several levels of response: low impact incidents will continue normal operation but increase monitoring; a medium-level response will address events of greater severity where the site moves to generator power supply (in anticipation of mains failure) and a severe impact event where the site undergoes controlled shut down. These are explained in more detail below.

5.1 Low Impact (incremental breach of key reference points)

Emphasis: Increase monitoring
Strategy: Ensure the site is fully prepared to escalate response

5.1.1 Receive notification of flood expectation

- Notify key staff
- Check with environment agency on expected extent of flood
- Brief Flood Management Team
- Check initial water level to establish a reference point for further rises
- Implement monitoring
- Check with energy supplier for any planned power supply outages (time of and expected duration)
- Monitor Radio and TV news for updates
- Notify Customer Support of situation

5.1.2 If key reference points are further exceeded

- Escalate to Medium Impact plan

5.2 Medium Impact Plan: (significant breach of key reference points)

Emphasis: Keep running on backup systems
Strategy: Protect key rooms and pump out any water entering the rooms, whilst keeping support systems running. Subsequent clean up and dry out.

5.2.1 Receive notification of flood expectation

- Notify key staff
- Check with Environment Agency on expected extent of flood
- Brief Flood Management Team
- Check initial water level to establish a reference point for further rises
- Position staff externally to monitor flood progress (ensure radio contact).
- Check with energy supplier re: planned outages (time of and expected duration)
- Order diesel to fill tanks (if not at capacity)

- Arrange diesel re-supply as appropriate
- Check inventory of emergency equipment
- Deploy sandbags/boards around doors and walls of relevant rooms (See Appendix E).
- Position pumps in each of the above rooms (ensure that fuel tanks are full).
- Cut hoses to pump water seeping through sand bags back out of sandbag protected area.
- Notify Customer Support of situation
- Implement Customer Communication Plan (advisory briefing – loss of service possible)
- Brief Board on possible need to implement site shut down plan.

5.2.2 Appearance of water imminent

- Switch to Generator & shut down mains supply (check responsibility for isolating HV).
    - Outline procedure
    - Load transferred to generators

5.2.3 During flood

- Observe safety precautions (See Appendix D)
- Monitor water levels and other key reference points
- Keep monitoring all affected internal areas. Refer to markers on walls.
- Monitor water level in all plant rooms. Isolate and shut down all affected plant (eg isolate batteries and disconnect terminals)
- Start pumps when water depth in rooms is sufficient for pump operation.
- Reinforce flood defences as required.
- If water level rising too fast escalate to high impact response and implement site shutdown plan.

5.2.4 Post flood

- Maintain flood barriers until all water on car park surface has been removed (by pump or drainage)
- Remove sand bags/boards
- Position humidity sensors
- Deploy propane heaters until all areas are dry
- Clear debris
- Re-supply from another (nominated) site if local supply chains are disrupted.

5.3 High Impact (1,000 Yr. event):

Emphasis: Controlled shut down

Strategy: In this scenario, the level of flooding is so severe that there is no alternative but to plan for complete controlled shutdown. Protect plant as far as possible. Subsequent clean up and dry out.

5.3.1 Receive notification (estimated 5 to 8 hours)

- Notify key staff
- Get confirmation from relevant authority (Environment Agency/water company/local authority/emergency services) that site will flood / defences will be breached and site canot be protected.
- Brief Flood Management Team
- Notify staff to move cars
- Check initial water level to establish a reference point for further rises
- Check with energy supplier for advice on power supply outages (time of & duration)
- Position staff externally to monitor flood progress (ensure radio contact)
- Order diesel to fill tanks
- Notify senior management / board (advise of requirement to implement Site Shut Down Plan)
- Check inventory of emergency equipment
- Check satellite phones are working
- Fit flood boards to relevant plant rooms.
- Apply silicone sealant around all door frames & fitted boards.

- Fit boards to generator grilles
- Notify customers of planned shutdown
- Implement Site Shut Down Plan

5.3.2 Implement Site Shut Down Plan

- Get approval for shutdown from relevant authority
- Relocate customer support to other sites to coordinate customer communication activity.
- Evacuate non-key staff
- Complete register of all personnel on site and notify personal contacts (family etc.)
- Evacuate visiting customers
- Maintain customer communications

5.3.3 Appearance of water imminent

- Implement shutdown – customer equipment
- Implement Site Shut Down
  - Procedure for plant shut down
  - Procedure for power shut down
    - Disconnect all battery terminals
    - Remove low lying batteries to higher shelves
  - Site off line
- Implement customer communication from other sites

5.3.4 During flood

- Observe safety precautions (see Appendix D)
- Monitor water level
- Keep staff on upper levels (do not use any lifts even if still operational)

5.3.5 Post flood clean up

- Position pumps and start pumping water out. Be aware of volume of water and time required. Note: surface drainage is likely to become blocked and so will be inoperable.
- Maintain flood barriers (around doors etc.) until all external water has been removed (by pump or drainage)
- Remove sand bags/boards
- Position humidity sensors
- Deploy propane heaters until all areas are dry (monitor humidity sensors)
- Clear debris
- Evaluate extent of water ingress into plant rooms
- Evaluate damage to plant
- When deemed safe to do so, bring plant back on line and test
- Check with energy supplier on mains power status
- Run site on Generator (if available) until mains is restored
- Re-supply from another (nominated) site if local supply chains are disrupted.

6.0 Post event analysis

Ensure that a thorough review of the response is conducted as soon as possible after the event. It should assess physical aspects as well as procedures and management. It should include:

- Assessment of emergency response; what went well, what did not, areas for improvement, lessons learned.
- Staff debrief and feedback
- Customer debrief feedback
- Implement remedial actions: additional defences / equipment, changes in procedures or other measures that would improve future preparedness.

Appendix A to Annexe III

Evaluating flood risk for London Docklands

The primary flood risk for this area is tidal surge or a combination of tidal surge and high river levels. Previous incidents have involved a combination of equinoctial events plus very strong winds funnelling water into the Thames Estuary. The worst incident in living memory was in 1953.

A.1 Tide levels and surges

Tide levels are steadily increasing owing to a combination of factors. These include higher mean sea levels, greater storminess, increasing tidal amplitude, the tilting of the British Isles (with the south eastern corner tipping downwards) and the settlement of London on its bed of clay. As a result tide levels are rising in the Thames Estuary, relative to the land by about 6mm per year.

Surge tides are a particular threat and occur under certain meteorological conditions. When a trough of low pressure moves across the Atlantic towards the British Isles, the sea beneath it rises above the normal level thus creating a 'hump' of water, which moves eastwards with the depression. If the depression passes North of Scotland and veers Southwards in the North Sea, extremely dangerous conditions can be created.

A surge occurs when this mass of water coming from the deep part of the ocean reaches the shallow southern part of the North Sea. The height of the surge may be further increased by strong northerly winds. If a high surge coincides with a high 'spring' tide (spring tides occur twice a month) reaching the bottleneck of the Straights of Dover and entering the Thames Estuary, there could be a real flood danger along most of the tidal Thames. The overall rise in water levels steadily increases the possibility of flooding.

A.2 Public flood protection infrastructure

London's main flood defences include a number of moveable gate structures, by far the largest of which is the Thames Barrier. Together with the Barking Barrier and significant gates at the entrances to the old Royal Docks, the Thames Barrier is maintained and operated by the Environment Agency. The Thames Flood Barrier is designed to protect London from a scale of storm surge, the nature of which occurs with a frequency of 1 in every 1,000 years (up to 2030). i.e. there is a 0.1% probability of one of these occurring in any given year.

A.3 Monitoring conditions

Dangerous conditions can be forecast up to 36 hours in advance. The decision to close the barrier is taken by the Barrier Controller. This decision is based on the predicted height of the incoming tide as estimated by the Meteorological Office's Storm Tide Forecasting Service (STFS), together with information from the Barrier's own sophisticated computer analysis. The STFS monitors tides along the east cost and issues warnings of dangerously high waters. Their estimates are based on meteorological information from satellites, oil rigs in the North Sea and from land based meteorological stations. They also receive tide readings from recorders as far away as Stornoway in the Western Isles and Wick in the North of Scotland. The Barrier is usually closed between one and three hours after low water, some three to four hours before the peak of the incoming surge tide reaches the site. Tidal forecasts are prepared for the area using astronomical tidal predictions, fluvial flow forecasts, and weather data. Output from the Meteorological Office 36 hour weather model is received twice daily at the Thames Tidal Defences Control Room at the Thames Barrier approximately four hours after the model run. This is combined with fluvial flow forecasts and the predicted astronomical tides to give a 32 hour long tidal forecast which is updated every 12 hours. Actual tide levels at the Barrier are monitored 24 hours a day, 365 days a year.

A.4 Advance hazard warning

Should dangerous conditions be detected, warnings will be issued no later than two hours before the tide reaches the area; however it is expected that warnings will generally be issued about five hours in advance of a high tide. Flood warnings will be broadcast by regular media bulletins on local radio and television and will be issued directly from the Thames Tidal Defences Control Room at the Thames Barrier.

In addition to the public broadcasts, incident management staff can be nominated to receive warnings by SMS/automatic voice messaging.

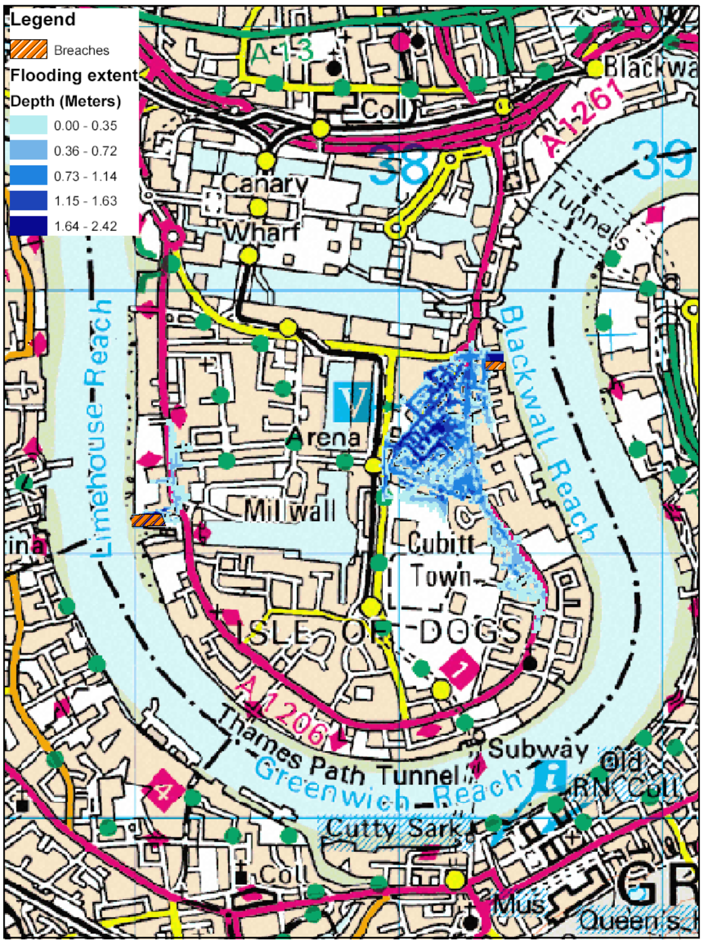
The conditions building up to the occurrence of a 1 in 1,000 year event would take some time to accumulate and would be evident some time before becoming an immediate threat to London and the Thames estuary. To put this in perspective, the event that occurred in 1953 causing 300 deaths and widespread flooding down the east coast of England was a 1 in 300 year event. Given that a 1 in 1,000 year event would broadly follow the same path, leaving a trail of destruction down the east coast, it would obviously be receiving a great deal of news coverage en route.

A.5 Times of increased risk

As a general rule, the level of risk is at its highest during the ‘Flood Season’, which runs from September to the end of April each year. This is due to higher rain fall giving rise to greater fluvial flow during this period. Decisions to close the barrier during high fluvial flow are more complex with more factors to balance, as closing the barrier increases the risk of flooding though the ‘Upstream Section’ (Putney Bridge to Teddington Weir).

A.6 Local area flooding scenarios

Although the Thames Barrier and its associated defences will protect the Docklands area from storm surges of up to the 1 in 1,000 year events (up to 2030), there are other potential flood scenarios that could arise with little or no warning. For instance, the Barrier Controller may allow a very high tide past the barrier (not quite high enough to trigger closure) and a key piece of flood defence may subsequently fail. Although the effects of this failure would be localised flooding, if it occurred at the point of high tide, then the flood would be impossible to stop and would give no warning. Such a scenario could arise through either an accidental failure, or as the result of deliberate damage. The likelihood and impact of such an event is increased during the flood season.



In order to establish vulnerability to such an event, the following analysis was carried out by the Thames Barrier Flood Incident Management Team, using ‘THEMIS’, their bespoke Hydrological Modelling software. This provides a visual of a potential flood impact on the Isle of Dogs should such a scenario occur. The scenario involves using a failure of the river defences on both the east and west side of the island simultaneously and is based on the following assumptions:

- The tide is the largest that would be allowed through without triggering a closure.
- The simulated breaches are very large (approx. 80 metres).
- Based on this analysis, this is an extreme scenario and very unlikely.

A.7 Expected depth of flood water

The Barrier Controller’s official approach is not to speculate on absolute water levels in the event of a major flood (1 in 1,000 yr. event), as in their view these levels will constantly change and would be impossible to predict or model. However they do suggest that in during major events, water levels of 1.5m higher than existing dock water levels are possible, but levels of 3.0m are almost certainly not possible. Therefore maximum flood levels envisaged are +3m.

Appendix B to Annexe III
Schedule of equipment & supplies

Equipment required:

- 2-way radios (+ spare batteries)
- Absorbent granules (tonnes, palletised if need be)
- Battery powered radio for news updates
- Blankets
- Buoyancy aids (life jackets)
- Cleaning equipment
- Climbing rope/s / harnesses
- Digital camera – collection of evidence for insurance purposes
- Drinking water (3 day supply)
- Dry suits
- Extension cables
- First aid supplies
- Flood lights
- Food rations (3 day supply)
- Gas/paraffin lanterns/candles
- Gas/paraffin stoves/cooking equipment
- Heavy duty bin bags
- High visibility jackets
- Hoses for pumps (length specified) + spare section for cutting to size
- Humidity meters
- Inflatable boat + oars
- Large supply of silicone sealant
- Masonry drill bits, screws & plugs
- Mops/buckets/shovels/hand bailers (plastic dustpans can substitute)
- Overalls
- Pallet truck
- Petrol driven water pumps (specify capacity based on potential volume of water)
- Plywood boards cut to size for fitting over vents etc.
- Portable petrol driven generator
- Power drill/s
- Power screwdriver/s
- Propane heaters (not to be used until all standing water has been removed).
- Protective goggles/face masks
- Rolls of polythene sheeting/duct tape
- Sand bags (palletised 1 tonne per pallet (in 1 tonne bags)
- Sanitation supplies
- Satellite phones (+ spare batteries)
- Sleeping bags
- Spare warm clothing
- Steel shelves/racking to stow low lying batteries
- Supply for fuel for above (n * x Lts barrels + hand pump + small petrol containers)
- Supply of gas for propane heaters
- Torches (+ spare batteries)
- Vermin control (rat poison/air gun)
- Waste bins
- Waterproof gloves
- Wellington boots (assorted sizes)

Appendix C to Annexe III

Impact of potential water damage on plant

The following is a brief summary of the potential impact of water damage to plant and equipment that is likely to be affected during a flood~~.~~

Batteries: Batteries submerged in water will short circuit across the terminals. This not only discharges the batteries, but causes corrosion of the terminals themselves. There is some risk of water getting into the cells through the vents, causing the electrolyte to become diluted and contaminated. Batteries will normally be perfectly resilient to being dropped briefly into a water bath; however prolonged exposure would generally result in the batteries becoming damaged beyond repair.

The main risk in entering a flooded UPS area is standing in the water and touching a live electrical termination, so the area should be isolated and drained as quickly as possible. Disconnection of battery terminals prior to submersion is recommended.

Cast resin transformers: If transformers are subject to total immersion in water there is a risk of the insulation breaking down causing water ingress in to LV windings. However, the Transformers should be able to withstand immersion in water up to a depth of x mm from mounting without sustaining damage.

Cabling: When any cable product is exposed to water, any metallic component (such as the conductor, metallic shield, or armour) is subject to corrosion that can damage the component itself and/or cause termination failures. If water remains in medium voltage cable, it could accelerate insulation deterioration, causing premature failure. Cable that is listed for use in only dry locations may become a shock hazard, when energised, after being exposed to water.

Electrical distribution equipment: Electrical distribution equipment usually involves switches and low voltage protective components such as MCCBs and fuses within assemblies such as panels and switchboards. The ability of the protective components to protect circuits is adversely affected by exposure to water and to the minerals and particles which may be present in the water. In MCCBs and switches, such exposure can affect the overall operation of the mechanism through corrosion, through the presence of foreign particles and through the removal of lubricants. The condition of the contacts can be affected and the dielectric insulation capabilities of the internal materials can be reduced. Some MCCBs are equipped with electronic trip units and the functioning of these trip units might be impaired. For fuses, the water may affect the filler material. A damaged filler material will degrade the insulation and interruption capabilities of the fuse.

Lighting fixtures and ballasts: Flooded lighting fixtures and associated equipment, may be damaged by corrosive materials, sediment and other debris in the water. Corrosion of metallic parts and contamination of internal circuitry may prevent the equipment from operating properly. Lighting fixtures and associated equipment known to have been submerged should be replaced.

Motors: Motors which have been flooded by water may be subjected to damage by debris or pollutants. This may result in damage to insulation, switches, contacts of switches, capacitors, overload protectors, corrosion of metallic parts and contamination of the lubricating means and should be evaluated by qualified specialist personnel.

Fuel: Check for water contamination.

Appendix D to Annexe III

Health and safety considerations

As general guidance that should be communicated to staff, the following points should be borne in mind when dealing with a flood:

- Floods can kill. Avoid walking through flood water – six inches of fast flowing water can knock you off your feet. Manhole covers may have come off and there may be other hazards that you cannot see.
- Never try to swim through fast flowing water – you may be swept away, or be struck by an object in the water.
- Always move slowly and carefully. Standing water and mud can obscure holes and sharp objects such as broken glass. Sediment can also be slippery.
- Wear protective clothes, sturdy boots, waterproof gloves and face masks when handling debris.
- Flood water may be contaminated by sewage, chemicals, or rat's urine (leading to Weil's disease). Keep your hands away from your face while cleaning and always wash your hands if you make direct contact with flood water or silt.
- Wash cuts and grazes and cover with a waterproof plaster. Get a tetanus jab if you are not already inoculated.
- Do not attempt to move heavy objects that may be unstable and could suddenly shift and trap or crush you.
- Do not use lifts even if still operational and backed up by generator.
- Evacuate all enclosed spaces when water level is rising.

Appendix E to Annexe III

Protective measures

Preparation & deployment of sandbags

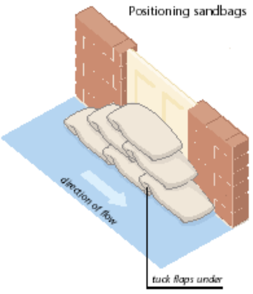
Sandbags are one of the most well-known devices for keeping floodwater out of your property. Unfilled sandbags and a supply of sand can be purchased from some DIY stores and Builders Merchants, but remember that if there is a flood in your area demand may exceed supply as people rush to buy them. Some local authorities may provide sandbags in an emergency, but again there may be limits to availability.

If you have not purchased sandbags and sand in advance, you can use alternatives such as pillow cases or refuse sacks and fill them with garden soil. Remember that they can get heavy quickly, so do not overfill, or fill them too far away from where you want to position them.

How to Fill and Position Sandbags

- Unless you have access to a sandbag filling machine, this is a two person job: one to hold the bag open and one to fill.
- Sand is abrasive – both people should wear protective gloves.
- Do not fill bags more than half full.
- It is not necessary to tie the end of the bag.
- Remove any debris from the area where the bags are to be placed.
- Place the half filled bags lengthways and parallel to the direction of the water flow. Tuck the opened end under the filled half of the bag and position it pointing into the water flow.
- Place bags in layers. Like a brick wall, make sure that in the next layer each bag overlaps the one below by half.
- Stamp bags firmly into place to eliminate gaps and create a tight seal.

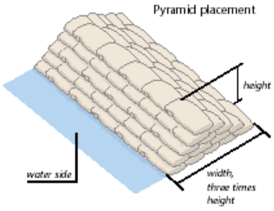
Positioning sandbags



Pyramid Placement Method

If you need to create sandbag protection that is more than three layers high you will need to build in a pyramid style. For the structure to be stable, you should build the 'sandbag wall' three times as wide as you need it to be high. It will also be more effective if you alternate the layers lengthways and crosswise. Stamp each bag in place and tuck the loose end firmly under the filled portion of the bag.

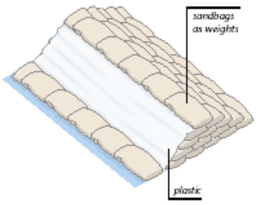
Pyramid placement



Additional Waterproofing

Lay plastic sheeting across the side of the 'sandbag wall' that will face the floodwater. Weigh down with additional sandbags. .

Additional waterproofing



Remember!

Sandbags are popular but they have disadvantages:

- During an emergency sufficient quantities may be difficult to obtain
- They are time-consuming and require two people to fill
- They can be difficult to handle, particularly for the elderly or infirm
- When they come into contact with floodwater they tend to retain contaminants such as sewage
- Sacking material is biodegradable, and will disintegrate if left in place for long periods of time

Flood boards can avoid some of these drawbacks

Preparation & deployment of flood boards & other methods

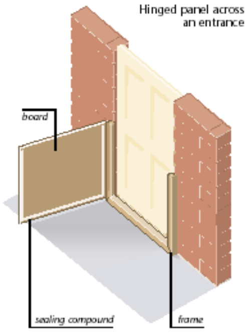
How to Make and Use Flood Boards

The most basic method is to construct a strong wooden or metal barrier that is secured flat against the wall or frame surrounding a door or window. The pressure of floodwater itself will help seal the barrier. This can be enhanced by adding suitable material to make a seal between the wall and the board, for example a blanket or silicone type sealing compound.

The efficiency of makeshift flood boards will depend on the strength of the walls and the durability of the fixings used to secure the wooden or metal panels.

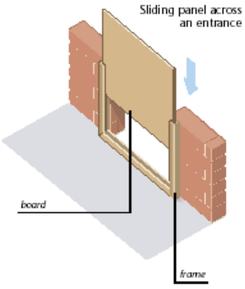
Purpose-made flood boards for doors, windows and air bricks will be more successful than sandbags for minimising floodwater entering a property. They are available commercially, but can be easily made by someone with DIY knowledge. In either case the product or materials will need to be purchased and installed in advance of a flood.

Hinged panel across an entrance

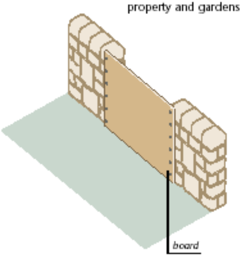


Most commonly, this type of flood board will comprise a frame and board or panel. Retaining fixtures may need to be a permanent feature of the property, but the frame and gate can be removed and stored when not in use. If a flood is imminent, most can be installed in a matter of minutes.

Sliding panel across an entrance



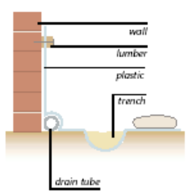
Using boards to prevent floodwater entry to property and gardens



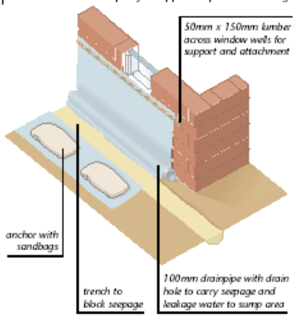
This is an advanced method of reducing the effects of floodwater by enclosing the bottom 600-900mm of a property in plastic sheeting.

The process requires some DIY ability, plenty of suitable materials and enough time to construct the wrapping prior to the property being affected by flooding. It is a method you need to consider and prepare for well ahead of any potential flooding alert.

Side view



Property wrapped in plastic sheeting


50mm x 150mm lumber across window wells for support and attachment
anchor with sandbags
trench to block seepage
100mm drainpipe with drain hole to carry seepage and leakage water to sump area

Hazard!

Do remember that in cases of very severe flooding (where the floodwater is more than one metre deep) keeping water out of your property can do more harm than good. Unless your building is specifically designed to withstand such stresses, the hydrostatic pressures involved with deep water can cause long-term structural damage and undermine the foundations of a property. Therefore you should not aim to prevent water from entering your property through any windows, doors, airbricks etc. more than one metre above the level of the ground surrounding the property.

Also consider the type of soil on which your property is built. If it is porous (eg chalk) and a water table lies immediately below the ground, it is very likely that in times of flooding water will rise up directly into your property through the ground floor. In these circumstances it is better to spend your time removing possessions to a safe place, rather than wrapping your home.

Annexe IV: Extract from CEN 50600-1 – Availability

5 Business risk analysis

5.1 General

The overall availability of a data centre is a measure of the continuity of its data processing, storage, and transport functions. The acceptable level of the overall availability of a data centre is determined by a number of factors including:

a) a downtime cost analysis (see 5.2) - the cost associated with a failure of service provision, which depends upon a number of factors including the function and importance of the data centre;
b) externally applied commercial pressures (e.g. insurance costs).

There is a link between the availability of the infrastructures specified in EN 50600-2 standards and the overall availability but it should be recognised that the recovery of intended data processing, storage, and transport functionality following the repair of an infrastructure failure depends on many factors related to the configuration of the hardware and software providing that functionality.

As a result, the role of the infrastructure is to support overall availability objectives but is not the sole factor in their attainment.

The availability of each of the facilities and infrastructures of the data centre required to support the desired overall availability is described by an availability classification (see 7.2). The design of each of the data centre infrastructures shall take account of their impact on overall availability and the costs associated with the predicted downtime associated with failure or planned maintenance.

The design and physical security of the facilities and infrastructures of the data centre may be subjected to a risk analysis (see 5.3) which maps identified risk events against the requirements of the availability classification (see 7.2). The availability classification for each infrastructure is described as providing low, medium, high and very high availability. Clause 7 further describes the situations (risk events) for which each infrastructure is protected against failure. Other approaches are to apply “% availability” to infrastructures but this is not supported by this standard series for reasons explained Annex X.

This analysis identifies the aspects of the facilities and infrastructures that require investment in terms of design improvements to reduce their impact and/or probability of those risk events.

Annex X

Overall availability and infrastructure availability (informative)

At its simplest level availability (A) is defined as:

$$Availability(A) = \frac{Uptime}{Downtime + Uptime} \qquad \text{Equation X.1}$$

The availability may be described in percentage terms (see Table X.1).

Table X.1 - Availability and annual downtime

Availability (A)	Common reference	Downtime

		(based on a 365 year)
90 %	1-nine	36,5 days
99%	2-nines	3.65 days
99.9% (3-nines)	3-nines	8,76 hours
99.99% (4-nines)	4-nines	52,6 minutes
99.999% (5-nines)	5-nines	5,3 minutes
99.9999% (6-nines)	6-nines	31,5 seconds

When applied to the overall availability of a data centre, such a percentage objective based on Equation x.1 may be valid. However, a percentage approach is not applicable to describe objectives for the infrastructures required to support that overall availability. A discussion of availability in terms uptime and downtime hides some fundamental problems for a given infrastructure. It is necessary to introduce the concept of mean time between failure (MTBF) and the mean time to repair (MTTR) following that failure. This is highlighted in the example below.

> As can be seen in Table X.1, an infrastructure with an availability of 99.99 % allows for approximately 53 minutes downtime per annum. While this might be a single 53 minute period of downtime with an MTBF of approximately 365 days, it could equally be 53 separate occurrences of one minute periods of downtime (or even 3150 separate one second periods of downtime with an MTBF of approximately 3 hours).
>
> A failure of power supply to ICT equipment of 1 second would almost certainly result in shutdown of the equipment. The additional time for the data centre to recover its intended functionality for data processing, storage, and transport would depend on a number of factors which would render the overall availability to be substantially lower than 99.99 %. This shown in Figure X.1 for 10, 100 and 1000 periods of downtime.

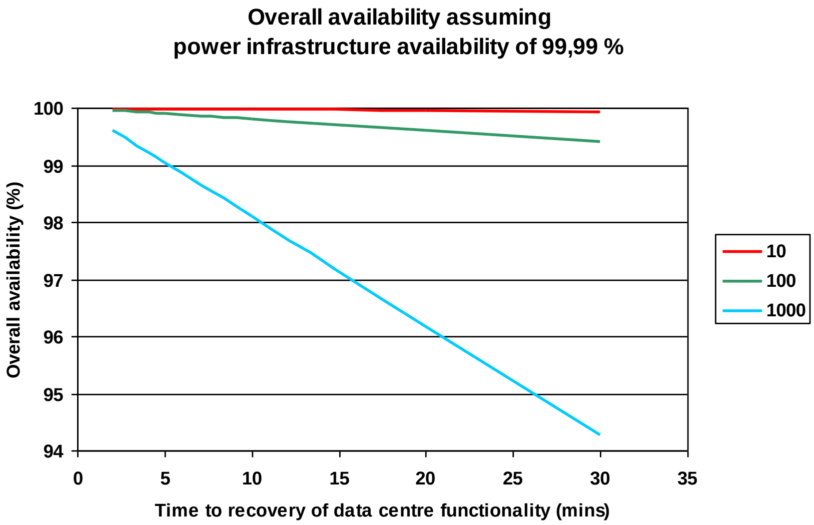


Figure X.1 - Impact of recovery of functionality on overall availability

> Reversing this calculation for a given infrastructure, the achievement of a given overall availability would not only require an infrastructure availability many times better than the overall availability but would also place demands on the number of periods of downtime and the time to recovery of functionality which has no relevance to the infrastructure.
> In the above example, if the number of periods of downtime was limited to 5 and the time to recovery of functionality following each period of downtime was restricted to 10 minutes then the availability of power supply and distribution system would have to be 99.9995 %.

For a given infrastructure it may be better to consider a modified formula for availability, A,

$$Availability(A) = \frac{MTBF}{MTBF + MTTR} \qquad \text{Equation X.2}$$

When represented in this way it is clear that an infrastructure with a longer MTBF (i.e. a lower frequency of failures) will have a greater availability and the MTTR will have a different effect depending on the value of MTBF. However, it should be noted that the demands for MTTR vary substantially for different infrastructures. As described in the example above when determining likely impact, the power supply and distribution (EN 50600-2-2) needs to address MTTR in the sub-second (or even milli-second) range to avoid ICT equipment shut-down. In extreme cases, a sub-second failure of the power supply and/or distribution system with a sub-second MTTR could potentially result in an overall data centre service downtime (MTTR) of several hours or even days. By comparison, the environmental control (EN 50600-2-3) system would typically only require MTTR values in the minute (or multi-minute) range without any effect on overall data centre availability. Therefore the application of a single value for infrastructure availability is non-viable.
Clause 7 describes availability classification for each infrastructure as providing low, medium, high and very high availability because:

- overall availability of the data centre cannot be directly related to the availability of individual infrastructures;
- availability of infrastructures cannot be directly compared, in percentage terms.

Clause 7 further describes the situations (risk events) for which each infrastructure is protected against failure i.e. by increasing MTBF and reducing MTTR (in availability Class 4 to zero).