Annex 4.9

OUR APPROACH TO RESILIENCE

The resilience of our network and operations underpins the critical services we provide to customers. Our resilience journey into the 2023-28 period and beyond requires us to continue to successfully adapt to external threat factors in an evolving and increasingly challenging landscape.

Resilience is embedded in our core values as a business and across our plan

Remaining resilient requires us to consistently conduct ourselves to the highest business and operational standards in terms of threat recognition and mitigation. Any significant failure to foresee risks and mitigate impacts can have serious consequences for our customers, and our business.

The external threat landscape is constantly evolving, whether that is from the decarbonisation transition presenting new challenges, changing weather patterns or the ever-present risk of malicious physical or cyber-attacks. We undertake regular threat assessments, analysis and modelling to assess risks and we carry out proactive business adaptations and asset hardening to mitigate impacts. We regularly drill our operational resilience plans and ensure long-term resilience is embedded in our asset replacement plans so that the assets we install today are fit for the environment in which they will be operating in the future.

Our approach to resilience cuts right across our business and is embedded in our six core business values (see Figure 1). They form the foundation for how we ensure our performance is robust in every way we deliver for our customers.

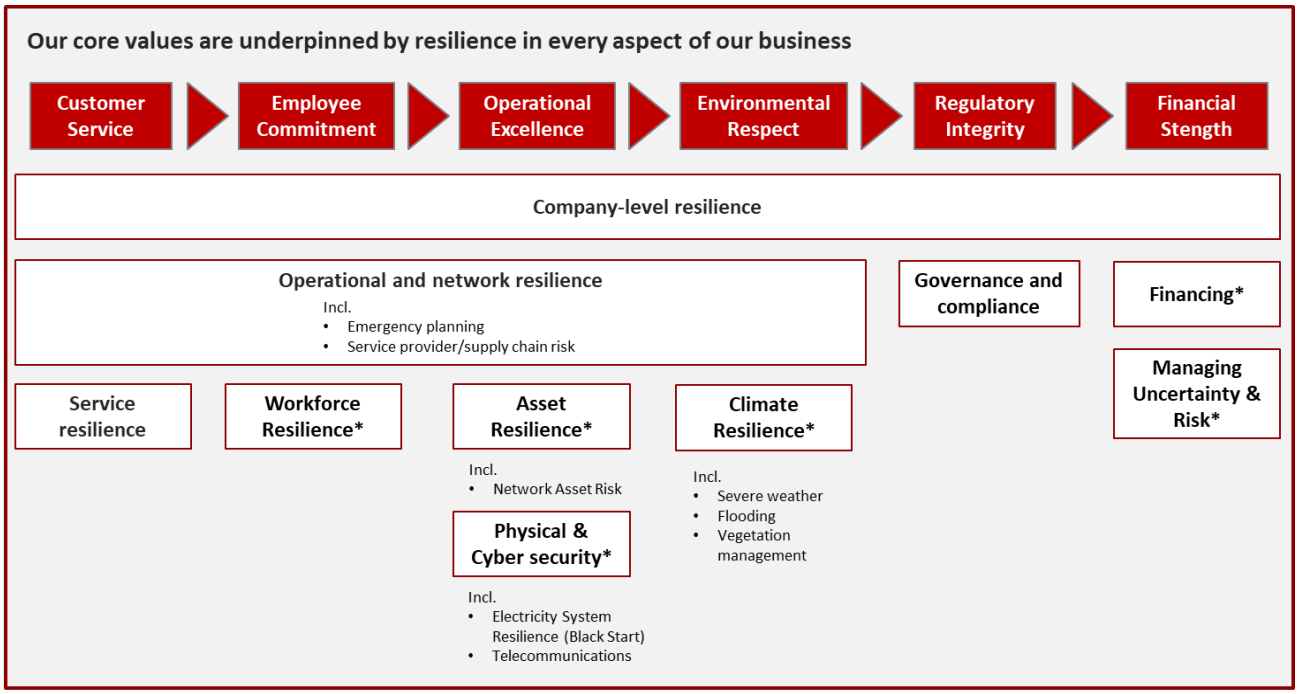

Figure 1 – Resilience in our 2023-28 plan

Resilience is addressed in a number of areas of our 2023-28 plan including the following strategies and business plan sections:

- climate resilience strategy
- asset resilience plans and Network Investment Strategy
- physical and cyber security plans;
- workforce resilience strategy
- financing
- our approach to managing risk and uncertainty

In this annex we explain aspects of our approach to resilience, covering in more detail those areas that are not set out as specific sections of our plan. We cover in turn:

- the growing importance of resilience;
- key aspects of our approach; and
- the evolving resilience landscape.

The growing importance of resilience

Our stakeholders are placing increased reliance on resilient power supplies

Resilience has been a key theme throughout our engagement with stakeholders. The greater reliance our customers will have on electricity as they decarbonise (e.g. for heat, transport and personal communications) increases their vulnerability to disruption from power loss.

Below are the key messages we have heard from our stakeholders:

- employ a resilient workforce which is there when it is needed - whatever the weather;
- continue to perform well and serve our customers during any crisis or disruption;
- recover quickly from any unplanned power interruption whatever the extent or cause;
- reduce the impacts of increasingly frequent severe weather upon our assets;
- minimise the risk of flooding to our assets;
- manage any external factors (such as vegetation infestation) which might contact live conductors and disrupt supplies or cause harm;
- protect ourselves from cyber security breaches by ensuring information technology (IT) and information system vulnerabilities are promptly identified and mitigated; and
- provide resilient IT and telecommunications to our workforce so that we can continue to operate successfully during any loss of mains power.

The growing reliance on electricity supply has been illustrated and underlined during the 'work from home' phases of the COVID-19 pandemic. The need for resilience to continue to be tackled through a government coordinated multi-agency approach was clearly demonstrated when we played our part in rapid deployment of the NHS Nightingale hospitals, oversight of power supplies to intensive care units and coordination with the designated COVID-19 vaccination centres. A 2018 report written by the Energy Research Partnership on the resilience of the UK electricity system highlighted the increased reliance upon electricity in today's communities[1] (see Figure 2):

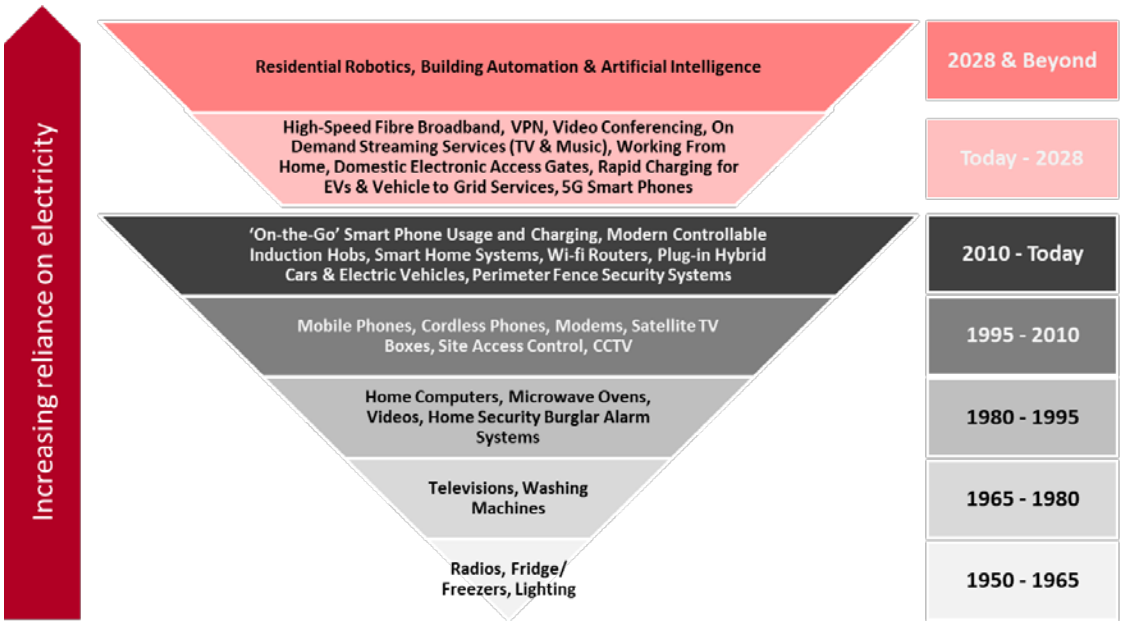

Figure 2 – Increasing stakeholder reliance and dependence upon electricity
(Adapted from the 'Energy Research Partnership' Report on the 'Future Resilience of the UK electricity system' - November 2018)

It is clear that the resilience of our power distribution service must improve to stand still in order to deliver to our customers' expectations.

[1] 'Energy Research Partnership' Report on the 'Future Resilience of the UK electricity system' - November 2018

Power system resilience will undergo rapid development as the nation decarbonises

The UK electricity system has seen significant change over the last decade with a trend towards decentralisation of generation, a rapid increase in intermittent renewable generation, flexibility being pursued as a solution for constrained networks and increased electrification of other critical infrastructures and sectors. There is a growing trend of society and businesses becoming increasingly reliant upon new technology, broadband and communications; all requiring electrical energy and ultimately leading to an increased interdependency between sectors.

In parallel, our operating context is evolving and changing; from climate change inducing more frequent extreme weather events, through to an increase in malicious intent to affect networks.

As a long-term outcome of the P2/7 electricity network planning standard for system security and interconnection, customers of the UK electricity system have enjoyed high levels of power supply reliability and resilience predominantly through duplication of source feeders and interconnection, particularly at higher voltages. Electricity networks continue to improve, providing a high degree of confidence to businesses and consumers that power will be available 24 hours a day, seven days a week, 365 days per year. However, a reliable electricity system is not necessarily a resilient one.

Reliable day-to-day network operation during normal circumstances is expected, but we must continue to improve our operational response capabilities (both in terms of preparedness plans and workforce responsiveness) to continue to be able to successfully deal with greater extremes in weather and more frequent disruptive events.

The decarbonisation transition will bring with it new dynamics for UK security of supply, making it necessary to ensure that any new infrastructure is built with the inherent level of resilience required to meet future needs.

The decarbonisation of heat and transport will introduce further complexity to the electricity system by increasing dependencies on electricity across many infrastructure sectors, and new energy vectors such as hydrogen will present new interactions and challenges. In addition to this, we should expect a rapid increase in the number of assets and different owners in the electricity system (such as domestic power generation) to continue.

In the future, the electricity system will impact an even wider range of technologies dependent on power, which in turn is likely to have a much larger impact on society than in the past, even for relatively localised unplanned power interruptions.

With these resilience-driving factors in mind, we expect that from now until 2028 and beyond, power system resilience will need to undergo more rapid development than we have seen at any point in our history so far.

Key aspects of our approach

UK Government central oversight of the National Risk Register (NRR) provides the backbone for energy sector resilience

The Department for Business Energy and Industrial Strategy (BEIS) facilitates integrated UK leadership and governance over energy sector resilience.

The Energy Emergencies Executive (E3) is the principal stakeholder in terms of UK electricity system resilience. The E3 sets and enacts resilience policy through its Committee (E3C) and sub committees which are the main forums for identifying the processes and actions necessary to prevent and handle emergencies affecting the supply of gas and/or electricity to consumers in the UK. E3 is tasked with providing assurance that adequate pan-industry and government emergency planning arrangements are in place and all participants are suitably trained and exercised as appropriate. E3C reports to E3 and is the main forum for delivering the agreed work programme, principally through a number of task groups, which currently comprise:

- electricity task group;

- Black Start task group;
- gas task group;
- cyber security task group;
- security task group; and
- communications task group.

Northern Powergrid is a leading participant in the E3C and its subcommittees.

The NRR is a key tool that keeps all parties focused and aligned on energy resilience (see Figure 3).

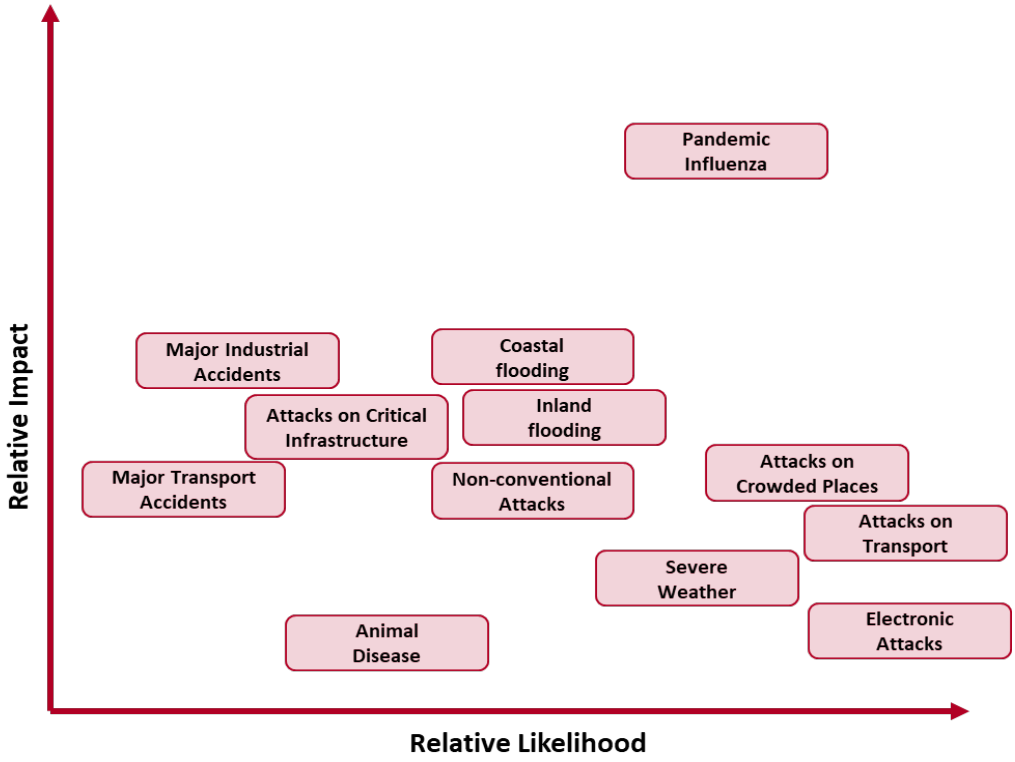

Figure 3 – Risk/Threat assessment adapted from the UK National Risk Register (NRR) December 2020 – unclassified version

We have an obligation to provide a resilient service under The Civil Contingencies Act (2004) (CCA)

The CCA places legal and statutory obligations on UK utilities to be resilient and responsive in emergency situations. As an essential public service, our customers and stakeholders have every right to expect from us a robust power delivery service which is resilient to and able to bounce back quickly from major events which test and challenge our durability under unusual or abnormal circumstances. We take both the spirit and the letter of these CCA obligations seriously. In the 2023-28 period we will continue to meet any new and emerging threats via tried and tested methodologies and plans which we have proven are fit for purpose.

Collaboration is at the heart of our approach

As a category 2 responder under the CCA, we work constructively with central government (BEIS) and the seven Local Resilience Forums in our service territory on a multi-agency basis to ensure we have a firm grip on the threats, risks and issues which feature on the latest version of the NRR administered by BEIS. This routine, structured and enduring stakeholder engagement allows us to plan and formulate 'joined up thinking' to drive coordinated responses to

emergency events that bring about or involve disruption to power supplies. This strong industrywide collaboration allows us to learn about situational exposures, insecurities or vulnerabilities that need proactive and proportionate mitigation, and to build actions into our business planning to further enhance our resilient network over the long term.

We set and uphold high company-level standards for resilience

Our shareholder, Berkshire Hathaway Energy (BHE), sets and upholds group-wide grid resilience standards against which we are audited and tested on an annual basis. This has taken us to the next level of preparedness. Through this approach we benefit from shared learning and formalised best practice on grid (network) resilience and grid improvement collaboration with our international group of companies.

At the company level, our Risk Advisory Board (RAB) reports into our Board of Directors. It is chaired by one of our non-Executive directors and ensures that our resilience approach remains current, proportionate and complete. This covers UK level threats included in the NRR and also any threats unique to our service territory that have a more regional or local focus. The RAB oversees update reports from both the Asset Risk Management Group (which deals with long term network resilience improvement) and the Emergency Planning Coordination Group (which oversees the effectiveness of our portfolio of operational response plans), while reviewing our response plans for top company-level risks such as cyber security.

Resilience doesn't just include the practical elements of network operations and service delivery, it extends into every aspect of how the organisation is run. We have clear delegations of authority for decision approvals, and strong policies in our controlled documentation system to ensure we remain compliant. In particular we aim to ensure that our conduct stays on the right side of protecting our reputation for open and transparent business ethics with appropriate speaking up mechanisms in place for any concerns to be raised.

We have established routines for operational and network resilience that underpin service delivery for our customers

We aim to maintain constant vigilance and readiness, even if that means we occasionally prepare and deploy our teams to address events that turn out to be low impact. Through continuous learning and good practice sharing with both UK resilience stakeholders and companies in the BHE group, we have built a portfolio of over 30 mature, modular, actionable operational response plans that we periodically review, drill, test or exercise to ensure we remain prepared and ready (see Figure 4 below).

Every one of our plans is subject to a formal review on not less than a three-year cycle. Our objective is to ensure that new, emerging, evolving or increased threat factors or threat levels are met with a proportionate level of preparedness.

Our operational response plans contain trigger criteria which (when forecast to be met in the near term) drive the extent of incident leadership, command and coordination that is warranted. We proactively move through controlled escalation stages of awareness, preparation, readiness and mobilisation as each trigger criteria is met or satisfied. In this way we are becoming more practised at switching between normal 'business-as-usual' operations and emergency response modes. For certain types of disruptive event, it can also be necessary to have a specific recovery phase to allow a smooth transition of resources back onto normal routines.

After major events (such as severe flooding) we follow a standard cycle to learn lessons and improve the outcomes for customers and stakeholders:

- review impact, damage and performance;
- identify gaps;
- learn from failure modes;
- develop mitigations and solutions for future events; and
- exercise, practice and drill.

The disciplines of crisis management, business continuity and disaster recovery are pivotal to supporting any recovery from disruption. Managing through a disruptive event requires our business support activities to be underpinned by 'back up/alternative' resilient infrastructures so that we can continue to be there when we are needed for both our electricity customers and our power system stakeholders. Rapid use of our 24x7x365 hour contingency standby sites enabled our control, dispatch and contact centre operations to be readily partitioned during the COVID-19 pandemic (to lessen the risk of cross team infection), illustrating the value of these previous resilience-driven service infrastructure investments.

In the 2023-28 period, for each of the identified new and emerging threats, we expect to promptly calibrate our controls and develop our proficiency in moving as seamlessly as possible between normal and emergency operations.

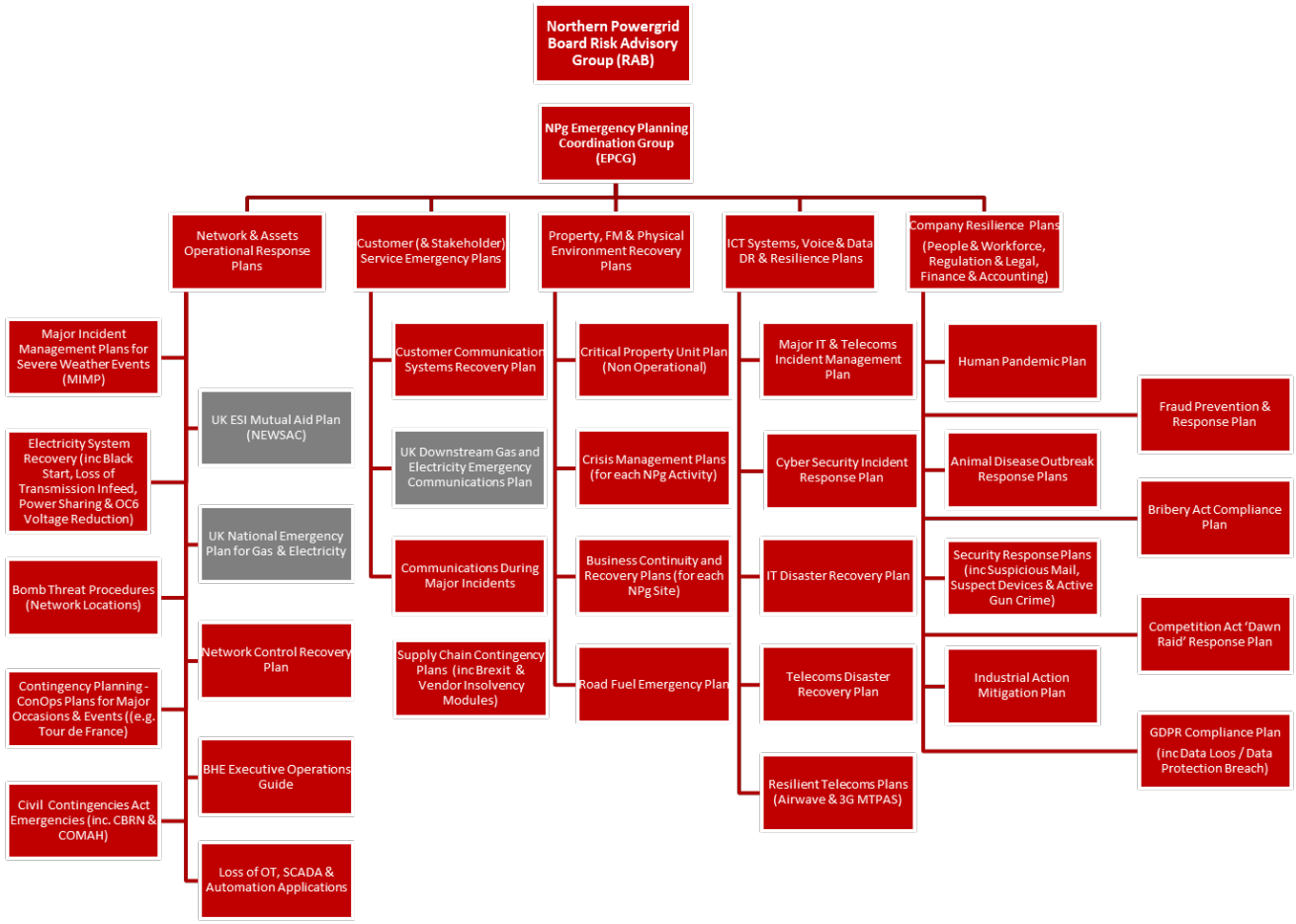

Figure 4 – Northern Powergrid's portfolio of actionable operational response emergency plans

The evolving resilience landscape

A dynamic threat landscape in the 2015-23 period has strengthened our approach to resilience

The 2015-23 period has remained highly active on the severe weather and flooding threat vectors. We have made significant investments in flood defences since 2015 as an area of high priority for our stakeholders, increasing our resilience levels, particularly in areas of high flood risk and criticality. Security of supply is actively on the agenda with action plans mobilised as part of the Black Start Task Group and in response to the August 2019 National Low Frequency Demand Disconnection incident. Business continuity plans for UK businesses, in general, have been stress tested by both the COVID-19 pandemic and the Brexit transition, with the pandemic revealing that resilience in the care sector is in need of attention and investment.

A brief summary of some of the significant recent events that have shaped our resilience priorities in the current regulatory period is set out below.

Storms Desmond and Eva – December 2015 flooding events/national flood resilience review (NFRR)

Storm Desmond in early December 2015 led to extensive flooding and widespread sustained loss of power in Lancaster, North West England. Later in the same month Storm Eva brought extensive flash flooding at Calderdale, Leeds and York, with a modest localised short duration impact upon supplies. At York, where the River Foss flood barrier failed, a major telephone exchange facility was flooded having widespread, sustained impact on voice and data mobile services, which in turn led to Government involvement in the recovery and aftermath. Following Storms Desmond and Eva the Government produced the NFRR. While the majority of the electricity network had been protected and was not affected by the flooding, the review recommended the flood protection standards were updated to protect substations that serve more than 10,000 customers. These recommendations were then carried forward by the industry and included in an updated version of Engineering Technical Report 138 which was published in 2018.

Beast from the East – February 2018

A winter weather system known as the Beast from the East impacted much of the UK with sustained sub-zero temperatures, significant levels of snowfall and windy conditions. Widespread travel and access issues continued over an eight-day period. During the event, significant numbers of staff were required to work from home leading to congestion on our remote virtual private network (VPN) connections. A post-incident improvement led us to increase the capacity and resilience of our VPN connections enabling us to operate fully during the COVID-19 pandemic.

National Low Frequency Demand Disconnection Incident – August 2019

On 9 August, 2019, over one million customers were affected by a major power disruption that occurred across England, Wales and some parts of Scotland. Though the power disruption itself was relatively short lived with all customers being restored within 45 minutes - the knock-on impacts to other services were significant. Formal investigations were carried out post-event by BEIS and Ofgem to understand the cause of the incident and lessons for the industry to learn. In particular, they considered the performance of National Grid electricity system operator (ESO), National Grid electricity transmission (NGET), distribution network operators (DNOs) in England and Wales and the two generators involved.

Brexit Transition – December 2018 through January 2021

Progressively from late 2018 through to the present we made and executed business continuity plans to deal with any foreseeable potential impacts from the UK's withdrawal from the European Union. The prime focus of our attention was to take steps to protect our supply chain from any potential disruption caused by the exit. A key part of the preparation both internally and for the wider energy sector was a series of bilateral interactions with the BEIS Resilience Team to allow information sharing and for us to provide evidence to BEIS of our preparedness. This engagement led to us holding an exercise in October 2019 to test our Road Fuel Emergency Plan ahead of the risk period.

COVID-19 Pandemic – March 2020 through June 2021

We successfully adapted our day-to-day operations, workforce arrangements and support infrastructure to maintain service levels during the COVID-19 pandemic. Many of these adaptations will be retained as we emerge from the pandemic. We also played our part in expediting power supplies to the two Nightingale NHS facilities in our service territory. We segmented our region's NHS intensive care facilities from our priority customer data and engaged directly with NHS counterparties over assurance of power supply integrity for the COVID-19 peak periods. We intend to follow up with a specific COVID-19 lessons learned exercise with this ring-fenced group of stakeholders.

SolarWinds (December 2020) and Colonial Pipeline (May 2021) cyber security breaches

We have made strong progress in enhancing our cyber security defences in the 2015-23 period however the threat is ever-present. These two successful cyber-attacks against operational technology control systems marked intensification

in our level of concern for the security and resilience of energy infrastructure installations. Up to this point the IT security against hackers in developed first world countries had been largely successful in defending against intrusion.

Suez Canal Shipping Disruption – March 2021

The multi-day blockage of maritime freight traffic through the Suez Canal again highlighted the importance of resilient supply chain design, coupled with effective contingency plans for any failure in our ability to import goods from international locations.

The threat landscape will continue to evolve in the 2023-28 period

The outlook for resilience will see new and emerging challenges for us to recognise and navigate. While it is impossible to foresee and predict individual discrete disruptive events, some examples of further areas where we expect to be actively challenged are set out below:

Flood impact prevention – the next phase of our resilience investment

Our plan continues with our programme of works to ensure all EHV substations meet the recommended specification of ETR138 for flood resilience. We will remain responsive to upgrades or system upgrade work that will be required as customer numbers and utilisation of the networks rise, increasing the importance of adequate flood protection for our substations. Our plan also expands our programme to include flood protection for distribution substations which provide supplies to critical sites.

Vegetation Management – contending with the impact of Ash Dieback

Since 2018 the sector has been working to update Engineering Recommendation ETR136 to cater for 'Ash Dieback'. The Tree Council prediction is that up to 90 per cent of all Ash trees in the UK could be impacted within 10 years. Ash trees, as a species, account for 30 per cent of the UK tree population. Our climate resilience strategy sets out our plan to address this risk as part of our vegetation management programme in the 2023-28 period, mitigating immediate threats to overhead line circuit integrity that could be exacerbated by severe weather wind events.

Black Start capability – next phase of resilience investment

During the 2023-28 period, all of our remaining substations identified as being equipped with electromechanical relays will be upgraded. This will require the battery installation to be updated to meet the requirements of Engineering Recommendation G-91. Since 2016, BEIS have been working with the sector to develop a mandatory resilience standard for Black Start. The primary aim of the standard is to formally introduce a timescale for the recovery from a Black Start. This standard will introduce a restoration standard of 24 hours for 60 per cent, and five days for 100 per cent, of national demand. As of June 2021, the draft standard is awaiting approval from BEIS.

Telecoms resilience – impact of communications network infrastructure changes

As commercial telecommunications systems become increasing reliant on electricity networks it highlights that it is becoming more difficult for network operators to solely, or predominantly, rely on commercially-provided telecommunications networks since they are not adequately resilient to a loss of power. Our plan responds to a number of resilience-depleting communications impacts on DNOs that are anticipated during the 2023-28 period, including:

- gradual 'switching off' of the public switched telephone network (PSTN)
- phasing out of the Airwave (the emergency communications systems used CCA responders) by 2025
- lower coverage and resilience from 5G cellular communications; and
- radio Interference from continental Europe.

To address this multi-faceted issue, the Office of Communications (Ofcom) is undertaking a study to consider the need for energy utilities companies to have a proportion of radio spectrum allocated for their use. Similarly, the Energy Networks Association Strategic Telecommunications Group has been working with government departments to evaluate the opportunities for resilient telecommunications and explore how the sector's future needs can be met.

Flexibility – realising resilience benefits while upholding safety standards

The development of more flexibility options associated with the network will improve the resilience mitigation options available to us going forward. We will ensure that protection schemes continue to ensure safety comes first with every incremental smart installation or flexibility contract. The importance of new smart technologies being designed to be failsafe will be paramount.

Trade/tariff wars leading to de-globalisation of supply chains

We anticipate that the friction between the USA and China over trade tariffs and infrastructure cyber security, and the longer term opportunities and consequences of the UK's post Brexit free trade arrangements, will continue to drive the need for more control over supply chains where they are critical to business continuity arrangements for DNOs. As a minimum, we expect that contingency planning for more 'local and freight/visa friendly' sourcing of goods and services will become necessary.

We must continue to remain alert to high impact/low probability events

Our risk management practices are structured to cover a wide range of high impact/low probability disruptive events. In a five year regulatory cycle we would expect to encounter numerous disruptive situations, for example:

- Significant infrastructure incidents (e.g. fires and explosions which require network safety isolations; embargoes from accessing unsafe or unstable structures, especially tunnels and bridges; and subsidence, sink holes, landslides and ground erosion which undermine our circuits and assets);
- Transport system disruption (e.g. fuel supply problems; traffic congestion and gridlock); and
- Land exclusions and property access denial (e.g. human and animal disease outbreaks; toxic spills and leaks).

It has become second nature to us to learn from unusual and previously rare events, and where they begin to show patterns or trends we put together plans for dealing with similar incidents going forward.

Figure 5 shows a mapping of resilience risks against indicative threat timelines.

	CUSTOMER SERVICE	EMPLOYEE COMMITMENT	OPERATIONAL EXCELLENCE		ENVIRONMENTAL RESPECT	REGULATORY INTEGRITY	FINANCIAL STRENGTH
Resilience Threat Timeline / Disruptive Event Frequency	*Customer Service Threats & Risks*	*Workforce Threats & Risks*	*Operational Risk – Network & Assets*	*Operational Risk – IT, Telecoms, Data & Physical Security*	*Environmental Risks & Threats*	*Regulatory & Legal Risks & Threats*	*Accounting & Finance Risks & Threats*
Continuous / Ever Present	Corporate / Company / Organisational Exposures						
Daily / Weekly	Service Resilience – Contact Handling & GoS issues	Workforce Resilience - unfit for duty	Asset & Network Resilience Routine faults & power loss	Cyber Security – Defence Vs Threats	Environmental Resilience / Streetworks	HSE Enforcement Risk	Cash Flow & Foreign Exchange Currency Risk
Monthly, Quarterly or Seasonally	Escalated PSR / vulnerable customer issues	Supply Chain Service Partner Performance Issues	Asset health/condition risks	Physical Security Alarm Response to Tresspass / Vandalism	Tree Cutting - Vegetation Reinfestation	Environment Agency & Defra Enforcement Risk	Energy Supplier Revenue Risk
Annually or Bi-Annually	Host Service faults (e.g. telephony / PSTN / 3G / Website)	Employee Lost Time Injuries	Severe Weather Events	Disruption to Telecomms Services – WAN / LAN Failures	Flooding Events / Land Erosion / Ground Subsidence	Ofgem Licence Compliance Risk	Inflation, Interest Rates, Corporation Tax impacts
Rarely – Typically Every Five or Ten Years	High volume contact call overflow events	Industrial Disputes or Strike Action	Voltage Reduction / Demand Disconnection	Physical Security – Intruder leading to harm	Animal Disease Outbreaks / Tidal Surge & Coastal Erosion	Election Risk / CMA Risk	Price Control Risks
Ultra Rarely – Once or twice Per Career	Harm to customers from power loss or electrocution	Pandemics & Long Term Health Issues (e.g. Asbestos)	Power Sharing Events / CNI Site Incidents	Data Centre Outage / UK Network Service Collapse	Seismic Events (Earthquakes & Volcano Ash Cloud Impact)	Major Fines or Penalties Risk	M&A Risk / Financial Crash Risks
Never Yet	Total service failure – all customer contact lost	Harm to employees (e.g. Legionella)	Major Loss of Power Generation & Transmission - Black Start	Major UK Power Loss due to security breach (Terrorism or Sabotage)	Space Weather Risk	Licence Loss or Forfeiture Risk	Insolvency or Bankruptcy Risk

Figure 5 – Resilience Risk Mapping

We will continue to adapt our network and operations to emerging threats in the 2023-28 period

While we know we will never be finished as far as improving our resilience is concerned, our approach means we are progressively building strength, competence and capability in navigating threats and challenges that bring about disruptive impacts.

Our track record gives confidence for the resilience of our network and operations in 2023-28 as we navigate through the significant changes in the decarbonising energy system. What is clear is that we will need to continue to adapt to 'new normal' situations that develop and test our resilience. Our overarching approach and specific resilience plans for the period mean our customers can have confidence that we will continue to deliver a power delivery service they can depend on.