Engagement Log: Resilience
NGET_A10.01_Engagement Log
December 2019

As a part of the NGET Business Plan Submission

nationalgrid

A10.01 - ENGAGEMENT LOG
Priority: I want the network to be protected from external threats

Author: Jade Ison
Document Version Number: 5

EXECUTIVE SUMMARY

Our Stakeholder priority of ***'I want the network to be protected from external threats'*** focuses on the importance of both enhancing and maintaining resilience of our network to ensure our assets are protected from unforeseen events such as cyber-attack, physical-attack and damage caused by extreme weather. It also focuses on ensuring we maintain a resilient network so that we can effectively respond and recover from incidents caused by external threats.
Stakeholder engagement in this area is necessary to determine both desired and required levels of resilience of our network. Engagement in this area has included stakeholder workshops to understand and determine priority focus areas as well as developing an understanding of the industry view on current and future threats posed by cyber and physical attack. We has also conducted consumer willingness to pay research in relation to recovery times in responding to incidents caused by threats.

We engage with industry through a number of industry working groups, which focus on either an element of resilience, or an approach for holistic resilience management, such as the London Resilience Forum, E3C Cyber Resilience Task Group, and the Energy Networks Association Resilience and Emergency Planning Group. This has allowed us to gain an insight into industry thinking and practise regarding resilience, which has been fed into our plans for RIIO T2.

Unfortunately, a few of the topics under this stakeholder priority are either of a confidential or sensitive nature, and therefore we cannot engage in detail with all stakeholders, specifically on the topics of cyber and physical attack. To develop our T2 plans, we are ensuring we engage with the specialists or authorities, such as BEIS, the NCSC, the CPNI and Ofgem who have relevant knowledge or information to help us determine required investments. We do however inform and consult with our wider group of stakeholders on our approach to be as transparent as possible.

CONTENTS

1. PRE-ENGAGEMENT

1.1 WHAT IS THE TOPIC AND WHY IS IT BEING ENGAGED ON?

The stakeholder priority of ‘I want you to protect the network from external threats’ covers all the investments required to both enhance and maintain the resilience of the electricity transmission system to ensure it is protected from a multitude of threats. These threats comprise extreme credible events such as weather (including flooding), cyber-attack or physical-attack. These events could impact our ability to provide a continued supply of energy to end consumers. This stakeholder priority will also cover the investments necessary to effectively and efficiently respond and recover from such incidents to restore power supply to end consumers as soon as possible.

Over recent years there have been significant changes in the threat environment in some areas brought about by such factors as advances in technology and changing threat actors (individuals, member states or organisations posing a threat). Due to the potential impact of a successful cyber or physical attack on our system, we must ensure it remains effectively protected by adapting and responding to the continual changes in the threat environment. The importance of protecting our network against these threats is supported by our stakeholders.

Within our RIIO T1 business plans, both security of sites and security of IT systems were areas in which outputs were uncertain for the eight-year period. Ofgem allowed uncertainty mechanisms in 2015 and 2018 for NGET to recover costs for required works on physical site security. There was no equivalent mechanism for NGET to recover costs to enhance security of IT systems. Due to the change in threat landscape and requirements for enhanced security, the need for investment in these areas increased significantly within the RIIO T1 period. Cyber risks also emerged from on our Operational Technology which has led us to invest in protection of these systems. It therefore forms a key priority for stakeholders within RIIO T2.

Consumers’ use of electricity has changed within RIIO T1 and is expected to change further in the future. With the advancement in technology, society is becoming more dependent on technology that is dependent on power. Other sectors, such as transport, are becoming more interdependent, with an increased use of communication and broadband networks that are power-dependent technologies. These changes result in society becoming ever more reliant on electricity in their day-to day lives. As a result, the impact of an incident on the transmission network, caused by any threat we face, will not only impact National Grid, but overall GB society.

The impact of such an event is anticipated to increase, with a world becoming more dependent on power, and a reduction in stored capacity. It is essential that our plans are created on the back of stakeholder views on this topic, so that we are addressing the key societal areas of concern, and our plans are in the best interests of consumers.

‘I want you to protect the network from external threats’ was created as a key stakeholder priority in response to the stakeholder engagement sessions held in 2017. Stakeholders told us that their top priorities are that we ‘provide a reliable network, so that electricity is there whenever it’s needed’ as well as ‘protect the network against external threats’. Stakeholders and members of the public were aligned in the view that there will be a greater need for a transmission network in the next 10 years than today, regardless of which scenario arises, due to the diverse sources of energy connecting to the system as well as the increase in reliance on technology[1]. When we asked our stakeholders, what mattered most about our future performance, a consistent theme was the management of threats against our system. To address the feedback, we have kept our reliability plans and ‘resilience’ (managing external threats) plans separate within our T2 submission. This stakeholder priority considers potential loss of supply events that are caused by external extreme events (High Impact, Low Probability), and our reliability topic considers potential loss of supply events due to National Grid operations such as through asset performance. The topics which we planned to engage upon with stakeholders are shown in *Figure 1* below.

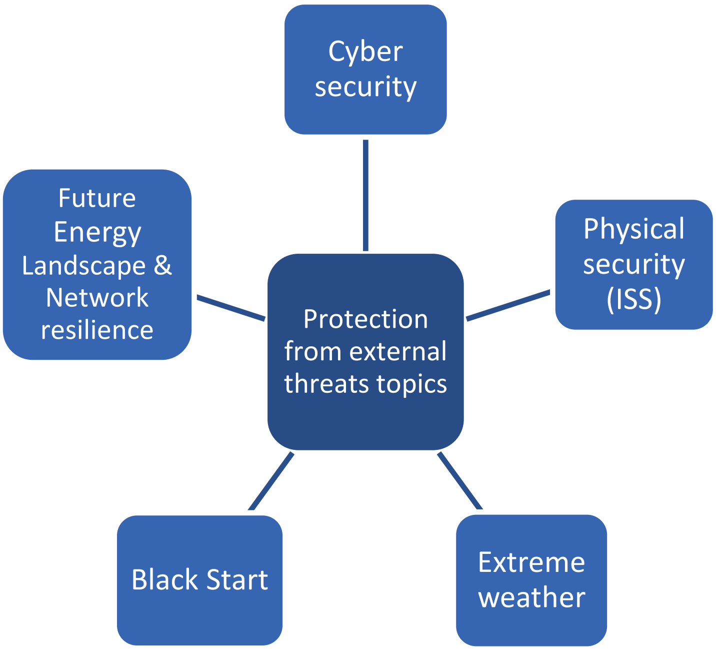

Cyber security
Future Energy Landscape & Network resilience
Physical security (ISS)
Protection from external threats topics
Black Start
Extreme weather

Figure 1: Topics for engagement under this stakeholder priority

Since it’s initial development, the scope of our chapter on ‘I want you to protect the network from external threats’ has been expanded to include OpTel (Operational Telecommunications) capabilities. This has been transferred from our IT investments due to the strong alignment with Operational Technology and providing a network resilient to external threats. Maintaining a resilient OpTel network is essential to running a reliable network and providing physical security and Black Start capabilities. As with our other investments on this topic, there is limited scope for stakeholders

[1] *National Grid Electricity Transmission Owner (2017) ‘Stakeholder workshops and online consultation: consolidated feedback’ [pdf] Available at: <http://yourenergyfuture.nationalgrid.com/media/1447/et-listen-report.pdf>*

to influence our plans due to the highly technical and specialist nature of our plans. We will engage with key stakeholders to ensure we have the capability of communicating with connected networks and having common standards.

1.2 WHAT EXISTING INSIGHT HAS BEEN UTILISED?

This topic was introduced because of testing the initial priorities with our stakeholders during our 'listen' phase of RIIO T2 engagement (throughout the 2017 workshops as mentioned previously as well as a consultation). Through understanding stakeholder views on external threats, it was clear that cyber security should be a key focus area for RIIO T2. A large proportion of our 'I want you to protect the network from external threats' investments will be made up of actions to protect from cyber-attack. Details of what we heard during our initial engagement can be found in our Listen report and in the write-up of our 2017 workshops and online consultation.

Prior to engaging specifically on our RIIO T2 plans, we have also engaged with our stakeholders through existing forums to both develop and understand an industry wide view on resilience, threats and appropriate approaches to mitigation. This engagement included groups such as Energy Emergencies Executive Committee (E3C), Energy Research Partnership and the Black Start Task Group.

Insight gained has reassured us that this topic is an area which our stakeholders view as highly important and should therefore a key focus over the next few years.

STAKEHOLDER SURVEY RESULTS

As well as ongoing engagement on our threat topics, we conducted a survey with our stakeholders in August 2018, to enquire about what topics they would like to see and discuss around 'protection from threats'. The results from this survey are included below in *Figure 2*, which show that the majority of our stakeholders top focus areas are the Future Energy Landscape and how to manage resilience levels in the future, as well as Cyber Security. The survey results helped to inform the agenda for a workshop which we subsequently ran in October 2018 with our stakeholders. The full responses are provided in Appendix 6.5.

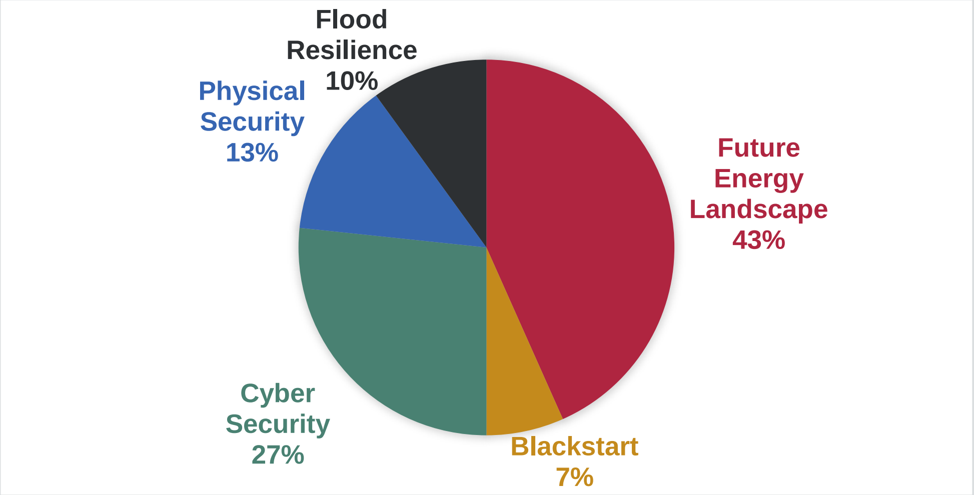


Figure 2: Survey Results on Our Stakeholders' Resilience Focus Areas (mid-September 2018)

Our pre-engagement insight and background to each of our key threat areas are as follows;

CYBER SECURITY

Feedback received from stakeholders within our initial RIIO T2 consultation included *'Cyber security for the transmission system is a national security issue'* and *'Cyber security should be considered alongside physical security'*. Having gathered this feedback from stakeholders it was clear that cyber-attacks should be one of the key threats that we will be protecting the network against.

In relation to protection from cyber-attack specifically, the UK Government has recently recognised and responded to the change in threat. This has been demonstrated by the creation of the National Cyber Security Centre (NCSC) in 2017 and more recently the adoption of EU legislation on enhancing security of assets required for the delivery of essential services through the Network and Information Systems (NIS) Directive in 2018. The NIS Regulations sets out clear security guidance for National Grid which we need to comply with, setting a baseline level of future investment. We engage closely with the Competent Authority of the NIS Regulations (a joint role held by BEIS and Ofgem) to understand and respond to the new requirements detailed in these new regulations.

The cyber and digital footprint of our company is vastly growing. We expect the external threat trend to grow considerably throughout RIIO T2 in volume, type, sophistication and complexity; in parallel to the organisation becoming more interconnected to respond to market changes and drive efficiencies. As an example, NCSC has told us that we need to take further measures to protect our key systems from attack – breaches from which could potentially impact multiple systems throughout the estate. Ensuring the appropriate cyber security protections are in place to protect both Information Technology (IT) and Operational Technology (OT) critical infrastructure will be vital to ensuring the reliable and safe delivery of energy to consumers.

For National Grid's cyber resilience, our systems over time are becoming increasingly interconnected, and as such the threat to both the IT and OT critical infrastructure increases. As the network has evolved, so have the systems that support our operation. Historically, our systems were largely internally facing – accessed locally by dedicated employees. Over time this has evolved to many systems being externally accessible, for example, creating the need for increased levels of protection. An increasingly significant amount of industry stakeholders, such as DNOs, electricity interconnectors and OFTOs rely on our systems so it is critical that we need to ensure continued reliability to underpin the end to end supply chain. In conjuncation with BEIS and the ENA, we supported development of the Cyber Security Procurement Guidance[2] to help overcome industry-wide cyber procurement challenges and take further steps to ensure the integrity of the energy system as a whole.

[2] Cyber Security Procurement Guidance available at: http://www.energynetworks.org/assets/files/BEIS%20ENA%20Cyber%20Security%20Procurement%20Language%20Guidance.pdf

EXTREME WEATHER

Regular engagement continues to takes place primarily through a stakeholder group (ETR138 Task Group) set up by the Energy Networks Association in 2007. This group includes National Grid, TOs, DNOs, Environment Agencies, Ofgem and BEIS (previously DECC) and aims to review the appropriateness of flood protection guidance whilst considering latest threat information.

The output of this group was an Engineering Technical Report (ETR138) initially published in 2009 which outlined flood resilience requirements. The findings of this report were all agreed to by the members of the group and helped inform our RIIO T1 Business Plans.

Within RIIO T1, the group have met several times and published updates to this report, with the latest being published in 2018. The main changes within the report, from our RIIO T1 Business Plans, are the new requirements for surface level flooding and the agreement that sites should be protected with a potential impact of over 10,000 customer points from surface level flooding. As a result, this has changed resilience requirements on sites and increased the number of sites we need to protect against flooding. All the members of the group were in agreement of these changes in 2018. These changes were later endorsed by BEIS and Ofgem with a requirement on network companies to implement these requirements (on National Grid by the end of RIIO-T2).

BLACK START

Blackstart is the worst case contingency for the UK electricity supply industry. The probability of occurrence is very low, but consequences are severe. The severity of such as event is recognised by Government and referenced in the National Risk Register, as plausibly happening within the next five years, where the consequences of the event would cause a civil emergency[3]. The National Risk Register references that Black Start recovery could take up to five days, with some potential for some additional disruption beyond this timescale.

We have summaried the insight gained from BAU engagement on this topic within the table below;

Industry Report/Working Group	Insight Gained
National Risk Register	Blackstart arrangements are a top hazard identified by UK government with the potential to cause a civil emergency. National Grid should continue to develop blackstart contingency plans
ENA Groups – Emergency Managers Planning Forum	Blackstart is a key focus area for electricity networks, and National Grid should continue to collaborate with DNOs and other industry parties to reach an efficient and cost-effective blackstart restoration plans
BEIS Task Groups: E3C, ETG, and Blackstart Task Group	The task group considers the adequacy of the GB industry's blackstart plans, and has indicated that the industry currently can achieve

[3] *Cabinet Office (2017) 'National Risk Register of Civil Emergencies' 2017 Ed [pdf] Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf>*

	restoration within 7 days. National Grid should continue to work with BEIS and industry to provide adequate blackstart restoration plans [redacted]
Ofgem and DECC reports following 2013 floods[4] [5]	Ofgem and BEIS (formerly DECC) advocate the requirement for networks to collaborate further, to meet appropriate resilience levels. National Grid will continue to work with DNOs, generators and local resilience forums to develop efficient and effective blackstart arrangements.
Local resilience forums	Energy resilience is a key focus for local authorities. National Grid should continue to develop blackstart arrangements, co-ordinated with other sectors such as emergency services

Table 1: Insight gained from stakeholders

We must also recognise that Black Start is a resulting situation and not a 'threat'. By addressing other threat areas, we will help to reduce the likelihood of a Black Start event, however we must also prepare for such an event to occur. Our Black Start engagement focuses on strengthening our resilience to manage, respond and recover as efficiently as possible from a Black Start incident.

PHYSICAL SECURITY (ISS)

Enhancement of the physical security of our sites is essential to ensure effective protection of our assets from physical attack. The physical security of our sites is primarily mandated by the Physical Security Upgrade Programme, an initiative to protect the UK's most essential infrastructure. All works are closely evaluated by Government assigned bodies, including the joint development of a prescriptive Site Specific Operational Requirements document between the Centre for the Protection of National Infrastructure (CPNI) and National Grid to which each site must be designed (in terms of physical security resilience).

The key stakeholders on this programme are the Department of Business, Energy and Industrial Strategy (BEIS) and CPNI. We meet with them to review the impact of the current UK threat level on the electricity transmission network and to discuss site classification and whether current measures are adequate. These insights influence the Physical Security plan which we use to plan which site security enhancements need to be delivered by certain dates to ensure the required level of security resiliency is provided.

OPTEL

Having and maintaining a resilient OpTel network is not a new requirement and therefore we have used our knowledge and experience from RIIO T1. We have experienced increasing trends of failure fibre wrap which is approaching end of life.

[4] *Ofgem (2014) 'December 2013 storms review – impact on electricity distribution customers' [pdf] Available at: < https://www.ofgem.gov.uk/ofgem-publications/86460/finaldecember2013stormsreview.pdf>*

[5] *DECC (2014) 'Severe Weather – Christmas 2013'[pdf] Available at: < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/287012/DECC_-_Festive_disruption_review_-_Final__2_.pdf>*

FUTURE ENERGY LANDSCAPE

The transmission system was constructed in a very different era, when reliance on electricity was not as significant as it is today. When the system was first designed, people were only becoming reliant on electricity as a source of light, heat and cooking. People could also tolerate power losses more readily, as people had living memory of being without electricity and still had a mixture of supplies such as coal fires, as a heat substitution for electricity in the event of a failure. However, from the inception of the Transmission system, an onus on reliability and resilience was recognised. As reliability of networks has improved, people have become very reliant on electricity to conduct their daily lives and this trend is set to continue. Our world is now dominated by dependency on the electricity network, from power to our homes, places of work, communication systems (especially with a heavy reliance on broadband internet), modes of transport, shopping and leisure. The UK Government published its “Clean Growth Strategy: Leading the way to a low carbon future” on the 12th October 2017. This document sets out how the de-carbonisation of transport and heating systems will lead the way, with many solutions utilising electricity such as Electric Vehicles (Cars and Buses), Electrification of Railways, and Heat Pumps[6].

At the same time reliance on electricity is becoming greater, affecting every part of our lives. As a result, the potential impact of an interruption in power supply is increasing as well. We are at greater risk than ever from external influences affecting the power system from extreme weather events due to climate change, to physical or cyber related attacks, which could cause wide scale disruption to networks. In addition to external threats, the way the system operates has changed, such as with the increase in embedded, distributed generation and falling system inertia. This makes the ability to respond and recover from system events more difficult in the future. In a world where we are heavily reliant on electricity, from heating our homes, buying a loaf of bread, or driving to work; the loss of power would quickly become intolerable to the population, especially for periods lasting longer than a day. Therefore, the consequences of high impact, low probability events, such as a local or widespread failure of the transmission system has changed significantly since the construction of the transmission system. As society becomes ever more reliant on electricity, the need to be resilient to such events shall become more critical, to ensure that we are prepared to respond and recover, as soon as possible.

National Grid as a Transmission Owner contributes towards the resilience of the entire electricity network. The network is vastly interconnected and is becoming increasingly so with further system integration. An incident on our network could impact our customers, distribution networks, the system operator, other Transmission Owners as well as consumers and other sectors such as transport and communications; all through us not being able to provide the service of electricity transmission. A widespread loss of supply could be detrimental to the economy, consumer welfare, the functioning of Government and society as a whole.

[6] *HM Government (2017) ‘The Clean Growth Strategy: Leading the way to a low carbon future’ [pdf] Available at: < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/700496/clean-growth-strategy-correction-april-2018.pdf>*

We have been participating in a cross-industry project, led by the Energy Research Partnership, which is focussed on the challenges posed to the resilience of the UK electricity system in the next 10 years. The project was initiated in May 2018, and due to conclude in November 2018, with the launch of an industry report reflecting the thoughts and recommendations made by the working group. A workshop was held in June 2018, which reviewed and discussed some common themes that were being discussed, and the outputs of which are feeding into the industry report. The growing reliance on electricity was a common outcome of the discussions, alongside growing threats to network infrastructure, and further complex interdependencies between different sectors such as transport and heat may become more interdependent on electricity.

The water industry has had a focus on resilience as a key regulatory output since PR14 (Price review 2014), with it being one of the four key themes that Ofwat review water utilities during their price review. Ofwat published ‘Resilience in the Round’ in September 2017, describing the benefits of a resilient water system, and by which they measure resilience. The report promotes a system-of-systems approach, with the interdependencies between sectors, and condones collaboration between sectors to deliver better outcomes for resilience and sustainability. Energy is identified as an interdependency, where electricity is key for transportation of water (water pumps) and the sanitation process[7]. The water industry can only be resilient if the sectors they are dependent on also adhere to similar levels of resilience.

The National Infrastructure Commission (NIC) published the National Infrastructure Assessment in July 2018. The findings from the report highlight a growing reliance on digital communications, change in generation mix including hydrogen as a possible replacement for natural gas, further electrification in the transport sector, an increase in likelihood of extreme weather affecting infrastructure, and further cross-sector interdependencies.

The resilience of cities is being measured, in line with the City Resilience Index as part of the 100 Resilient Cities programme, pioneered by the Rockefeller Foundation. The programme is dedicated to helping cities around the world become more resilient to the physical, social and economic challenges that are a growing part of the 21st century. ‘100 Resilient Cities’ supports the adoption and incorporation of a view of resilience that includes shocks and stresses. Bristol is one of the 100 Resilient Cities, that has assessed its resilience as a city for 2050. Energy supply was identified as a focus area for Bristol, as a basic need, and the Bristol City Council have since developed an energy framework to ensure a continual energy supply is provided in an uncertain future[8] .

[7] Ofwat (2017) ‘Resilience in the round: Building resilience for the future’ [pdf] Available at: < https://www.ofwat.gov.uk/wp-content/uploads/2017/09/Resilience-in-the-Round-report.pdf>

8 100 Resilient Cities (2017) Bristol Resilience Strategy [pdf] Available at: <http://www.100resilientcities.org/wp-content/uploads/2017/07/Bristol_Strategy_PDF.compressed.pdf>

1.3 WHAT ARE THE DESIRED OUTCOMES FOR THIS ENGAGEMENT?

Due to the formal requirements in place to protect the network from threats, we engaged with Government and relevant specialist agencies to ensure our plans meet those requirements and are proportionate to the risk that we face. For each threat area, these stakeholders include;

Extreme Weather – BEIS and Environment Agency
Physical Security – BEIS and CPNI
Cyber Security – Ofgem and BEIS (as NIS Competent Authority) and the National Cyber Security Centre (NCSC)
Black Start - BEIS

Our RIIO T2 investment proposals are based on insight gained from stakeholders. This may range from general feedback to specific requirements provided by Government and specialist organisations.

The purpose of our engagement on this topic will be to;

a) Ensure we fully understand stakeholder views on how important this priority is to them (including willingness to pay).
b) Determine appropriate investments for T2 by understanding threats and agreeing requirements with relevant authorities or specialists.

Overall, our desired outcomes from the engagement are to:

- Understand whether stakeholders agree that our current key topic areas (Cyber, Flood, Physical, Black Start) are the right topics to focus on
- Understand stakeholders' high level views on the importance of maintaining a resilient network in the future, and whether this may change over time
- Understand the impact on stakeholders' businesses/lives if our network was not resilient (including some education on what a non-resilient network could mean)
- Explore the key topic areas in more detail with stakeholders, including sharing the details of our plans (where possible) and costed options where appropriate, to allow them to make informed decisions on how/if we should invest in each area of resilience in the future
- To understand whether resilience (particularly black start) carries a different importance with stakeholders according to geography (i.e. urban vs rural)
- Gather ideas on how we could measure resilience (which will then be further explored with Ofgem and BEIS)
- Engagement with CPNI and BEIS to inform our Physical Security Upgrade Programme risk position and action required to protect sites.
- Engagement with NIS Competent Authority and E3CC to inform our cyber risk position and agree works required to mitigate threats.
- Engagement with BEIS and industry parties through the Black Start Task Group to contribute to the discussion and proposal of a Black Start Standard

- Engagement with BEIS and industry parties through the ETR138 working group to understand T2 guidance on protection from surface water flooding and BEIS'

Unfortunately on the topics of cyber-security and physical security, there is a limited amount of information that we will be able to share widely with stakeholders on our plans. This is due to the confidentiality and sensitivity around where and how we aim to protect our network. We will however be informing our stakeholders on the process in which we will follow to develop our plans with the relevant authorities or specialists. Our requirements across this topic are also quite prescriptive, which also gives stakeholders limited ability to influence our plans, however if we do hear any overarching feedback on an area which is not currently being addresses, we will be able to factor this into our business plans.

Specifically for cyber security, in Q1 2019 we completed an updated assessment of our cyber security and capabilities against the NIS Regulations. We are working with the Competent Authority (Ofgem & BEIS) under the framework to agree an appropriate strategy and investment plan in this area, at both a shorter term tactical level (for RIIO-T1); as well as medium to longer term plans to be effective from April 2021 onwards which form our T2 plans.

For our OpTel investments, successful engagement would result in agreed approach with National Grid ESO, which is consistent wih Scottish TO's where it needs to be. We would also like to seek technical advice to future proof the technology and have a credible forecast of capacity growth.

1.4 WHAT IS THE ENGAGEMENT APPROACH?

We use the principles of the AA1000 stakeholder engagement standard to determine the most appropriate approach to engagement, so that engagement is tailored by topic and by stakeholders. These principles align with the principles of good engagement set out by our Independent Stakeholder Group (see Appendix 6.1).

Stakeholder mapping across segments was undertaken to establish an approach as illustrated in Figure 3 (see Appendix 6.3 for the full list)

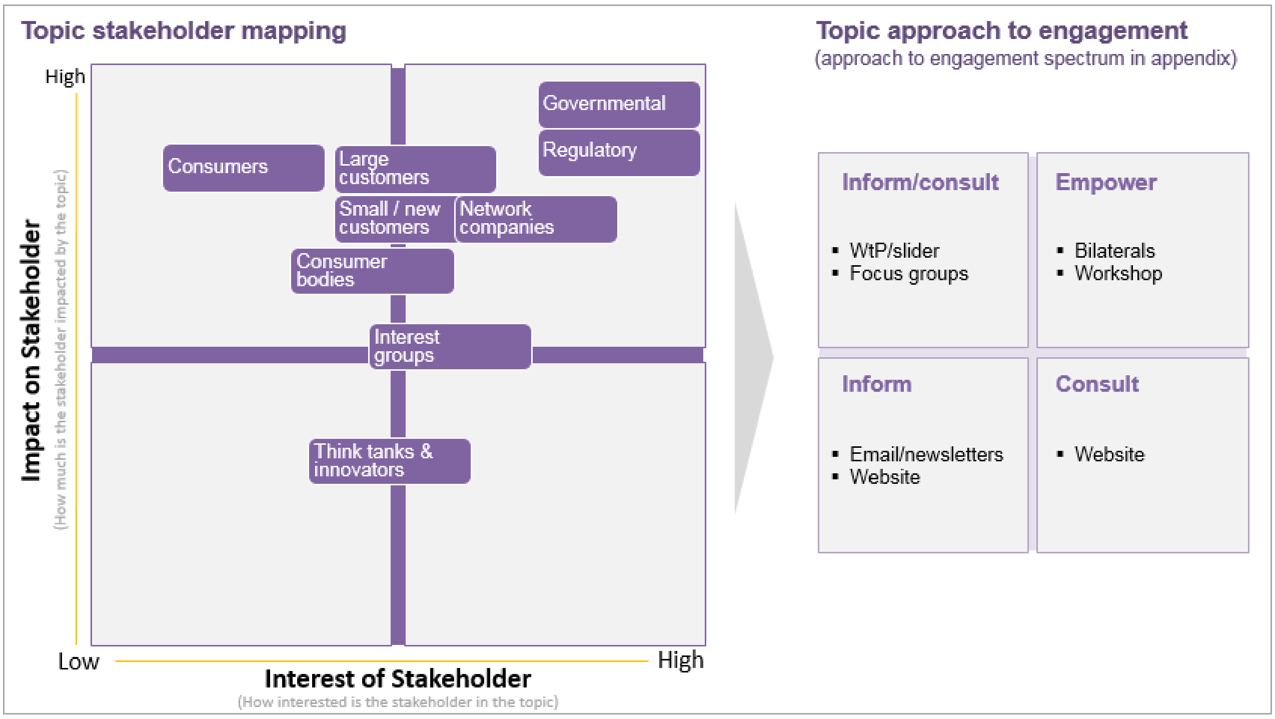


Figure 3: Stakeholder mapping and engagement approach

Added to this, we use ongoing feedback from stakeholders to shape our engagement. For example, we used feedback from our 2017 Listen workshops to improve the way we engaged in 2018 and tailor our engagement so that it worked for our stakeholders.

The primary purpose of engagement on this topic is to consult our stakeholders on what we need to include in our plans for RIIO-2, by sharing options (including our current/default approach where appropriate), understanding their priorities and preferences, and including any new insight in how we build our plans. In order to do this, we may also need to inform stakeholders – different stakeholders have differing levels of knowledge about what we do, particularly when looking at sub-topics. Informing stakeholders sufficiently at the beginning of our engagement is, therefore, important to allow them to contribute in a meaningful way and provide an informed opinion. For this topic, this may be less relevant than for others, as those stakeholders that we can share detailed information with are generally well-informed or are specialists in the topic area.

For us to meet the desired outcomes for this stakeholder priority, and in addition to our ongoing conversations via working groups and other existing channels with stakeholders such as Ofgem, BEIS and other specialists, we chose to run a workshop as the most effective method for discussing and debating the sub-topics with interested and impacted stakeholders. This decision was also informed by a short survey which we issued to our stakeholders in August-September 2018. This asked stakeholders which channels they found most effective, and which sub-topics they would like to discuss with us under this stakeholder priority. Workshops and face-to-face engagement sessions were the clear favourite. The responses to this survey can be found in Appendix 6.5.

Our approach to engagement was to start development of RIIO T2 plans by engaging with a wide group of stakeholders via a workshop in October 2018. The purpose of the workshop was inform and consult stakeholders on our initial thoughts on the topic developed through initial engagement. We would test whether stakeholders agreed with our approach of developing business plans with relevant authorities and specialists. We also wanted to understand whether stakeholders felt we had covered all relevant threats for mitigation and areas of enhanced resilience within RIIO T2.

In developing the content for the workshop, we used the previous survey as a source of insight. We had already identified relevant stakeholders by looking at how they were impacted, or what interest they have in different areas of this stakeholder priority. These stakeholders included;

- Current industry resilience working groups such as E3C
- Government bodies to reflect national societal interests
- Networks dependent on National Grid such as DNOs, water companies
- Energy Networks Association (ENA)
- Customers which have raised resilience/threats as a concern
- Representatives of national business interests such as the Confederation of British Industry
- Representatives of consumers such as Citizens Advice Bureau and Ofgem
- Academics which have a record of researching power system resilience, including the Institution of Engineering and Technology
- European bodies and associations, aligned to cyber policy developments

We would test the success of our engagement on the level of attendance and feedback received during and following the session. We also planned to use the workshop as an opportunity to gather stakeholder views on levels of protection / resilience to be applied to our network and systems. Another measure of success for our engagement was whether we were able to gather such information effectively which could be used to inform our business plans. In order to gather this information, we may need to use example scenarios to determine stakeholder views.

Due to the confidentiality and sensitivity of our threat information, we are unfortunately not able to engage widely on this topic. We have however identified key stakeholders who we can engage with on each planned area of investment. This will help us understand expectations of us to maintain a resilient network and also what our key stakeholders want us to invest in.

There may be also opportunity to work with specific stakeholders such as the DNO’s and the Scottish TO’s to understand where our plans complement each other’s system protection or if there are any joint projects which could be completed. However, again we will be restricted on the level of information which can be shared.

Channels used/planned, including our initial Listen phase workshops, are listed below:

Channel	Who	When
Initial workshops	NGET stakeholder list invite	July 2017
Online consultation	NGET stakeholder list invite	July-August 2017
Consumer research	Representative sample of 2,081 household consumers	October 2017
Topic-specific workshop	Targeted stakeholders from NGET stakeholder list	October 2018
Bilaterals	Ofgem, BEIS, CPNI and TO's	Bi-monthly

Table 2: Engagement channels used

We also aimed to share our approach and workshop content with Frontier Economics, and incorporate any necessary changes before we engage. Output from this review is can be found in Appendix 6.8.

Specifically for cyber, the threat landscape that we are facing is constantly evolving and as such we engage with key external stakeholders to both understand emerging threats, in addition to sharing any lessons learnt. As an example, we engage with NCSC on a quarterly basis to understand and share views on emerging threats; receive regular threat briefings from BEIS; and ensure that through effective communication, we routinely share key information internally with our threat mitigation teams to put the necessary monitoring in place or take the appropriate action.

As such, in addition to the figure above, our cyber specific engagement channels also include:

Channel	Who	When
Workshops and surgeries	NIS Competent Authority	2018 onwards (bi-monthly on average)
Briefings	BEIS	Monthly
Bilaterals	National Cyber Security Centre (NCSC)	Quarterly

Table 3: Engagement channels used for cyber engagement

2: POST-ENGAGEMENT

2.1 WHAT WERE THE ENGAGEMENT OUTCOMES AND HOW HAS THIS INFLUENCED OPTIONS?

The key methods in which we have engaged with stakeholders are outlined below;

RESILIENCE WORKSHOP

On 23 October 2018, we held a workshop in London on the topic of resilience (how our network should be protected from threats). We sent out invites to approximately 240 stakeholders, based on a list we had compiled of key stakeholders identified or those expressing an interest in being involved in the creation of our RIIO T2 business plans. The aim of the workshop was to consult stakeholders on the topic of resilience and to give them the opportunity to contribute their views on our current plans. Our decision to run a workshop was based on previous learning that face-to-face workshops are the preferred means of engagement for many of our stakeholders, and that they allow debate to take place amongst attendees.

As mentioned earlier within this engagement log, this is a topic in which we are restricted on both the flexibility of changing our plans (due to formal requirements for works) and the amount of information we can share with stakeholders (due to the sensitive nature of the content). We also understand that those stakeholders attending the workshop may have different levels of understanding on this topic. For this reason, we made sure to provide context when opening the workshop so that our stakeholders had an understanding of what threats we faced and the potential impact of incidents on the electricity transmission network. They also understood that whilst we wanted to hear their views on this topic and our proposed high-level plans, there were certain elements of our plans that we would not be able to change, no matter what we heard.

39 stakeholders representing 26 organisations attended the workshop, covering 9 of our key stakeholder segments / sub-segments. The topics we presented and welcomed feedback on within the workshop included the impacts of the future changing energy landscape on levels of resilience required, physical security, cyber security, extreme weather events (including the potential impact of climate change) and 'black start' (where the whole or significant parts of the GB electricity network suffer a complete loss of power).

We needed to ensure that attendees were able to provide input in an informed way, so we began the workshops with a high-level overview of what we do, our approach to engagement and how we currently protect the network from threats. We then structured the day around topic-specific sessions, using a similar format to previous workshops on our other RIIO T2 topics, which had received positive feedback from attendees. These involved;

- A short presentation to provide enough context for stakeholders to be able to discuss the subject area
- A facilitated table discussion, during which all stakeholder comments were captured to provide qualitative feedback
- Where relevant, a short voting exercise, allowing us to capture qualitative feedback where there are options regarding our strategy, approach and/or what we include in our plans.

As with previous workshops, we deliberately chose not to use a third-party facilitator, but made sure that all National Grid employees were fully briefed so as not to introduce any potential bias to the conversations. This again was well-received by attendees, with a Net Promoter score of +40 and an average score of 8.4 out of 10 when asked how likely they would be to recommend the workshop to a friend or colleague.

The feedback received at the workshop included comments such as;

- Really good and interesting breadth of issues.
- I found the workshop informative (while a little bit generic for people deeply involved in this topic), but I mostly enjoyed the fact that NG is willing to engage with other stakeholders. This will be crucial as we move into the future.
- Thought provoking and very useful to all those who attended.
- Good level of discussion, would be good to understand the detail of the plans. i.e. what enhanced level of resilience would be provided by £xm investment.
- Excellent if someone has an interest in general resilience issues; very comprehensive.

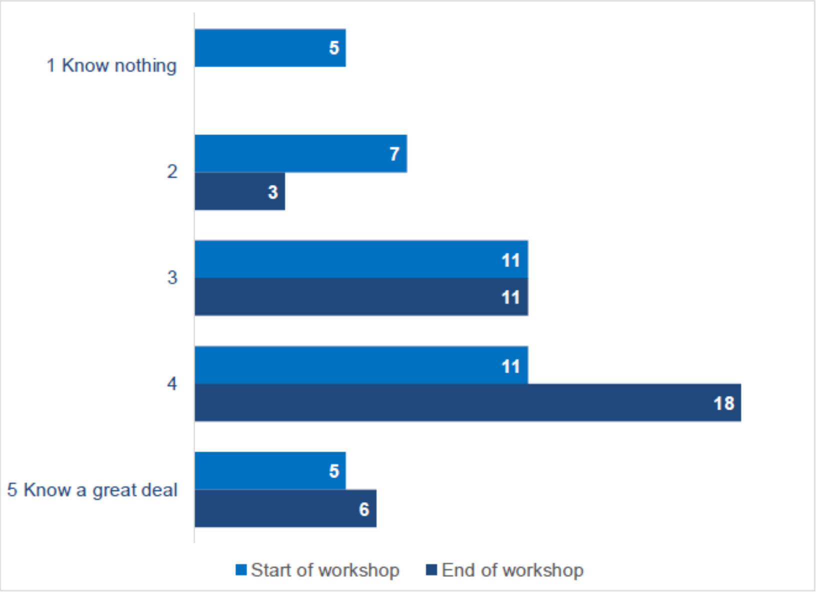
The key headlines from the workshop were:

- The need for a resilient electricity network will increase in the future
- Cyber-attacks are seen by many stakeholders' as the biggest short-term threat and climate change could have the greatest longer-term impact
- Our approach to physical security is supported
- For cyber resilience and black start recovery, we need to be joined up with the right organisations to ensure a coordinated approach
- Our approach to extreme weather resilience needs to be flexible, forward looking, and adapt to likely future changes.

Within the workshop, we used forms in which attendees could answer specific questions we posed throughout the workshop, and through which we could capture feedback to help us understand how useful they found the workshop and what their views were on resilience levels required in electricity transmission.

Shortly after opening the workshop, we asked attendees to answer the question; *On a scale of 1-5, where 1 is know nothing and 5 is know a great deal, how much would you say you know about electricity transmission resilience?* We re-tested this at the end of the workshop and saw a difference in the mean score of +0.6 from the start of the workshop. Figure 4 below shows the difference in responses which were received during the workshop.

The results indicate that our engagement approach was successful in informing stakeholders of the topic and the approaches we are taking to address external threats.



Start of workshop mean score = 3.1 (39 respondents)
End of workshop mean score = 3.7 (38 respondents)

Figure 4: Workshop attendee awareness of electricity transmission resilience

The answers to one of these questions concluded that all attendees felt that there would be a greater need for a resilient network in the future, ranging from a slightly greater need to a significantly greater need. The range of responses are outlined in figure 5 below.

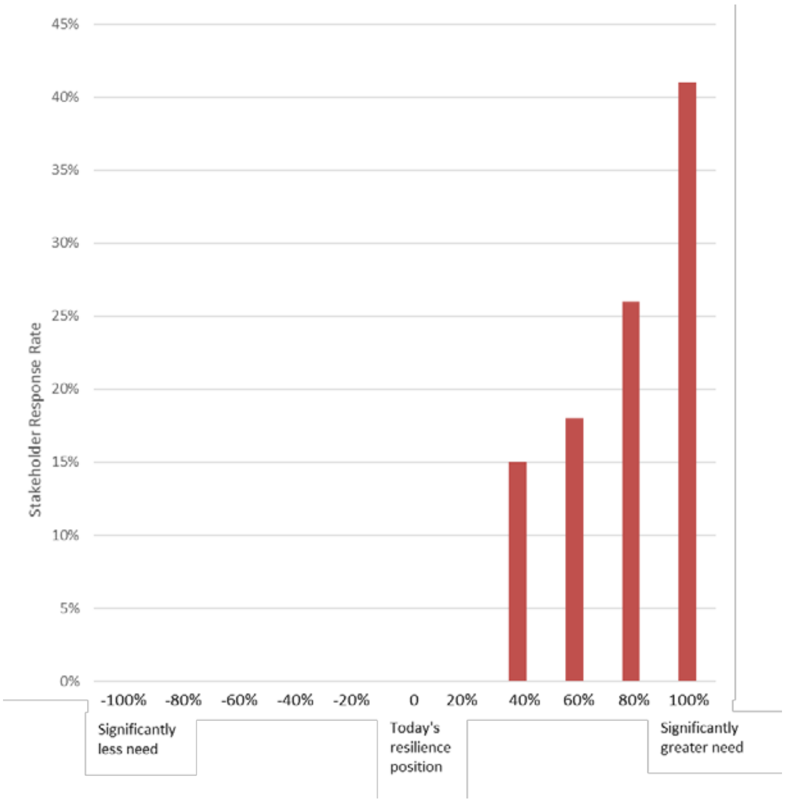


Figure 5: Workshop attendees' view of the need for a resilient transmission system in the future

We are currently working through the more detailed feedback and specific comments received from stakeholders to consider whether there is anything that we can address within our RIIO T2 business plans. If there is any feedback which we can act on we will investigate how we can incorporate these into our RIIO T2 plans.

Following an initial review of the feedback, some key comments stood out as suggestions on how we should approach ensuring a resilient system, these were;

- We should prioritise investment based on likelihood and impact, and should take a balanced approach across all threats.
- We need to adapt to change and use intelligence available to predict future changes (for example the impact of solar weather and wildfires).
- We need to coordinate activities with distribution networks and the system operator as a whole system approach is required.

Following the workshop, we published the slides from the meeting and a report summarising the content and feedback received on the day on the 'Your Energy Future' website.

The slides can be found here: http://yourenergyfuture.nationalgrid.com/media/1630/20181023-nget-resilience-stakeholder-workshop-slides.pdf

The report can be found here: http://yourenergyfuture.nationalgrid.com/media/1629/20181023-national-grid-et-resilience-workshop-report.pdf

ENERGY RESEARCH PARTNERSHIP RESILIENCE REPORT

As mentioned earlier, we are also a member of the Energy Research Partnership (ERP). The ERP is a forum consisting of both public and private sector organisations, Government and academia.

In November 2018, the ERP published a report titled 'Future resilience of the UK electricity system'. This was an ERP led project which aimed to identify and assess energy landscape changes that are likely to impact the future resilience of the electricity system and deduce key focus areas for recommendations and proposed outcomes. The project sought to gather insights from stakeholders and use these to help inform a common view of resilience of the electricity system. The report was derived following an extensive programme of workshops, working groups and reviews to provide a balanced view of future energy needs.

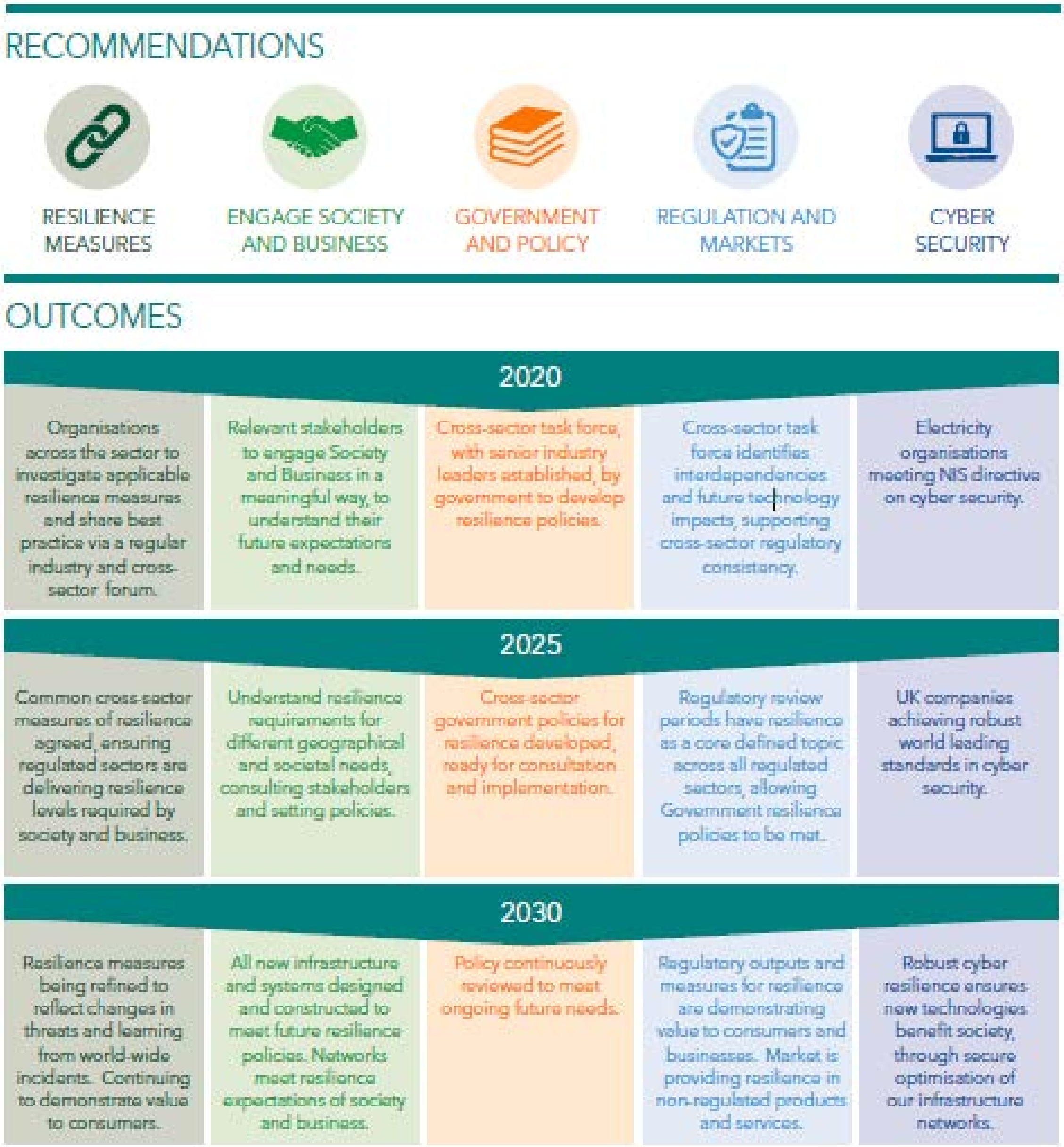
The report was also created in conjunction with non-ERP members invited to bring specialist knowledge to the project.
The ERP report has identified four key factors that are expected to affect the resilience of the electricity system in the future, these are;

- An increasing reliance upon technology and networks
- Increasing complex interdependencies between networks
- Growing threats to network infrastructure
- The growing economic importance of metropolitan centres

The report concluded that electricity use has changed significantly since the majority of the current electricity infrastructure was put in place. They expect this trend to continue with further electrification of sectors such as transport and heat, leading to a greater reliance upon electricity in the future. It is also highlighted that given a power disruption today, the impact on society and business will be higher for a similar event in the future.

Assessing the factors affecting the resilience of the electricity system the ERP report makes recommendations to maintain and improve resilience with target outcomes to be achieved by specific years in the future. Figure 6 below provides a high level view of these recommendations and outcomes. More detail to the recommendations and outcomes can be found within the report.

The ERP report can be found here: http://erpuk.org/wp-content/uploads/2018/11/4285_resilience_report_final.pdf



RECOMMENDATIONS

OUTCOMES

	RESILIENCE MEASURES	ENGAGE SOCIETY AND BUSINESS	GOVERNMENT AND POLICY	REGULATION AND MARKETS	CYBER SECURITY
2020	Organisations across the sector to investigate applicable resilience measures and share best practice via a regular industry and cross-sector forum.	Relevant stakeholders to engage Society and Business in a meaningful way, to understand their future expectations and needs.	Cross-sector task force, with senior industry leaders established, by government to develop resilience policies.	Cross-sector task force identifies interdependencies and future technology impacts, supporting cross-sector regulatory consistency.	Electricity organisations meeting NIS directive on cyber security.
2025	Common cross-sector measures of resilience agreed, ensuring regulated sectors are delivering resilience levels required by society and business.	Understand resilience requirements for different geographical and societal needs, consulting stakeholders and setting policies.	Cross-sector government policies for resilience developed, ready for consultation and implementation.	Regulatory review periods have resilience as a core defined topic across all regulated sectors, allowing Government resilience policies to be met..	UK companies achieving robust world leading standards in cyber security.
2030	Resilience measures being refined to reflect changes in threats and learning from world-wide incidents. Continuing to demonstrate value to consumers.	All new infrastructure and systems designed and constructed to meet future resilience policies. Networks meet resilience expectations of society and business.	Policy continuously reviewed to meet ongoing future needs.	Regulatory outputs and measures for resilience are demonstrating value to consumers and businesses. Market is providing resilience in non-regulated products and services.	Robust cyber resilience ensures new technologies benefit society, through secure optimisation of our infrastructure networks.

Figure 6: Energy Research Partnership recommendations and outcomes overview

PLAYBACK OF STAKEHOLDER VIEWS – FEBRUARY 2019

In February 2019, we published a T2 wide playback document entitled ‘Shaping the electricity transmission system of the future’[9] in which we gave an overview of what we have heard from our stakeholders when thinking about T2 business plans. We invited views from our stakeholders on all eight stakeholder priorities including ‘I want you to protect the network from external threats’

We asked a mixture of general questions such as;

- Have we understood your feedback and priorities correctly?
- Have we reflected your feedback correctly in our direction of travel?
- What else would you like to tell us? What have we missed? What should we change?

As well as topic specific questions like;

- What are your views on the direction of travel and investment drivers in relation to resilience?

In summary, the feedback we received highlighted the importance of maintaining a resilient network and told us that our stakeholders believe we are in a position to manage this. It was also suggested that consumers could better manage their own back up systems. Outlined below are the three responses received directly in response to the question on network resilience;

Respondant	Response
[redacted]	The risk assessment needs to be realistic. If more people were encouraged to have back up systems and take responsibility it would empower them in times of shutdowns, be it weather related, cyber or physical. We still need reassurance that the system is robust.
[redacted]	I agree with the necessity for protection against cyber attacks and quick recovery.
[redacted]	In my view, NG are following the correct direction of travel and this should be an area where levels of investment reflects the increasing risk level and we should not shy away from spending more if required. I believe this is a risk which is likely to increase over time in terms of impact and probability and so would be understandable and acceptable if investment levels were above the governments minimum requirement. They should be flexible (through uncertainty mechanisms, re-openers) to reflect future developments in the risk profile.

Table 4: Specific stakeholder responses to October survey on network resilience

For Cyber, as part of our recent work under the NIS Regulations, in conjunction with the Competent Authority we have developed both a self-assessment and short-term Improvement Plans..

The self-assessment report consists of an assessment against a Cyber Assurance Framework (CAF - developed by the National Cyber Security Centre) and includes a consistent business-wide risk-based approach. Using this methodology, we have identified specific risks to address. of the risks

[9] *Stakeholder playback document https://www.nationalgridet.com/document/129316/download*

identified range from 'very high' to 'low' which we are considering as how best to address; whilst monitoring the evolving threat landscape.

We will continue to work with the Competent Authority to help refine and develop our plans throughout 2019 and beyond, to ensure we continue to address current and future threats. This engagement will help inform and develop our T2 plans, which will be shared with the Competent Authority in advance of submitting to Ofgem in late 2019.

BEIS BLACK START TASK GROUP

[redacted] As part of the Black Start Task Group (BSTG) we are working with BEIS and other energy sector participants to develop a new Black Start standard, with improved restoration times.

BSTG sets out various scenarios, using societal/economic impact of an event to determine target restoration times. The eventual target is likely to be based upon a combination of societal/economic impact and technical feasibility. BEIS has asked industry players to indicate costs to achieve a 'high degree of confidence' of achieving scenario restoration times. We have provided outline costs to BEIS and included within our Draft Business Plan Submission and will continue to work with BEIS and the BSTG to contribute to the development of the new standard. We will update our October and December Business Plan submissions to enable us to provide a 'high level of confidence' in our ability to achieve the new Black Start standard.

OPTEL

We have engaged with a specialist consultancy to provide background on development in the telecommunications market, knowledge from other TO's and associated industries to help inform our technology selection and provide a credible view on future growth and capacity.

We have regular engagement with the Scottish TOs in 3 way sessions, to discuss engineering standards, methodology to achieve outcomes and potential new requirements to ensure we are operating on a common platform where we are exchanging data.

We have engaged with National Grid ESO on future requirements and services including Black Start. This will help to ensure we have the right capabilities for a future Black Start solution.

ENGAGEMENT WITH THE NIS COMPETENT AUTHORITY THROUGHOUT 2019

Under the NIS Regulations, network companies must take appropriate and proportionate technical and organisational cyber security measures to manage the risks posed to the security of the network and information systems on which their essential service depends, and to prevent and minimise the impact of incidents on these essential services.

We have been continuously engaging with the NIS Competent Authority to further understand the requirements of National Grid under the NIS Regulations and determine appropriate steps to be take to ensure alignment with the Regulations.

The NCSC has developed a sector-agnostic Cyber Assessment Framework (CAF) to assist operators covered by the NIS Regulations to perform self-assessments. We performed a self-assessment against the CAF in early 2019, which was later submitted to the NIS Competent Authority, followed by a short-to-medium term 'tactical' business plans to mitigate immediate risks highlighted by the self-assessment. This plan included investment up to the end of the RIIO T1 period and was aligned to further guidance issued by the Competent Authority. This guidance (the CAF basic profile) outlined the Competent Authority's sector specific expectations of network companies to achieve prior to April 2020.

The Competent Authority are yet to share an advanced profile which we expect to outline longer term expectations of network alignment to the CAF.

Our engagement ongoing engagement with the NIS Competent Authority is crucial to the development of our T2 business plans, which have been informed by the self-assessment completed using the CAF provided by the NCSC.

SCOTTISH TO ENGAGEMENT SESSIONS – CYBER

As the NIS Regulations cover a number of ‘Operators of Essential Services’, these regulations are also applicable to other industry participants such as the Scottish Transmission Owners.

In January 2019, ahead of completing and submitting our NIS self-assessment and RIIO-T1 tactical improvement plans, we met with the Scottish TO’s to compare thoughts on cyber risk to our systems, NIS process of developing and submitting business plans and differences between our systems which may result in our plans being different.

The purpose of this session was coordinate views on threats and approach to addressing cyber risk and all parties found this very beneficial to ensure an aligned approach to NIS Regulations from the GB Transmission Owners.

Following our first meeting, we submitted both our NIS self-assessments and RIIO-T1 tactical improvement plans to the NIS Competent Authority. Ofgem also published their Sector Specific Methodology Decision, in which they announced their approach to regulatory treatment using a ‘use it or lose it’ allowance mechanism for our Operational Technology cyber business plans and the use of re-openers to manage uncertainty within RIIO-T2.

This progress resulted in us arranging another engagement session in August 2019 to discuss both regulatory treatment within RIIO-T2 and progress made on development of RIIO-T2 business plans.

[redacted] Feedback received from these sessions were that they were beneficial for all involved and we plan to continue engagement following submission of our RIIO-T2 business plans and into the T2 period.

BEIS AND NCSC INTRODUCTION TO CYBER SESSIONS

In June 2019, we invited cyber teams from BEIS and NCSC to provide an overview of National Grid with the overall aim of introducing key contacts within the business and assisting them in understanding how our business works. We ran this as a day-long session giving an overview of the ET, GT, ESO and Security businesses as well as Regulatory treatment of allowances for cyber security. We arranged for the attendees from BEIS and NCSC to visit the Transmission Network Control Centre (TNCC), the Gas National Control Centre (GNCC), our Cyber Security Operations Centre (CSOC) and Alarm Receiving Centre (ARC). The purpose of this session was to give these key stakeholder organisations an overview of our control systems and how we currently protect our network from threats. They wanted to understand how we manage incidents and the key risks that we face so that they support implementation of our cyber business plans. Feedback received on this session included;

“To get such a complete overview of such a large and complex element of the CNI is key for both the NCSC and BEIS in being able to understand your challenges and how we can help” and;
“The sessions were well structured and informative and served as an extremely useful introduction to NG, which we’re looking forward to building upon over the coming weeks and beyond.”

We had a second session in September 2019 to run a deep dive on our ET, GT and CNI systems, including our risk assessment methodology and plan to hold another session to complete a more detailed technical CNI overviuew before the end of the year.

Our future plans on this engagement is to continue to engage directly with the NCSC on the specifics of our RIIO T2 business plans to understand and agree where we can work together and receive support in implementing these plans. We envisage this will be continuous engagement throughout the remainder of T1 and throughout T2. This engagement helps us build the relationships with relevant people at key stakeholder organisations to ensure we can effectively continue to protect our network from threats, specifically cyber throughout the T2 period and beyond.

KEY STAKEHOLDER OUTPUTS TO INFORM OUR BUSINESS PLANS

Due to the confidential and/or sensitive nature of our plans, stakeholders have told us to engage with the relevant specialists where possible to develop and agree appropriate solutions. These specialists have proposed that we;

1. Implement the revised standards set out in Engineering Technical Report (ETR)138 (requirements for site flood protection) by the end of the T2 period.
2. Implement required levels of Physical Security on designated PSUP sites.
3. Implement agreed cyber security enhancements in line with the NIS Regulation guidance.
4. Ensure rapid restoration in a Black Start scenario in line with BEIS proposals.

2.2 WHAT WAS THE FEEDBACK ON THE ENGAGEMENT APPROACH?

To help ensure we are taking the right approach to stakeholder engagement, we are working with research and consulting specialists ‘Truth’. Truth are supporting our stakeholder engagement by providing a comprehensive review and debrief of our BAU and specific RIIO T2 engagement for each of our stakeholder priority topics including resilience.

Over several weeks, we have worked with Truth to provide background to each of the topic areas, informing them on our stakeholder engagement approach and BAU activities to help them understand how best we can engage with stakeholders to inform RIIO T2 business plans.

As a result of this work, Truth have provided reports to National Grid summarising their review of materials provided and evaluation of National Grid’s stakeholder engagement. The key messages from the report focusing on resilience were that Truth considered that our resilience workshop, the output and resulting report were particularly well executed, analysed and reported (and could be adopted as a benchmark for future workshops). Through discussions with Truth, they understood the limitations of engagement in this area due to sensitive and confidential content however recognised that we are interested in welcoming stakeholder views where possible. Truth did not highlight any areas which require further action or suggest additional engagement activities on this topic.

The Truth report has been attached for reference here;

181113 NG
Resilience report.pd

Given the positive feedback received from the attendees of the resilience workshop and Truth in assessing our approach, we are considering how learnings from this engagement can be shared. In January 2019, we plan to host a similar workshop on the topic of reliability. For this event, we will be using a similar format where possible, with the same stakeholder engagement leads within National Grid organising and facilitating the event. As the topic of reliability is also less sensitive in nature in terms of expected content in the workshop, we should also be able to share more detail on our plans and give costed options for stakeholders to provide views on.

We have made significant progress on engaging with the NIS Competent Authority in developing our cyber security plans. So far through our engagement we have completed an updated self-assessment of our risks across our cyber landscape against the Cyber Assessment Framework provided as part of the NIS Regulations material. As a result of this, we have been able to highlight highest risk areas and prioritise investment within T1 to address these. We have now completed our T1 'tactical' improvement plan which either addresses or starts to address highest risk areas. We are currently working with the competent authority to finalise these plans, after which we will be working collaboratively to develop our longer term T2 'strategic' improvement plans. We plan to share these plans with Ofgem later in the year and include them within our December business plan submission.

FRONTIER FINDINGS

We commissioned Frontier Economics to carry out assurance of how our stakeholder engagement had been reflected within our July draft business plan. They assessed how well the lgic between stakeholder evidence and business plan actions has been documented, and identified gaps or areas of improvement.

Frontier highlighted that domestic and non-domestic consumers appear to be willing to pay a higher bill for improved network resilience. Consumers would be willing to increase their yearly bill by the following amounts for the following improvements that are partially or entirely related to network resilience.

For domestic consumers:

- £7.70 for a 2 hours decrease in the hours of powercuts at a 1.5% probability;
- £9.70 for a 4 hour decrease in the hours of powercuts at a 1.5% probability;
- £3.58 for every fewer day to recover from a blackout;

For non-domestic consumers;

- £43.30 for a 2 hour decrease in the hours of powercuts at a 1.5% probability;
- £66.95 for a 4 hours decrease in the hours of powercuts at a 1.5% probability;
- £24.15 for two fewer days to recover from a blackout;

Furthermore, the majority of consumers (60%) surveyed in the acceptability testing research agreed with NGET's proposals on protecting the network from external threats, and the associated impact on bills.

Finally, the service valuation research conducted by Explain found that 86% of consumers felt that NGET should adopt very high, high or medium-high levels of protection for the network. Only 9% felt that NGET should adopt medium-low levels, low levels or that this shouldn't be a priority area.

Frontier note that overall, the stakeholder engagement on this topic is challenging given that security plans often cannot be shared with stakeholders due to confidentiality. However, the stakeholder engagement on this topic appears to be comprehensive and well-designed and that NGET have clearly attempted to provide stakeholders with the necessary level of knowledge to express informed views.

Fronteir suggested a few areas of improvement including the follows, for which we have provided detail of how this feedback has been addressed;

Feedback received	How this was addressed
The business plan sets out the views provided by specialist stakeholders (the NGET should implement the standards set out in Flood Resilience Engineering Technical Report 138 by the end of RIIO-T2), but it is not clear in the proposed action whether NGET is committing to address this. This could be clarified.	Our outputs and proposed activities are now clearly outlined within our business plans. To clarify, where there are clear requirements (Physical Security and Extreme Weather) we are following stakeholder advice and implementing these changes.
The views of non-specialist stakeholder do not appear to be explicitly mentioned in the justification for this action. These stakeholders said that NGET's approach to extreme weather resilience needs to be flexible, forward-looking and able to adapt to future challenges. We think that it could be clarified in the business plan whether NGET considers it has developed an approach that meets these criteria.	This should now be clear within the business plan and justification report. We have needed to develop a flexible approach as site specific requirements for flood resilience are yet to be confirmed. We have also requested a re-opener in this space to account for required changes to plans in response to changing requirements (if required).
Be more specific, explain in more detail how NGET will protect sites, what actions it will take to better understand how to protect from weather-related threats, and whether ETR138 will be implemented.	We have clarified within our business plans that we will implement ETR138 within T2, however further detail on how we may protect sites is included within the Justification Report.
On physical security, it could be made clearer in the business plan that the action around the Physical Security Upgrade Programme is a government mandated requirement, and it is not driven by the views of wider stakeholders.	This should now be clearer within the business plan and supporting justification report.
On cyber security, NGET could be clearer on whether it is meeting Government-mandated requirements, or going beyond these requirements. The action could also be made more specific, clarifying what types of actions it is taking on cyber security. If this is not possible due to confidentiality, this could be stated explicitly alongside the action.	We have touched upon this in our business plans, our approach is to meet Government actions in a way which addresses our key risks. Due to complexity of our plans, detailed information on how we meet these requirements and what types of activities we are completing are included within the 'Business IT Security Plan' and the 'Cyber Resilience Plan'.
On operational telecommunications, there is limited supporting evidence due to the complexity of the topic and the limited scope for stakeholders to feed in. This could be made clearer in the business plan. NGET did engage with a specialist consultancy, other TOs and National Grid ESO, and it could be helpful to summarise the findings of these engagements.	We have provided much more information justifying our plans on operational telecommunications since July and have also received feedback from the Stakeholder User Group that we have addressed similar feedback from themselves.

On Black Start, provide some general information on what types of investments NGET is making to improve its response in a Black Start scenario. It could also possibly be added to the action that NET is still working with BEIS and other energy sector participants to develop a new Black Start standard, with improved restoration times.	This has been addressed within our business plans, we have provided additional information on the specific activities we are completing on our Black Start proposals.

2.3 WHAT WERE THE INITIAL NATIONAL GRID CONCLUSIONS?

With our business plans under the ‘protection from threats’ topic being largely prescribed by Government and formal requirements, the outcome we were aiming for with our stakeholder engagement was mainly to;

a. Inform stakeholders of the threats (and impact of such threats) we face as electricity transmission owner and how we plan to address these.
b. Understand stakeholder views on the topic to ensure we are addressing main concerns of stakeholders within our business plans.
c. Test our approach to protecting the network with stakeholders
d. Understand and agree with the relevant specialists the requirements for protecting the network from external threats.

Through our initial engagement, we understood that this is an area in which our stakeholders are interested in. We had a high level of attendance at our resilience workshop and received positive feedback on how informed stakeholders felt on the topic, even when we could not share some detailed information on our physical security and cyber security plans. Stakeholders understand the constraints around engagement on this topic due to the confidentiality and sensitivity of the information in our business plans and are comfortable for us to engage with key stakeholders only to agree appropriate mitigation measures.

Across the different channels of engagement there were some consistent views from our stakeholders which will help to inform our business plans and support the need for the level of investment we are proposing.

The main view which was consistent across stakeholders was that there is an increasing need for a resilient electricity network, and this trend is likely to continue (see figure 6 and output from ERP report above). As well as the key stakeholder groups which attended our resilience workshop in October and those which helped inform the ERP report, this trend has also been confirmed by Government. In 2011, the UK Government published its first cyber security strategy recognising the emergence of this threat. Followed by a second cyber security strategy in 2016, the creation of the NCSC and introduction of cyber specific regulations, this focus encourages owners of critical national infrastructure in the UK to create more resilient network. On the topic of cyber security, this threat is emerging and changing rapidly and requires flexibility to respond to changes in threat level as well as a baseline level of protection from known threats. In responding to this threat, we have had to invest in cyber protection and capabilities within RIIO T1 (even though it was not included within our original RIIO T1 business plans) and will be a key focus area for investment within RIIO T2 as part of our NIS strategic Improvement plans. We will continue to work with the Competent Authority to develop these plans to ensure they are robust and delivered efficiently.

We have also drawn conclusions from the views heard in our workshop and in the Black Start Task Group that there is an ask for a quicker response to a Black Start event than what could currently be provided. As mentioned previously, this is something that is being considered and worked through within the Black Start Task Group and will be consulted on. The output of this task group will inform our business plans, however the feedback received within the resilience workshop showed that stakeholders understood the practicalities of responding to a Black Start event and how long this takes as well as asking for electricity to be restored as soon as possible, especially within urban areas.

We have made significant progress in our Cyber Security plans by engaging with the Competent Authority. We have done this by following a defined process in which we have assessed our existing level of cyber security and capabilities and built short and long term plans on addressing the output of this assessment. We continue to engage with the Competent Authority to ensure these plans are fit for purpose and have the flexibility to adjust within the T2 period in line with changing threats and requirements.

We have made initial conclusions from previous engagement with BEIS and CPNI on our physical security plans. [redacted] sites which were descoped from our business plans within RIIO T1 are due for commissioning within RIIO T2 and therefore will require a level of security to be applied.

We have explored options in the market for delivering a highly resilient Telecommunications Network (OpTel). The requirement to provide high speed teleprotection limits the technology options.

3. STAKEHOLDER GROUP CHALLENGE & REVIEW

3.1. WHAT POINTS OF CLARIFICATION AND INTEREST WERE RAISED?

Points of clarification and interest were raised by the stakeholder group and included within the table below.

3.2 WHAT WAS THE OUTCOME OF THE STAKEHOLDER GROUP CHALLENGE AND REVIEW?

The table below shows the challenges and actions raised by the stakeholder group within their meetings and our response. The stakeholder group challenge and review has so far resulted in further clarity being provided within our submission document, Justification Reports and Stakeholder Engagement log and has informed how we engage with our stakeholders.

Topic specific challenges from Stakeholder Group discussion				
ID	**Date**	**Meeting**	**Challenge**	**National Grid Response**
27	03/10/2018	SG3	Differentiate between consumers, communities and citizens.	Have updated engagement log only to use the term 'consumers' to avoid confusion.
28	03/10/2018	SG3	Provide clarity on our role in resilience vs that of others /key players.	Will provide detail within engagement log, chapter and Justification Reports to provide key messaging around this.
Actions from Stakeholder Group discussion				
ID	**Date**	**Meeting**	**Action**	**National Grid Action**
9	03/10/2018	SG3	Will need to split topics and potentially engage	We have taken onboard this feedback and are ensuring that we undertake appropriate engagement for each of the sub-topics. We have run a combined workshop for all topics, where separate sessions were held for (i) cyber, (ii) physical security, (iii) extreme weather and (iv) Black Start. When engaging bilaterally with key stakeholders or relevant authorities/specialists we often only discuss one or two of these topics depending on stakeholder.
10	03/10/2018	SG3	Need to add explicit consumer impact	Consumer consequences of threats to the transmission network and the impact on their bills is included in our engagement on these topics. We will be explicit about this in our business plans and Justification Reports.
11	03/10/2018	SG3	Consider role of Amazon, Schneider, etc. w.r.t internet of things	We are currently considering how relevant this might be for us in the T2 period and how this may impact our engagement.
12	03/10/2018	SG3	Be careful how we're engaging on probabilities, balanced approach, separate our HILP events.	We have taken this onboard and will be mindful of this in future engagement.
13	03/10/2018	SG3	Look at workforce resilience within this topic	We have definite plans to consider workforce resilience explicitly in our plans. It is unlikely to sit within this priority.
14	03/10/2018	SG3	Provide the group our risk management procedure as contect to look at the business plans through	The recent webinar (7th November) covered risk management from a project specific perspective. The overarching approach to managing risks across the organisation will be shared with the Group in advance of business plan scrutiny.
15	03/10/2018	SG3	The group is keen to see that our Board understand the role of this	Trisha McAuley will be invited to meet our Board in the coming months, as part of a programme of meetings

			Group and understand / appreciate it's importance.	with key senior leaders in the National Grid business. We are seeking to arrange for one of the Senior Independent Directors from the NGG and NGET business to attend a future Stakeholder Group meeting (in the New Year).
16	03/10/2018	SG3	Build in lessons learnt from incidents we've had and that of others	Our internal process automatically reviews lessons learned from incidents and improves our approach based on this. Our cyber plans will be partially built on assessing our ability to withstand specific incidents and exsting capabilities.
17	03/10/2018	SG3	Ensure we articulate the problems in a way that will resonate with stakeholders – having someone there who has experienced it is helpful.	Articulating the benefits / consequences associated with investing in these areas is a challenging rask. Having someone there who has experienved it is a great idea that we will seek to incorporate into our engagement approach if possible. We will use examples of impact of previous incidents when discussing cyber capabilities and plans with the NIS Competent Authority.
18	03/10/2018	SG3	How we're considering interaction with other TSOs and international standards.	Comparison against international standards and benchmarks is a key part of the process for planning our resilience approach (e.g. KPMG Cyber Security Benchmark). We also collaboarate and sit on groups with other network and key infrastructure organisations (e.g. the Energy Emergencies Executive Committee E3C and CIGRE).

Table 5: Challenges and actions from the Stakeholder User Group

Separate to the Stakeholder Group meetings, we also held individual sessions for each stakeholder priority with members of the Stakeholder Group. Each Stakeholder Group member were allocated a topic to be a sponsor for. In summer 2019, we held a teleconference with our stakeholder sponser for 'protection from external threats' to challenge and give feedback on our July business plans. This session was helpful in providing feedback on our plans and clarifying certain points which perhaps unclear within our July document.

In November 2019, we also received feedback from the Stakeholder User Group which had clarified that their previous feedback from July and the stakeholder sponser session had been addressed. We also received the following feedback that has been addressed within our December submission.

1. The Group expects to see further detail and expansion of the work done on external benchmarking, with clarity on the outcomes of benchmarking exercises i.e. what has changed and why.
2. Explain the breakdown of £40m on physical security costs.
3. Provide more detail on the resourcing for OpTel and deliverability.

4. CONCLUSIONS

4.1 WHAT DOES NATIONAL GRID INTEND TO DO NEXT?

Many fo our investment plans on this topic are currently being developed as we are either confirming requirements for T2 or those requirements are currently in development.

On Cyber security, we have been engaging with the NIS Competent Authority on a regular basis since late 2018 to ensure they have sufficient information and understanding to allow them to determine how our networks and systems are currently protected from the threat of cyber attack. We have used the Cyber Assessment Framework provided to us as part of this process to complete an updated self-assessment of our risks. This self-assessment has been submitted to the Competent Authority alongside workshops to discuss. Using their feedback and advice, with the formal guidance received as part of the NIS Regulations, we have focused on addressing immediate 'high' risks on our self-assessment to develop a short-term tactical improvement plan. We are currently in the process of finalising these plans with the Competent Authority and aim to do so by end of June 2019. Following our July business plan submission, our focus will shift to the development of our RIIO T2 cyber business plans. We will continue to work with the Competent Authority as well as further engage with the Scottish TO's to ensure a consistent approach to the NIS Regulations.

We will continue to engage with BEIS and other network companies through the Black Start Task Group to help develop and align our plans to a standard on Black Start restoration. In the absence of a restoration standard being in place by the time we submit our business plans we will engage with BEIS on understanding their expectations for us as a network company in preparing for RIIO T2.

4.2 WHAT IMPACT HAS THIS FEEDBACK HAD ON THE BUSINESS PLAN?

CYBER SECURITY

Stakeholder engagement specific to the topic of cyber security has had a large influence over our RIIO-T2 business plans. Whilst we have taken a risk-based approach to our business plans and responded to the specific risk on our network, our plans have also been aligned to the requirements under the NIS Regulations. These requirements include a Cyber Assessment Framework (CAF) and RIIO-2 guidance consulted on by Ofgem in September 2019. We have continuously engaged with the NIS Competent Authority and other network companies through the E3CC throughout 2019 to keep informed of latest threats and priority topics. This has helped to shape our approach to prioritisation of investment within the T2 period. This prioritisation is reflected in our view to focus on four topic areas for immediate investment in the first couple of years of RIIO-T2. These immediate focus areas are included within our 'baseline' allowance request, with the remainder of investment which is currently more uncertain, to be requested through reopener opportunities within RIIO T2.

OTHER INVESTMENTS TO PROTECT FROM THREATS

General feedback received from stakeholders has informed the shaping of this stakeholder priority and confirmed that it is a topic that is important to stakeholders and consumers.

Our other investments have been informed by the specialist stakeholders relevant to the investment area. Outputs have been informed by specific requirements on each threat area, further detail of which can be found in the ‘I want you to protect the network from external threats’ chapter within our main submission.

5. DOCUMENT CHANGE CONTROL

Version Number	Date Updated	Updated by	Comments
0	10/08/18	Charon Balrey	Template updated post SG2 comments and to include iterative nature of engagement
1	18/09/18	Jade Clarke	First draft of log for 'Resilience' log
2	13/12/2018	Jade Clarke	Second draft of log for January stakeholder group meeting
3	24/10/2019	Jade Ison	Final stakeholder log for Ofgem submission

6. APPENDIX

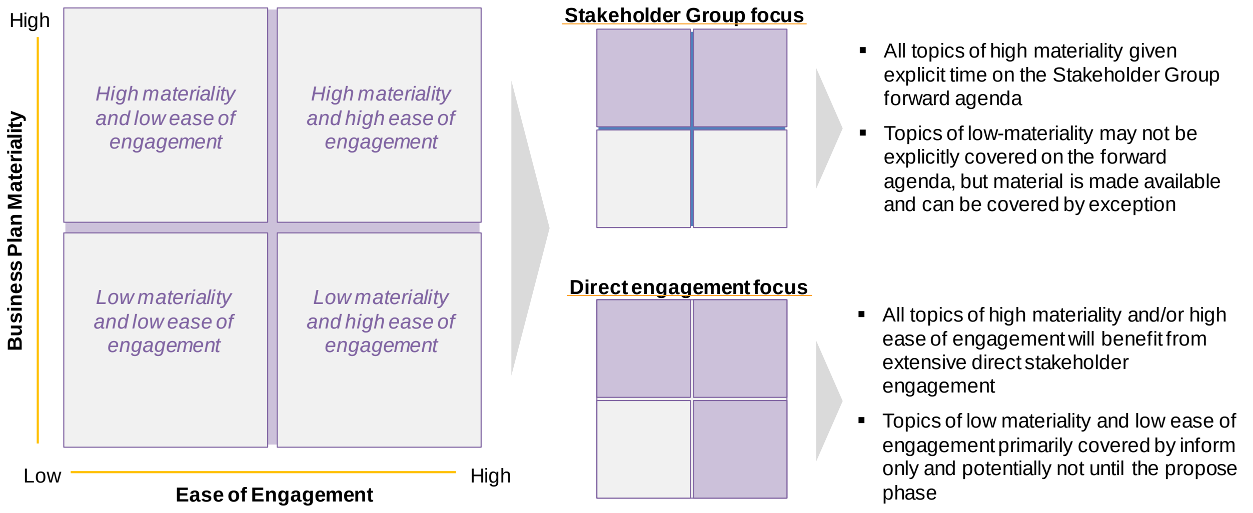
6.1 ENGAGEMENT PRINCIPLES CHECKLIST

1	Define and map your stakeholders - anyone who believes they are affected by your decisions. Recognising the different threads of the public interest – stakeholders, customers, consumers, citizens, communities (geographical and interest)
2	Be clear what you want to achieve with "engagement" – have clear policy objectives and measures of impact; (incl. where you most need to engage)
3	Understand the "spectrum of participation" and difference between each part of that spectrum: inform, consult, involve, collaborate, empower
4	Engage early in the process, review and improve throughout
5	Leadership – effective stakeholder engagement must be led from the top of the organisation
6	Commitment – to listen to stakeholders' views and act on or respond to them
7	Objectivity – an open approach to obtaining stakeholders' views and to interpreting them. Seek to understand views on a range of topics and on all aspects of the business plan, rather than pre-determining their priorities or seeking to endorse your own priorities
8	Transparency – to build stakeholder trust and show that you take their views seriously (incl. how we've considered views, weighted and managed trade-offs)
9	Be inclusive: work with stakeholder groups to gather the fullest range of interests. Understand and balance the differences between different segments. Understand and balance the differences between existing and future stakeholders
10	Be aware that those who often participate i.e. the "usual suspects" are not always representative
11	Be accessible to all (e.g. in consideration of the tasks, timelines, contact person, tech., locations, challenges of communication, etc.)
12	Use targeted approaches to tailor engagement to suit the knowledge and awareness of different groups
13	An ongoing process that is embedded across the business – not just a stand-alone business planning/price control review exercise.
14	Evidence based – use a full range of available sources of info to identify priorities, views and challenges (e.g. operational insight, bespoke research,
15	Gather evidence through a range of methodologies and tools including willingness to pay, qualitative research, surveys, complaints intelligence, market data

16	Be responsive – seek to adopt a flexible process to engagement, responding to the information revealed as the process progresses
17	Demonstrate impact of engagement – ensure that the engagement design process plans for and allows evaluation of success
18	Innovation – trying new and innovative ways of engaging

6.2 BUSINESS PLAN / ENGAGEMENT TOPIC PRIORITISATION FRAMEWORK

Business plan / engagement topic prioritisation framework


High
Business Plan Materiality
Low
Ease of Engagement
High
High materiality and low ease of engagement
High materiality and high ease of engagement
Low materiality and low ease of engagement
Low materiality and high ease of engagement

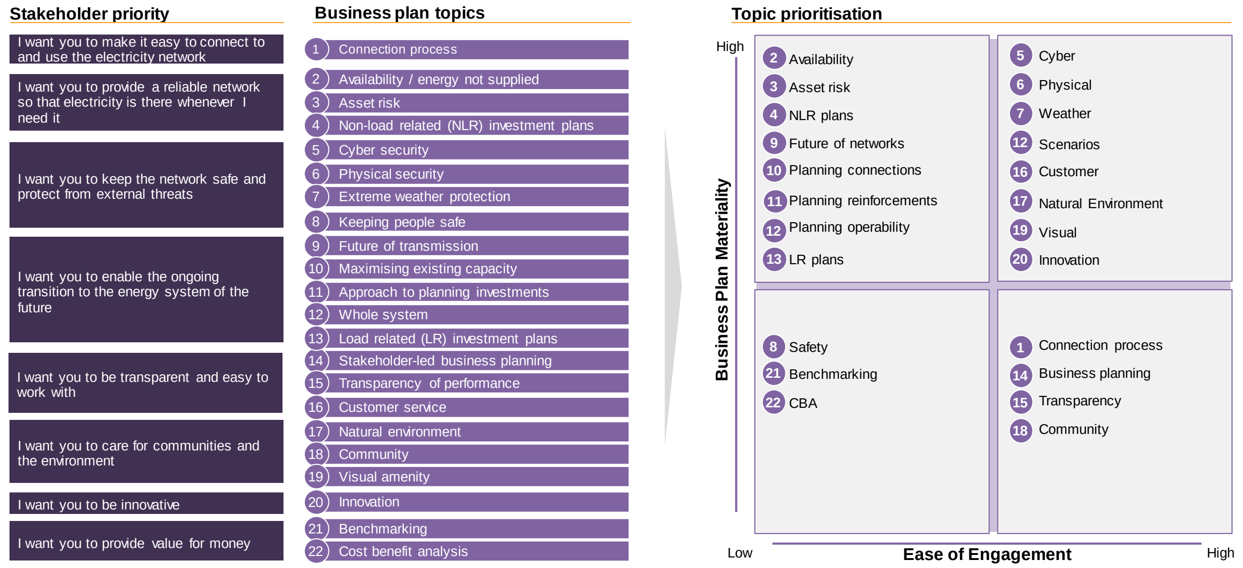
Stakeholder Group focus

- All topics of high materiality given explicit time on the Stakeholder Group forward agenda
- Topics of low-materiality may not be explicitly covered on the forward agenda, but material is made available and can be covered by exception

Direct engagement focus

- All topics of high materiality and/or high ease of engagement will benefit from extensive direct stakeholder engagement
- Topics of low materiality and low ease of engagement primarily covered by inform only and potentially not until the propose phase

Business plan topics and mapping onto framework



Stakeholder priority

- I want you to make it easy to connect to and use the electricity network
- I want you to provide a reliable network so that electricity is there whenever I need it
- I want you to keep the network safe and protect from external threats
- I want you to enable the ongoing transition to the energy system of the future
- I want you to be transparent and easy to work with
- I want you to care for communities and the environment
- I want you to be innovative
- I want you to provide value for money

Business plan topics

1. Connection process
2. Availability / energy not supplied
3. Asset risk
4. Non-load related (NLR) investment plans
5. Cyber security
6. Physical security
7. Extreme weather protection
8. Keeping people safe
9. Future of transmission
10. Maximising existing capacity
11. Approach to planning investments
12. Whole system
13. Load related (LR) investment plans
14. Stakeholder-led business planning
15. Transparency of performance
16. Customer service
17. Natural environment
18. Community
19. Visual amenity
20. Innovation
21. Benchmarking
22. Cost benefit analysis

Topic prioritisation

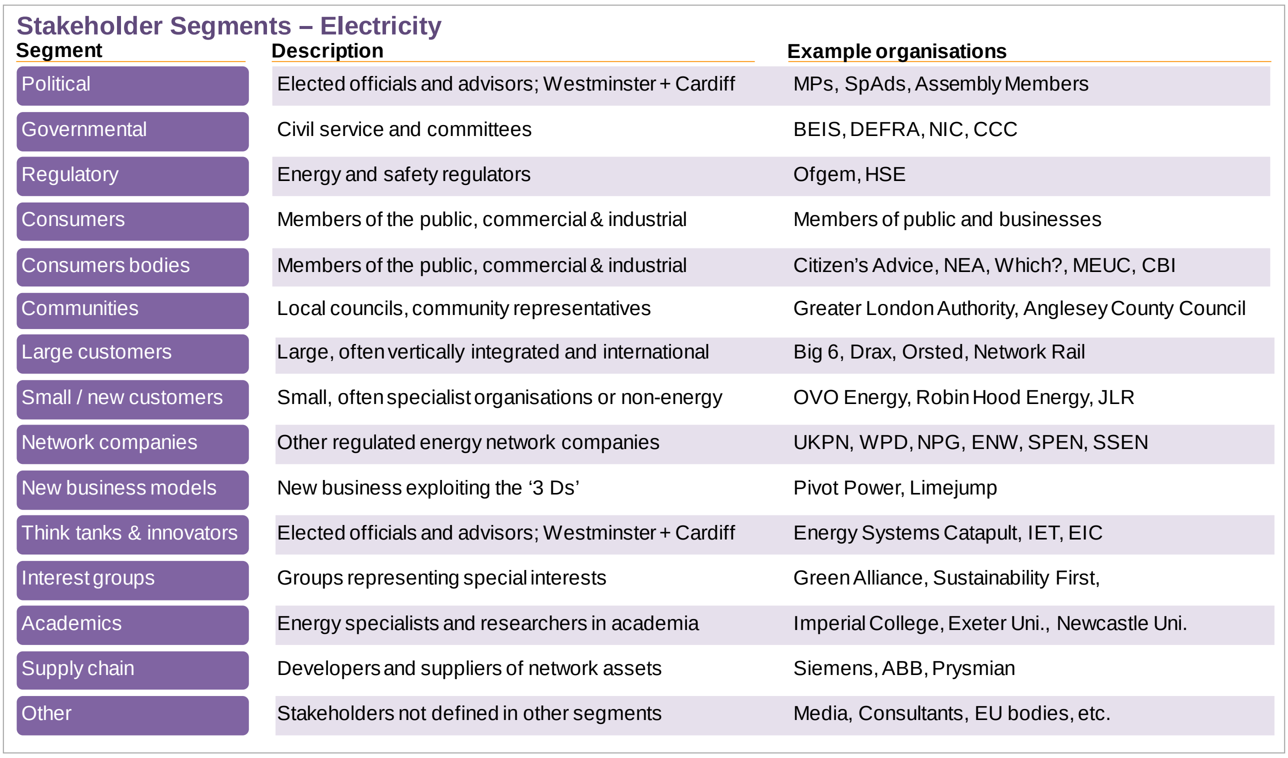
High materiality, low ease of engagement: 2 Availability; 3 Asset risk; 4 NLR plans; 9 Future of networks; 10 Planning connections; 11 Planning reinforcements; 12 Planning operability; 13 LR plans

High materiality, high ease of engagement: 5 Cyber; 6 Physical; 7 Weather; 12 Scenarios; 16 Customer; 17 Natural Environment; 19 Visual; 20 Innovation

Low materiality, low ease of engagement: 8 Safety; 21 Benchmarking; 22 CBA

Low materiality, high ease of engagement: 1 Connection process; 14 Business planning; 15 Transparency; 18 Community

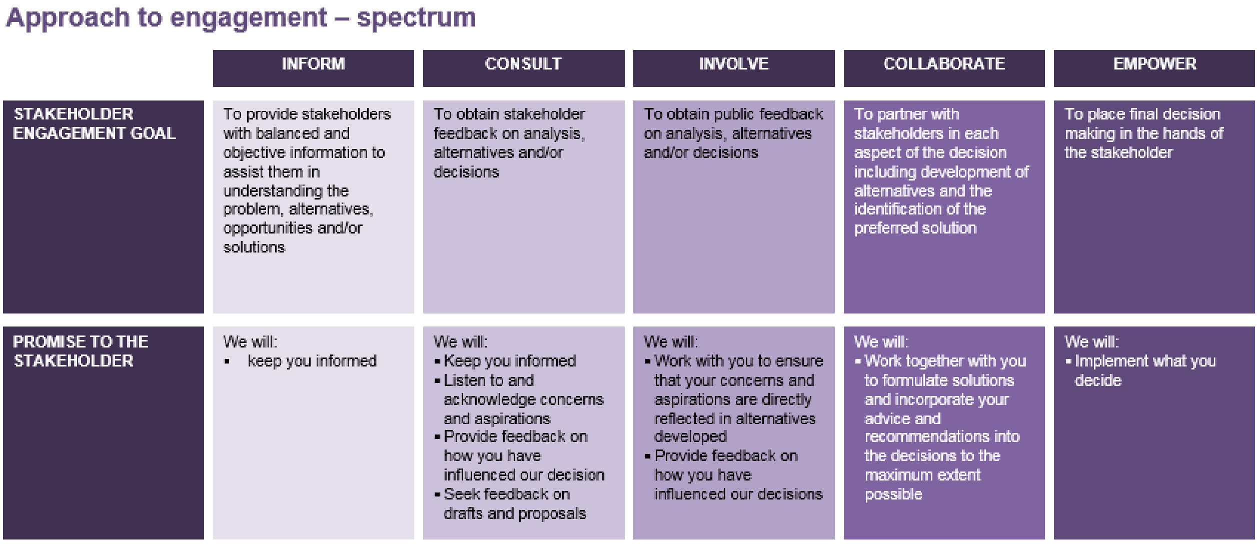
6.3 STAKEHOLDER SEGMENTS



Stakeholder Segments – Electricity

Segment	Description	Example organisations
Political	Elected officials and advisors; Westminster + Cardiff	MPs, SpAds, Assembly Members
Governmental	Civil service and committees	BEIS, DEFRA, NIC, CCC
Regulatory	Energy and safety regulators	Ofgem, HSE
Consumers	Members of the public, commercial & industrial	Members of public and businesses
Consumers bodies	Members of the public, commercial & industrial	Citizen's Advice, NEA, Which?, MEUC, CBI
Communities	Local councils, community representatives	Greater London Authority, Anglesey County Council
Large customers	Large, often vertically integrated and international	Big 6, Drax, Orsted, Network Rail
Small / new customers	Small, often specialist organisations or non-energy	OVO Energy, Robin Hood Energy, JLR
Network companies	Other regulated energy network companies	UKPN, WPD, NPG, ENW, SPEN, SSEN
New business models	New business exploiting the '3 Ds'	Pivot Power, Limejump
Think tanks & innovators	Elected officials and advisors; Westminster + Cardiff	Energy Systems Catapult, IET, EIC
Interest groups	Groups representing special interests	Green Alliance, Sustainability First,
Academics	Energy specialists and researchers in academia	Imperial College, Exeter Uni., Newcastle Uni.
Supply chain	Developers and suppliers of network assets	Siemens, ABB, Prysmian
Other	Stakeholders not defined in other segments	Media, Consultants, EU bodies, etc.

6.4 ENGAGEMENT APPROACH – SPECTRUM



Approach to engagement – spectrum

	INFORM	CONSULT	INVOLVE	COLLABORATE	EMPOWER
STAKEHOLDER ENGAGEMENT GOAL	To provide stakeholders with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions	To obtain stakeholder feedback on analysis, alternatives and/or decisions	To obtain public feedback on analysis, alternatives and/or decisions	To partner with stakeholders in each aspect of the decision including development of alternatives and the identification of the preferred solution	To place final decision making in the hands of the stakeholder
PROMISE TO THE STAKEHOLDER	We will: ▪ keep you informed	We will: ▪ Keep you informed ▪ Listen to and acknowledge concerns and aspirations ▪ Provide feedback on how you have influenced our decision ▪ Seek feedback on drafts and proposals	We will: ▪ Work with you to ensure that your concerns and aspirations are directly reflected in alternatives developed ▪ Provide feedback on how you have influenced our decisions	We will: ▪ Work together with you to formulate solutions and incorporate your advice and recommendations into the decisions to the maximum extent possible	We will: ▪ Implement what you decide

Adapted from the International Association of Public Participation – Public Participation Spectrum, 2007

6.5 PRE-ENGAGEMENT - SURVEY RESULTS

Electricity%20trans
mission%20network

6.6 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6.7 ENGAGEMENT APPROACH – SPECTRUM

PLAN AND PREPARE	IMPLEMENT & REVIEW	ACT
Clear scope and outcomes defined☐	Triangulate diverse views ☐	Use conclusions to build business plan ☐
Information sources identified ☐	Share outcomes and conclusions ☐	
Unbiased material produced ☐	Evidence to justify conclusions ☐	
Tailored to our diverse stakeholders; targeting those most impacted ☐	Undertake further engagement where required ☐	
Options consistent with our checklist ☐	Articulate where trade offs or no action taken and why ☐	
Ensure inclusivity of views ☐		