



# Annex A15.13 Engagement Log: External Threats December 2019

As a part of the NGGT Business Plan Submission

# ANNEX A15.13 – Engagement Log: External Threats

Stakeholder Priority: 'I want you to protect the system from cyber and external threats'

Author: Jonny Hosford  
Stakeholder Group meeting: N/A  
Document Version Number: 2

## Executive summary

Our stakeholder priority *'I want you to protect the system from cyber and external threats'* focuses on the importance of ensuring our assets are protected from cyber and physical attack.

Stakeholder engagement in this area is necessary to determine both desired and required levels of resilience of our network. 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 will engage with on each planned area of investment. This will help us understand expectations on us to maintain a resilient network and also what our key stakeholders want us to invest in. This has included engaging with government and industry experts to scope, agree and deliver our cyber and physical security programme alongside developing an understanding of our wider stakeholders' views on current and future threats posed by cyber and physical attack.

We have engaged extensively on a bi lateral basis with government and Ofgem, including representatives from the Centre for the Protection of National Infrastructure, the National Cyber Security Centre, BEIS and Ofgem in their role as joint Competent Authority for the NIS (Network and Information Systems) Regulations, 2018. Their feedback and direction has shaped our proposals. On cyber resilience, this has included significant developments in our approach to risk assessment and identification of proportionate security levels. For physical security, acting upon feedback to our July draft plan, we have included in our December business plan additional information on our asset replacement scope and an additional supporting annex regarding our maintenance costs. Our engagement with the HSE has also confirmed how we must apply security requirements in the context of major accident hazard regulations whilst feedback from Citizen's Advice has also supported an approach proportionate to security levels, validating our method of prioritisation of sites and systems.

This is a topic around which we cannot engage in detail with all stakeholders due to the confidentiality and national security sensitivity of our proposals. However, insight from our high-level engagement interactions on security threats has reinforced the view that this is a high priority area, which could cause disruption to the network and energy supplies and have direct consequences for our stakeholders and their businesses. This topic therefore became one of our key stakeholder priorities for RIIO 2 and we continue to engage with Ofgem following the publication of their sector specific methodology document, on how the costs to meet our physical and cyber activities should be grouped within the business plan.

We also 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. We have also established a shared sites forum with the Gas Distribution Network businesses to benchmark and collaborate on our approaches to tactical and strategic plans. These engagements have allowed us to gain an insight into industry thinking and practice regarding resilience, which has been fed into our plans for RIIO T2.

# Contents

Executive summary .....	2
Introduction.....	4
Consumer Impact .....	4
Background and drivers.....	4
Physical security - RIIO 1 .....	6
Cyber security- RIIO 1 .....	7
RIIO 2 engagement .....	8
Ofgem and BEIS engagement.....	8
<b>Engagement timeline</b> .....	10
Health and Safety Executive.....	10
Industry working groups and best practice.....	10
Wider stakeholder engagement.....	11
Stakeholder user group engagement.....	12
Other voices .....	13
Triangulation of stakeholder engagement outputs .....	14
Conclusions and next steps .....	15
Document change control.....	15
Appendices.....	16
Appendix 1: Engagement table.....	16
Appendix 2: Definitions of Stakeholder Segments .....	21
Appendix 3: Engagement Approach Spectrum .....	21
Appendix 4: Engagement principles checklist.....	22
Appendix 5: Decision making framework checklist.....	22

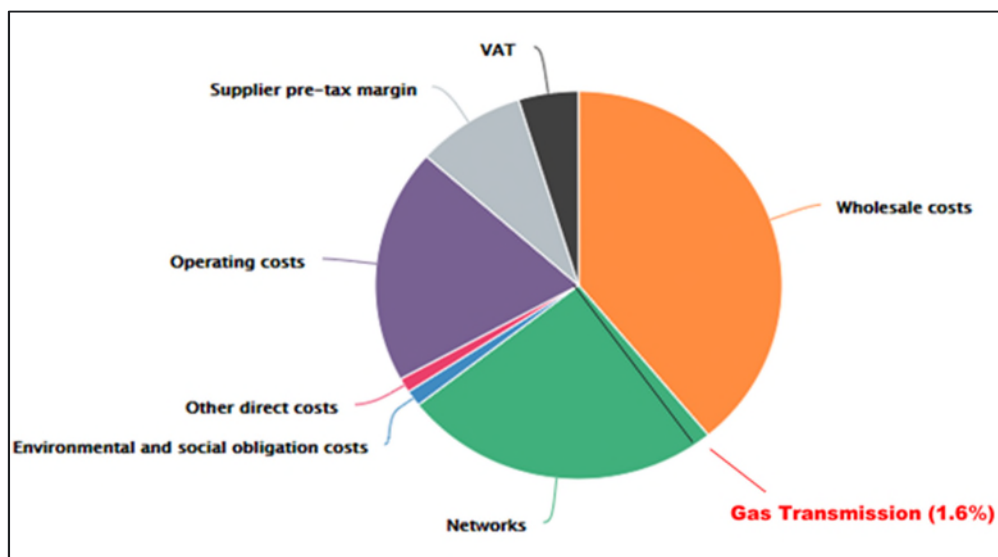
## Introduction

The stakeholder priority of 'I want you to protect the system from cyber and external threats' covers all the investments required to both enhance and maintain the resilience of the gas transmission system to ensure it is protected from cyber or physical attack. These events could impact our ability to provide a continued supply of energy to end consumers.

## Consumer Impact

Our engagement on this topic has been designed to enable us to understand and articulate the needs of our stakeholders as we move towards a future energy system; maintaining the correct balance between risk, cost and future flexibility.

The topic impacts gas consumers as costs associated with protecting the network from cyber and physical threats will form part of our TOTEX allowance which flow through shipper charges to the end-consumer bill. Over the RII0 2 price control our forecast baseline totex expenditure on cyber and external threats is £592m. Although the overall gas transmission part of the typical consumer bill is small, the impact of a malicious security incident on the gas transmission network however, would disrupt GB energy supplies, and consequently have a significant effect on other sector costs (networks and wholesale costs). In particular, the electricity sector has a strong dependence upon gas transmission with ~40% of electricity generated from gas fuelled power stations.

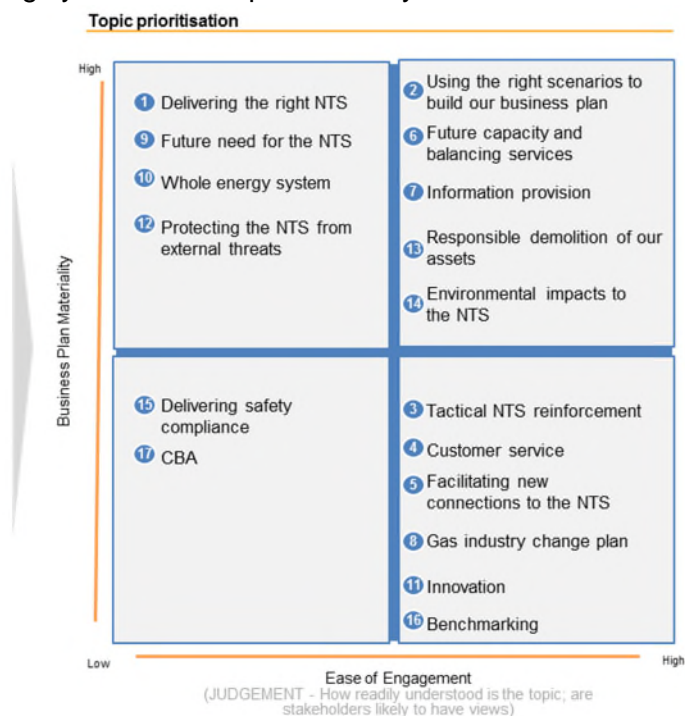


## Background and drivers

Over recent years there have been significant changes in the threat environment brought about by such factors as advances in technology and changing threat actors (individuals, member states or organisations posing a threat). Our business has already been subject to cyber and physical attacks, and to date these attacks have been largely non-destructive. The threat of a significantly damaging attack remains high and the consequences of a successful cyber or physical attack on our system would be severe. We must ensure it remains effectively protected by adapting and responding to the continual changes in the threat environment.

The network was designed with sound engineering and safety considerations at the forefront rather than with a mindset of protection from malicious threats. As threats have emerged, we have mitigated them, beginning a process of physical security hardening in advance of the 2012 Olympics which has continued through the current price control. The cyber threat landscape is evolving rapidly and the energy sector has experienced a significant increase in the volume of reported attacks since the 'Stuxnet' attack in 2010.

Government restricts the information we can share in relation to our current level of resilience or proposed mitigations to reduce network vulnerability when engaging with wider stakeholders. This has necessarily limited our wider engagement programme in this area. In terms of topic prioritisation, this topic scores highly on business plan maturity but low on ease of engagement with the wider stakeholder segments.



However, we focused our wider stakeholder engagement on understanding stakeholder and consumer views about the topic in general rather than any specific plans. For example, stakeholders have told us that managing security threats should be a priority and that they identify with the increasing threat both to society and to their own businesses. The key industry stakeholders whose requirements have directly shaped our plan are government and its security specialists and Ofgem (in their role as Competent Authority for the NIS regulations). The mapping of interest and impact of stakeholder segments is provided below, with key insight and outcomes from this engagement provided in the next sections.



Stakeholder Segment	Description	Example Organisations
Regulatory	Energy and safety regulators	Ofgem, HSE
Governmental and Political	Civil service and committees Security agencies and specialist groups	BEIS physical and cyber security teams, National Cyber Security Centre (NCSC), Centre for the Protection of National Infrastructure (CPNI),

## Physical security - RIIO 1

Following a series of attempted terrorist attacks on some of the UK's major energy infrastructure assets in the 1990s and early 2000s, the need to review and improve the physical security at key infrastructure locations was recognised by government. A national programme was established to identify critical sites and ensure delivery of physical security enhancements. The programme was initiated by the Home Secretary and led by the Department of Trade and Industry (as was), involving all the major utilities. BEIS (the department for Business, Energy and Industrial Strategy) is now the government lead for this programme.

National Grid has worked with BEIS and their security advisors, CPNI (Centre for the Protection of National Infrastructure) to identify sites as CNI (Critical National Infrastructure) based on BEIS' pre-defined criteria (such as the number of consumers affected by loss of a site on our network). CPNI define CNI to be:

“Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.”

BEIS maintains and regularly reviews the list of CNI sites. Factors affecting the list include the nature of the threat to CNI and the likelihood of occurrence. National Grid also reviews the CNI list based on changing operational conditions and guidance from BEIS and CPNI. The CNI site list was reviewed in 2005, 2009, 2010/11, 2014 and 2017. At each review, the net number of sites on the list increased, however some sites have been removed. The programme to date has been characterised by continuous evolution of site scope and volumes: the number of approved CNI sites increasing from just two in 2005.

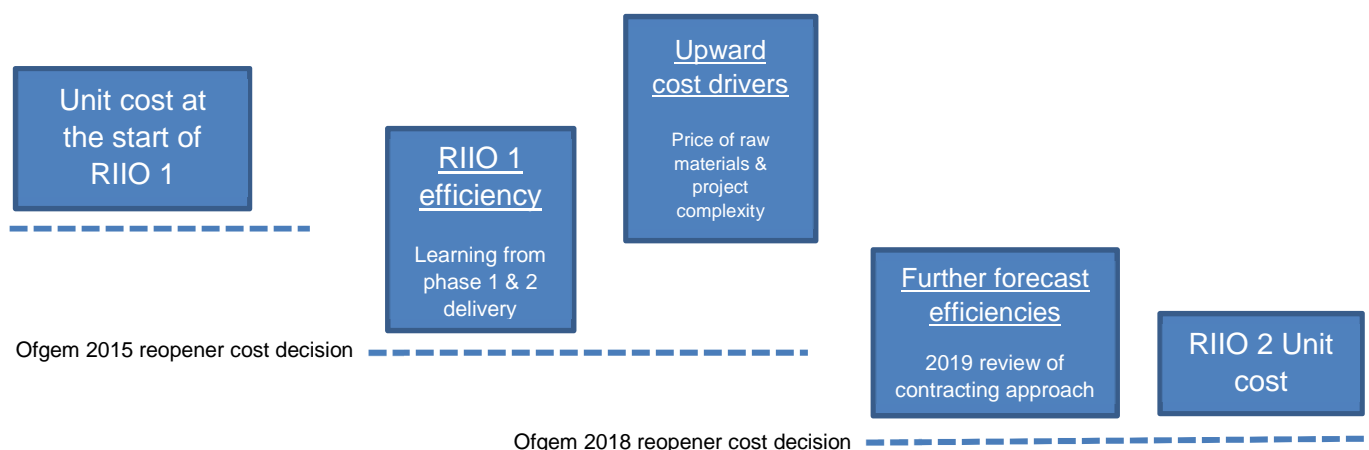
CNI sites become eligible for the Physical Security Upgrade Programme (PSUP) to increase their resilience to security threats. Not all CNI sites enter the PSUP but are monitored for inclusion or removal based on the evolving threat. BEIS sets the overall guidance for the scope of physical security enhancement works, based on CPNI's assessment of the probable attack methodologies. National Grid's PSUP includes a range of different operational site types, most of which have challenging process safety working environments, such as high pressure compressor stations, multi-junctions, pressure reduction installations (PRIs), above ground installations (AGIs) and gas terminals. Although each site is different, the typical project scope will usually include a mix of the following physical elements:

- High security perimeter barrier, with substantive foundations and anti-burrow cills;
- Various controlled access points (e.g. vehicle gates, pedestrian access);
- Intruder detection;
- High technology closed circuit television (CCTV) and lighting systems (visible and infrared);
- Power cabling and ducting;
- On-site asset and building protection (e.g. transformers, switchgear, control rooms, generators);
- On-site communications infrastructure (cabling, transmitters, receivers, processors); and
- Two-way 24/7 communications to the centralised ARC (Alarm Receiving Centre).

In 2014, following a review of sites included on the CNI and PSUP lists, BEIS issued a letter confirming site numbers and names. However, for the purposes of our RIIO T1 business plan, 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 National Grid to recover costs for required works on physical site security. As we move from RIIO 1 to RIIO 2 the government focus for threat mitigation is changing from physical to cyber. Therefore, investments in protection of IT and operational technology to reduce cyber risk are increasing areas of focus.

Our RIIO 2 cost proposals are heavily driven by the challenge and focus across the RIIO 1 price control. An external audit process was established early in the PSUP programme in order to provide assurance that the PSUP work was technically fit for purpose and that the costs incurred are value for money. The audit process included a separate technical and value for money (VFM) audit at the start and at the end of the project delivery process. In addition, two reopeners in May 2015 and May 2018 have driven efficiencies to unit cost of physical security work. This is illustrated on the chart below:



Through both reopeners, Ofgem reassessed the benchmark cost for physical security solutions. In May 2015, this involved industry consultation (full set of responses available [here](#)), reducing the funding request from £187.6m (in 2009/10 prices) to £160m. A further reopener submission was made in 2018 seeking funding for a number of sites owned by the GDNs, but containing National Grid assets (“shared sites”). The reopener was once again subject to consultation and [Ofgem’s final view](#) of the efficient cost of £8.6m did not meet the materiality threshold of the reopener of £14.5m. As a result, no further adjustment was made to our RIIO 1 allowance. The PSUP work at shared sites has subsequently been rescheduled for delivery in RIIO 2.

Our RIIO-2 plan represents our response to Ofgem’s cost efficiency challenge – we have pledged savings of £7.5m compared to the original position presented in our 2018 reopener submission. Our RIIO-2 forecast is in line with allowances set by Ofgem in 2015 and is as close as we consider attainable to Ofgem’s 2018 reopener view of efficient costs, given the circumstances (site access, complexity etc) of the ■ sites in question. It represents an ambitious challenge for our business and will require significant changes to our ways of working. We currently expect to pursue a new procurement and contracting approach moving away from use of national contracts to use of smaller local firms with more hands-on project management by our capital delivery team. We think this will bring better value for money for the type of work to be delivered in RIIO-2.

## Cyber security- RIIO 1

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 requires operators of essential services in the UK

to create more resilient networks. 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 response, we are implementing a suite of cyber resilience initiatives which were approved by Ofgem pursuant to the [2018 enhanced security reopener](#) uncertainty mechanism. These initiatives implement key foundational capabilities which we are building upon going forward.

[REDACTED]

[REDACTED]

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. 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. The risks identified range from 'very high' to 'low' which we are considering as how best to address; whilst monitoring the evolving threat landscape. This approach uses the CNI rating as a proxy for cyber impact which has been accepted as a pragmatic approach by the Competent Authority.

## RIIO 2 engagement

The threat landscape that we are facing is constantly evolving and in order to develop robust and proportionate proposals for RIIO 2 we have engaged with a range of key external stakeholders to 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, our cyber specific engagement channels also include:

Channel	Who	When
Workshops and surgeries	NIS Competent Authority	Ongoing, 2018 onwards
Briefings	BEIS	Monthly
Bi-laterals	National Cyber Security Centre (NCSC)	Quarterly

These are described in more detail in the sections below:

### Ofgem and BEIS engagement

The key stakeholders, who's requirements have shaped our plan for dealing with external threats are government (BEIS) and their security specialists, and Ofgem in its joint role with BEIS as Competent Authority for the NIS regulations. Our engagement with each of these parties in developing our RIIO 2 proposals is summarised below:

**Ofgem NIS** As mentioned in the previous section on RIIO 1, as part of our cyber work under the NIS Regulations we have developed both a self-assessment of risk and short-term improvement plans. Through 2019 we have worked collaboratively with the NIS Competent Authority to develop our 'strategic'



improvement plans which, as requested by Ofgem, are submitted as part of our RIIO 2 business plan in the form of a Business IT Security Plan and a separate Cyber Resilience Plan (Operational Technology).

The feedback from the competent authority on the first draft of the self-assessment documents led us to significantly develop our proposals. We undertook a major review involving a dedicated team, to change and standardise our approach presenting a clear, risk based, prioritised programme based upon security level risk classification. For example:

- For higher risk compressor and terminal locations: proposed full asset replacement, backed up by multi-criteria cost benefit optioneering
- For lower risk compressor sites: partial system enhancement in T2 pending replacement in T3
- It would be impossible to deliver all the work in T2 due to network outage considerations, so a rolling programme continues through T3.

We have undertaken two deep dives with the Competent Authority to review the status of inflight cyber security projects and implications arising from NIS self-assessment and improvement planning exercises. Feedback was received primarily on improving the clarity of project status. We continued to discuss progress on the Improvement Plans with feedback and clarification of next steps. We are undertaking the drafting of the required "plans on a page", with ongoing dialogue and feedback from Ofgem.

**Ofgem RIIO 2** The Ofgem RIIO 2 team have been clear that BEIS and the team within Ofgem acting as the competent authority for NIS scrutinise the cyber security part of our business plan. They have expressed a preference to see all costs in one part of our plan which we addressed through our business plan structure, splitting out the cyber work associated with compressor control systems, telemetry, metering, analysers and boundary control from the remainder of the asset health work. Our December 2019 Cyber Resilience Plan acts upon detailed feedback from the Ofgem cyber team, from its review of our July 2019 draft. For example, we provide additional information on how we prioritised sites for replacement of legacy operational technology, the basis upon which we have proposed to defer replacements at some other sites, the alternative options we have considered (including least functionality options) and providing more granularity of cost breakdown.

We have also discussed the approach for physical security in the RIIO2 business plan in detail including capex for new PSUP solutions at both NG and shared sites, commencement of asset replacement programme, opex for Alarm Receiving Centre (ARC) etc. Acting upon feedback received in summer 2019 we have included in our final business plan additional information on PSUP asset replacement proposals, and an additional PSUP maintenance annex covering our physical security opex costs. Our business plan proposals are based upon the arrangements for sharing of responsibilities and costs at shared sites in accordance with the outcome of a working group with National Grid and Gas Distribution Network representatives. We have acted upon Ofgem feedback that we should clearly show how our physical security RIIO 2 plan fits with the RIIO 1 re-opener and RIIO 1 close-out.

## **BEIS**

On the 26<sup>th</sup> June, BEIS and NCSC, visited National Grid House. National Grid provided an overview of electricity and gas network operation and the challenges posed by cyber security at the visit to National Grid House. The team also visited the GNCC and TNCC control rooms and were given an overview of cyber resilience priorities in RIIO 1 and proposals for RIIO 2. The visit was well received and further deep dive sessions to be set up to get into further detail including to talk through further detail of RIIO2 plans.

## Engagement timeline



## Health and Safety Executive

In its [2018/19 business plan](#), the HSE reflects an increased focus on the emerging risks of cyber security and it has recently updated its operational guidance on cyber security for industrial automation and control systems. This is specifically relevant to us because we operate these systems for major hazard risk reduction and continuity of gas supplies, and our planned RIIO-2 cyber resilience activities are in line with latest HSE guidance. We have undertaken bi-lateral meetings which have further confirmed that we must apply the higher security standard, whether a NIS requirement or a major accident hazard requirement.

## Industry working groups and best practice

Our RIIO 2 engagement encompasses a number of industry working groups. The focus of these groups and interactions is on either an element of resilience, or an approach for holistic resilience management.

- Current industry resilience working groups such as E3C
- Government bodies to reflect national societal interests
- Networks dependent on National Grid such as electricity and gas distribution companies, 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
- European bodies and associations, aligned to cyber policy developments

We collaborate on best practices across the National Grid group where we own gas and electricity transmission and distribution networks across the north eastern United States. Working closely with US colleagues helps us gain more powerful insights in our 24/7 analysis and management of global security information and event data. We have also recently had a technical and asset management benchmarking session with Enexis, a Dutch electricity distribution company. In December 2018, we supported and partook in an incident exercise in Estonia. NGGT was instrumental in developing the exercise and providing the gas transmission engineering advice into the incident exercise. These inputs were both recognised through correspondence from BEIS following the event.

We have visited a number of gas distribution networks to understand and share best practice on their approach to physical security. For cyber, we run the shared sites forum for cyber, and an incident management procedure is about to be submitted through the Offtake Arrangements Document (OAD) process to permanently embed this on behalf of all networks. We are also undertaking cyber risk assessments on shared sites and will be sharing our cyber asset taxonomy with the gas distribution businesses.

We have undertaken a number of innovation projects in this area, drawing on new skills and technology developments in open source programming, particularly in relation to cyber security on our SCADA systems.

## Wider stakeholder engagement

Although there were limitations due to the confidential nature of the topic, our engagement approach to building the RIIO 2 proposals was designed to gain insight on stakeholders' concerns relating to resilience of the transmission system against cyber and physical threats. A summary of the events, the attendees and their insight is provided in the table below:

What	Who	Location	Summary
Shaping the future events	Gas distribution networks, Energy network operators, Regulators, Academics, Industry trade bodies, Supply chain, Customers (shippers), Customers (entry), Customers (exit), Interest groups, other non-energy	London, Edinburgh, Warwick	Broad engagement events designed to understand stakeholders' priorities for energy now and in the future.
Future needs of the network workshops at our Terminals	Customers (entry), Other energy industry, Government (Local Authorities)	Bacton St Fergus	The regional and terminal events were one day events which have been central to our RIIO 2 engagement approach. The events included a series of overview presentations followed up with facilitated discussions and voting to capture stakeholders' views.
Future needs of the network workshops - Regional engagement	Gas distribution networks, Energy network operators, Regulators, Academics, Industry trade bodies, Supply chain, Customers (shippers), Customers (entry), Customers (exit), Interest groups, other non-energy	Workshop within different GDN boundaries Chester & London (Hull was cancelled due to lack of take up)	
Cultural analysis	Consumers - domestic	National	Innovative approach to understand why consumers make the choices they do and the influences around them. Looking into the future to see how these will change etc
Acceptability testing	Consumers – domestic and non domestic	Nationally representative	A survey to understand the level of acceptability of our business plans.
Slider tool	Consumers – domestic	Nationally representative	A survey based on an interactive online tool that allows consumers to make choices on the level of service

			they receive and see an immediate impact
Question	Response		
What is important to you and your business?	<ul style="list-style-type: none"> <li>• “[RIIO 2] outputs need to include cyber security. Full agreement around the table that this definitely needs to be there and funded” – [REDACTED]</li> <li>• “Cyber security - huge impacts as a consumer” – [REDACTED]</li> <li>• “If cyber-attack took down transmission network - how would the UK last? National security issue - what are the impacts not just country runs out of gas” - [REDACTED]</li> <li>• “Agree 100% with the critical need to protect the transmission system against cyber and external threats. National Grid need to highlight the minimum expectations of its stakeholders” – [REDACTED]</li> <li>• “All agree cyber safety is essential and non-negotiable. There needs to be risk management and systems need to be put in place” – [REDACTED]</li> <li>• “There needs to be innovation” – [REDACTED].</li> </ul>		

We have also engaged across a range of stakeholder segments with number of individuals and organisations in each segment presented in the table below:

<b>Consumer interest group</b> Total engaged: 1 No of org: 1	<b>Consultant/ supply chain</b> Total engaged: 46 No of org: 24	<b>Customer (entry)</b> Total engaged: 38 No of org: 21	<b>Customer (exit)</b> Total engaged: 22 No of org: 9
<b>Customer (shipper)</b> Total engaged: 41 No of organisations: 22	<b>Energy network operator</b> Total engaged: 15 No of organisations: 9	<b>Environmental interest group</b> Total engaged: N/A No of organisations: N/A	<b>Gas distribution network</b> Total engaged: 30 No of organisations: 4
<b>Industry/ trade body</b> Total engaged: 29 No of organisations: 14	<b>Other energy industry</b> Total engaged: 21 No of organisations: 8	<b>Other non-energy industry</b> Total engaged: 8 No of organisations: 7	<b>Regulator/ Government</b> Total engaged: 33 No of organisations: 10
<b>University/ think tank</b> Total engaged: 34 No of organisations: 9	<b>Major energy user</b> Total engaged: 19 No of organisations: 14	<b>Domestic consumers</b> Total engaged: 4341	<b>Non-domestic consumers</b> Total engaged: 150

## Stakeholder user group engagement

A briefing paper by Jonny Hosford on the "protect from threats" stakeholder priority was submitted to the third meeting of NG Stakeholder User Group in September 2019. This was also shared with Ofgem RIIO 2 team for consideration in relation to RIIO-2 framework development. The Stakeholder Group's view was that in light of confidentiality and security sensitivity this is not an area of the plan that they would get into the detail on. They would limit their involvement to consideration of the process we follow, leaving the detail to be worked out by the key stakeholders Ofgem, BEIS, HSE and advice from security agencies.

In June 2019, we had feedback from SG on our pre-July draft business plan. We presented to four members including independent chair, Trisha McAuley, Paul Denniff, Zoe McLeod and Campbell Murdoch.

The Stakeholder Group discussed if NGGT can go beyond the minimum on this topic, as the benchmark to get to the minimum required standard is already very challenging. Members noted that NGGT could engage with stakeholders on identifying risks, which has been done successfully in other sectors. NGGT

could also seek to engage with consumers on what makes them feel safe and gives peace of mind. NGGT need to emphasise how they are delivering value for money e.g. visit to SGN, benchmarking and competition. Members asked for clarification on the term 'energy sector leader'. NGGT described some of their collaborative and leadership activities in this area.

Subsequent to this meeting, and in advance of the July submission, we made a number of changes to the chapter draft including:

- ❖ Greater clarity on costs included within the chapter, calling out in chapter narrative and in assumptions log that we have consciously included OT and enhanced security asset replacement costs in this chapter and the reasons why.
- ❖ Efficiency narrative made stronger in costs section of chapter and key messages.
- ❖ Updated narrative to recognise further engagement with Ofgem and Competent Authority is expected to result in refinements to how our plan is presented.
- ❖ Clarified the term "energy sector leader" and updated chapter to quote our mission statement for security

## Other voices

To make a balanced evaluation of stakeholder views, presented below is an overview from a number of other third party external organisations, primarily on cyber security in the energy sector. There are a number of common themes including preparation for worst case scenarios and establishing the right level of funding for the risk.


The European Commission, [Cybersecurity in the energy sector](#), March 2019

"Although there is a comprehensive overall legal framework for cybersecurity, the energy sector presents certain particularities that require particular attention:  
Real-time requirements - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

Cascading effects - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.

Combined legacy systems with new technologies - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats."

The report, by the global insurance and risk management group Marsh, *Could Energy Industry Dynamics Be Creating an Impending Cyber Storm?*, shows that more than one in four respondents were aware that their company had been hit by a damaging cyber attack in the last year, while more than three quarters of respondents (76%) were worried about cyber attacks interrupting their business operations, with a similar proportion (77%) preparing to increase the amount they invest in managing cyber risks.

Yet, despite these fears about the impact of cyber attacks on production and revenues, more than half of energy executives in the survey had not quantified or did not know what their worst possible exposures could be.  The Marsh study follows the

### EY, [Spotlight on security spending for CNI firms](#)

The UK energy industry spends around £265m a year to protect itself against data breaches and system outages.



Yet 94 per cent of the sector has seen an increase in the number of breaches over the last five years, with 30 per cent having battled an online security breach in the past 12 months,

#### **Spending according to sector benchmarks**

I often get asked: "How much of their overall budgets should CNI firms be spending on security? Should certain sectors be increasing their spend amidst new regulations and threats to match others across their industry?" The simple answer is: "It all depends".

As a sector, benchmarking security spend can provide useful guidance but must correlate with the maturity of CNI companies benchmarked against.

A company that invested considerably on security improvement a few years ago may see overall spend decrease as certain processes mature and efficiencies are realised (e.g. through centralisation of monitoring, identity provisioning, automation). Therefore, benchmarking a company's security spend should be against CNI companies in a similar place in terms of technology maturity, investment cycle and business transformation.

Furthermore, different CNI companies have different risk appetites and tolerance levels, even in the same industry.

As cyber resilience continues to be a major concern, particularly for companies that make up critical national infrastructure, collaborating across industry, by sharing investment and security strategies, will be vital in helping us move towards a better working and protected society.

## Triangulation of stakeholder engagement outputs

In September 2019, on our behalf, Frontier Economics undertook a study to draw out the robust messages from stakeholder research based on a systematic triangulation of evidence. Stakeholder views have been collected from a wide range of sources. Each source can provide insights, but also has limitations. By triangulating multiple strands of evidence, the aim is to derive robust conclusions on stakeholders' views from a holistic assessment of the entirety of the evidence. Their results are presented in the form of answers to five questions:

### "What new evidence is there on stakeholder views?"

The majority of consumers accept NGGT's investment proposals to protecting the system from external hazards, along with their associated costs. However, the majority accepting this is significantly lower than

for other areas, including for safety. More than a third of consumers accepted the proposals but did not accept the bill increase. A significant proportion of respondents also responded 'no' or 'unsure' to a hypothetical willingness to pay question that related specifically to cyber security.

Is there a consensus among stakeholders?

35% of consumers accepted the proposals to protect the system from external threats but were not willing to pay more. Discussion in the focus groups suggested that this may be because consumers see this as a basic requirement of NGGT, rather than something they should pay extra for.

How does this compare to the findings described in the July Business Plan?

This evidence reinforces the view that consumers see this area as important and adds additional evidence on the consumer acceptability of the specific proposals.

Based on this new evidence what changes to the Business Plan conclusions and proposed actions are justified?

No changes are justified.

How have trade-offs been made in reaching these conclusions?

A relatively significant proportion of domestic consumers were not happy with the bill increases associated with the safety investments. However, given these investments are driven primarily by the need to comply with legislation there is not a case for reconsidering them.”

## Conclusions and next steps

The engagement we have completed to date has been extremely useful in reinforcing the importance of this topic to our stakeholders and the importance of getting the right strategy and investment for all current and future stakeholders.

## Document change control

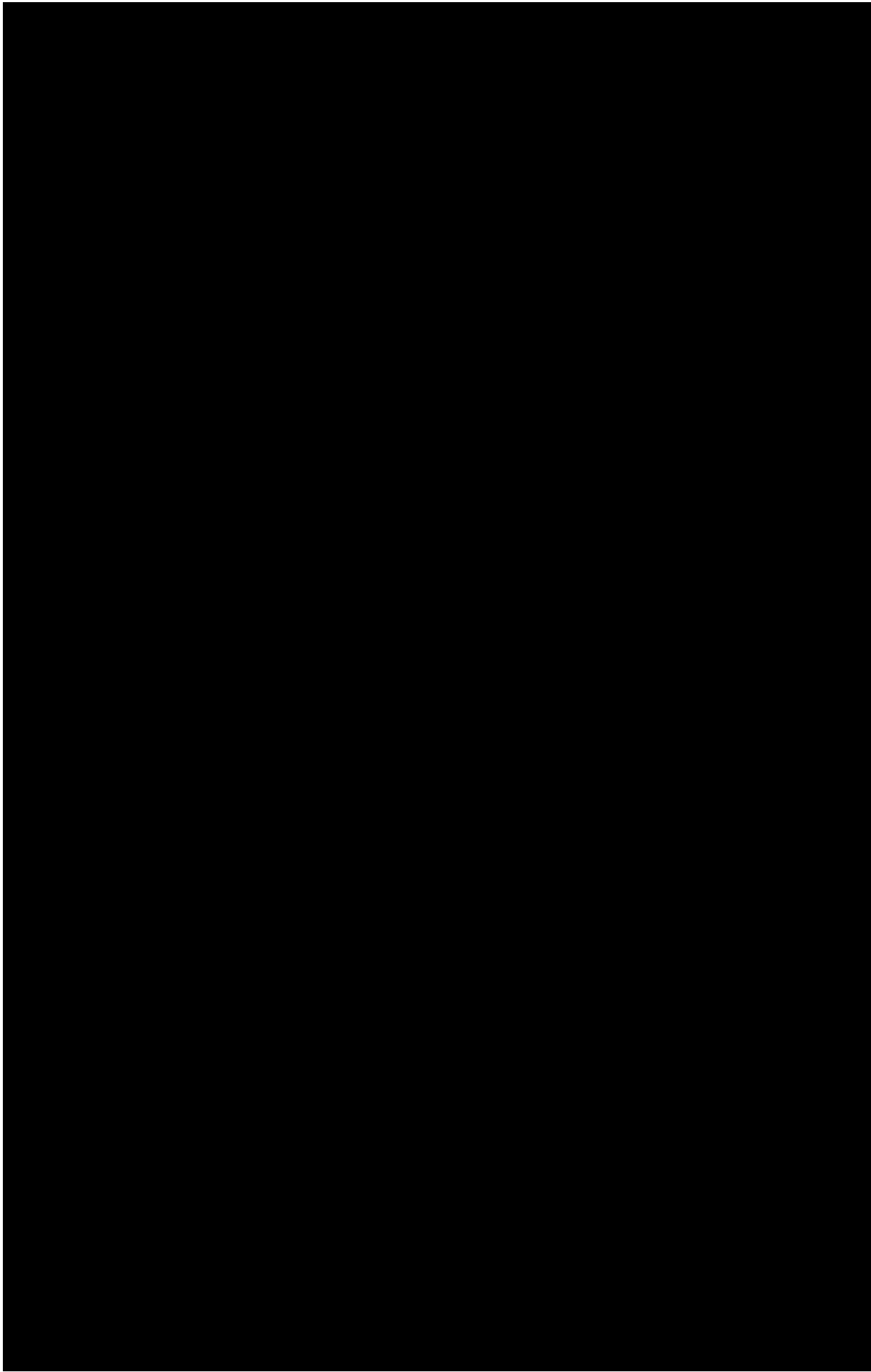
Version Number	Date Updated	Updated by	Comments
1	September 2019	Tamsin Kashap	October submission
2	November 2019	Jonny Hosford	December submission

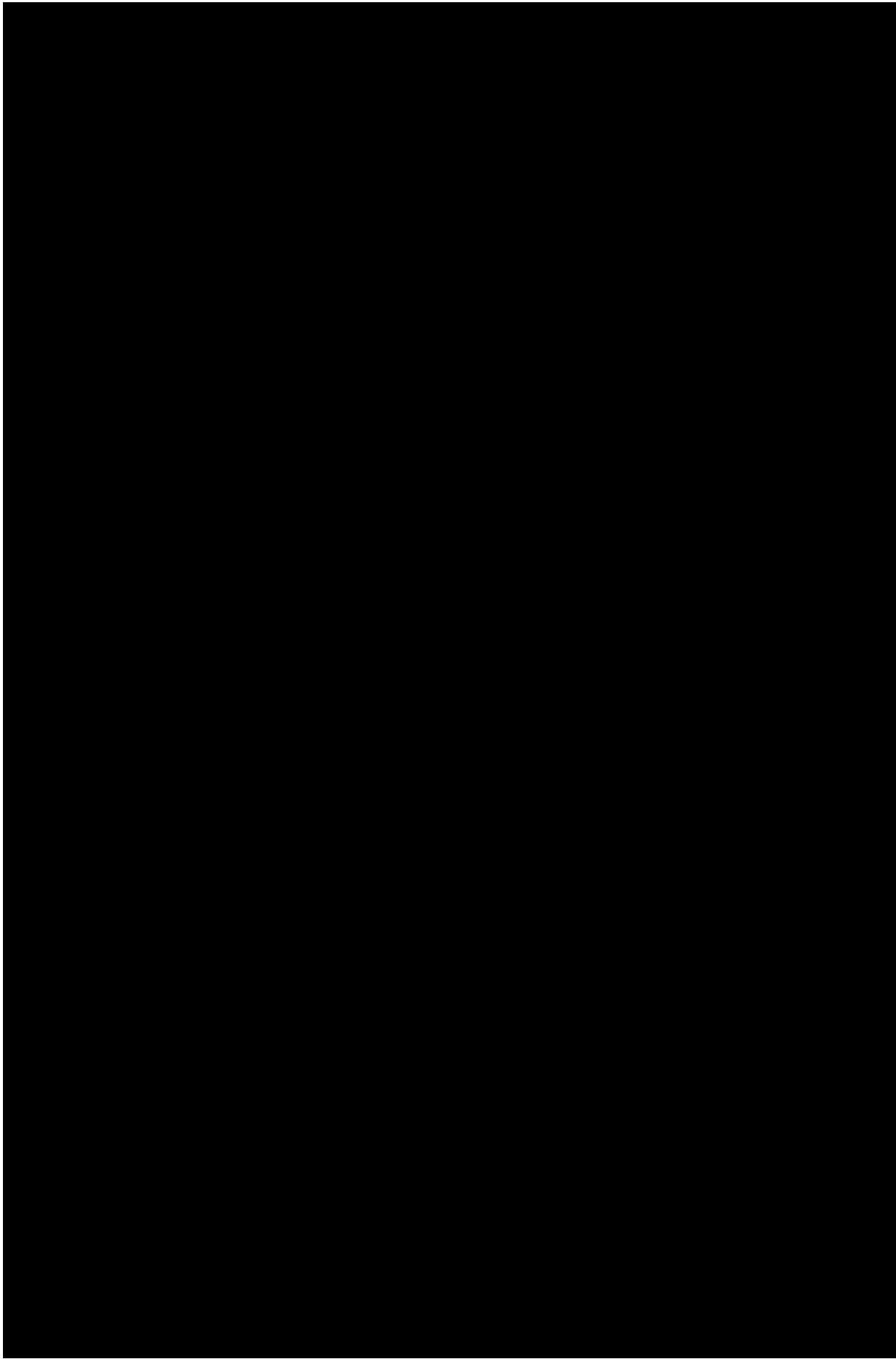
# Appendices

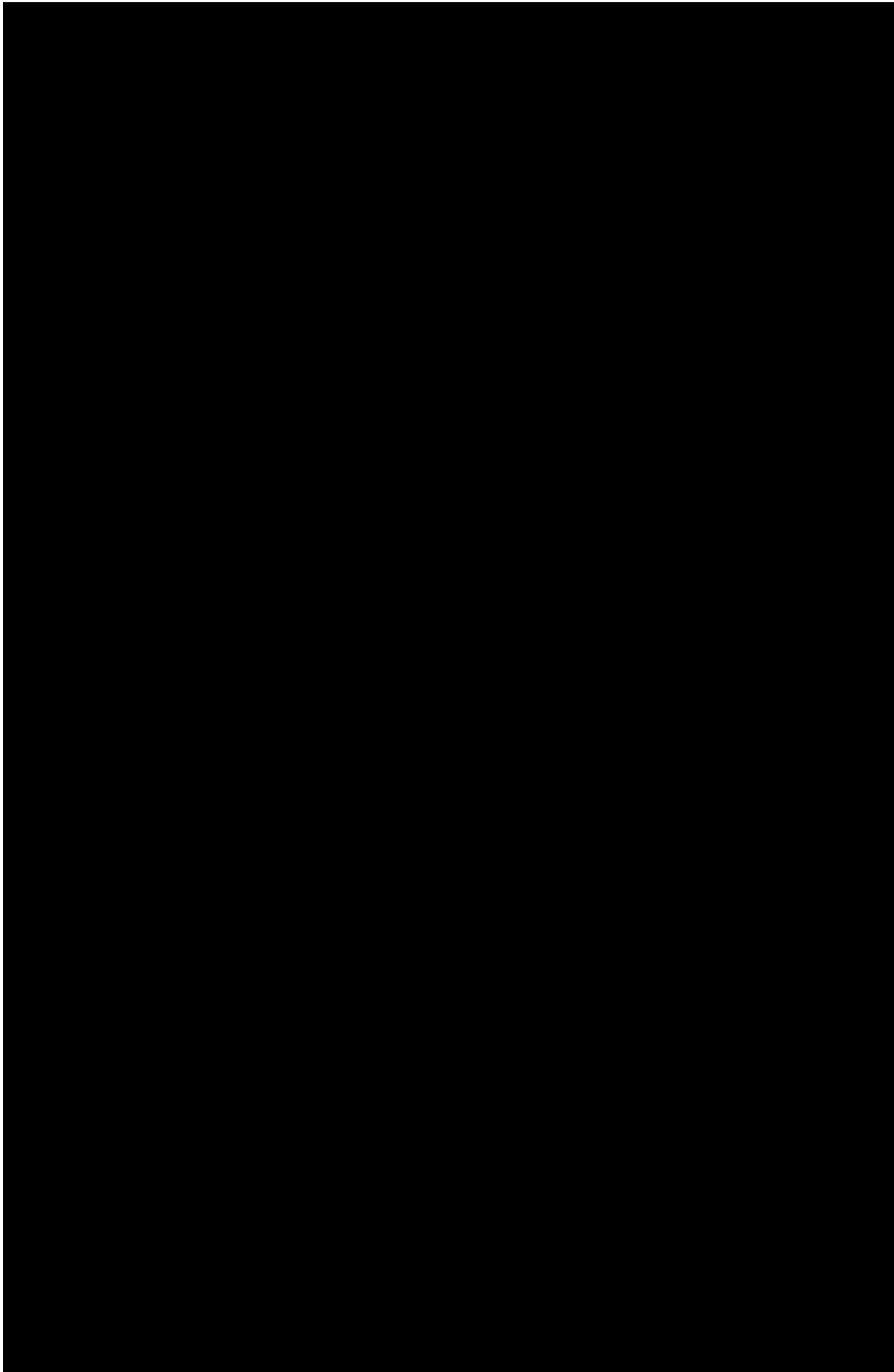
## Appendix 1: Engagement table

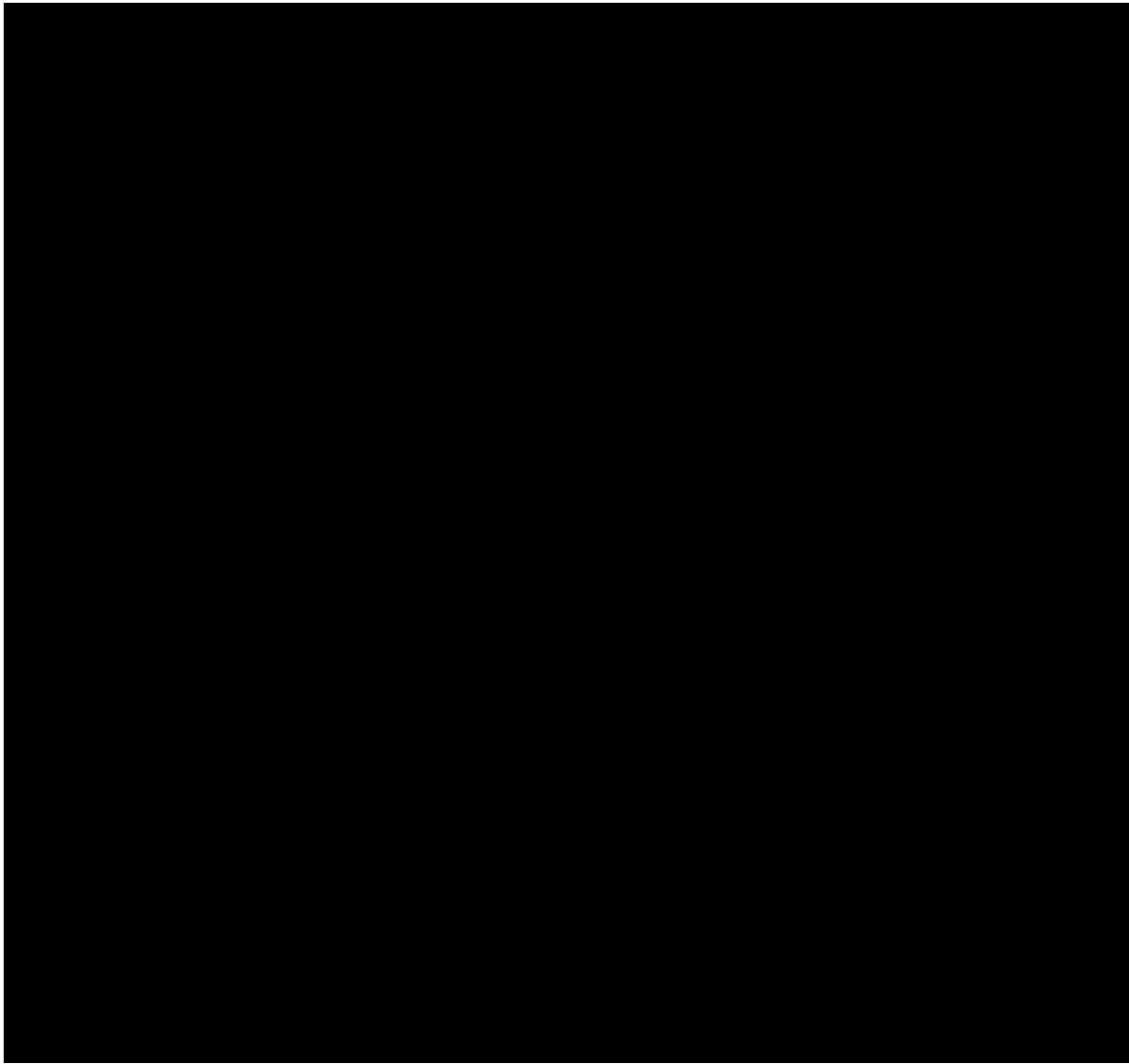
Date	Channel	Who	Outcome
[Redacted content]			











## Appendix 2: Definitions of Stakeholder Segments

Stakeholder Segment	Definition
Political	Elected officials and advisors including Westminster, Scotland and Wales
Governmental	Civil service and committees including BEIS
Regulatory	Energy, safety and environmental regulators
Domestic and industrial consumers	Household consumers Major energy users who use gas as feedstock e.g. Ceramics and chemical industries
Consumer bodies	Representatives that protect the interest of consumers
Local communities	People who are impacted in areas where we operate or have major projects
Customers - Entry	Customers connected to the NTS that put gas on to the network. Including terminals, producers and storage operators
Customers – Exit	Customers connected to the NTS that take gas off the network. Including power stations and major industrial users
Customer – Shippers	Customers that buy and sell gas
Network companies	Other regulated network companies including distribution networks
Think tanks, innovators, academics	Energy specialists, innovators and advisors
Interest groups	Groups representing specialist interests including environment
Supply chain	Developers and suppliers of network assets
Industry trade bodies	Groups that represent specific groups of customers or stakeholders including IGEM, UKOPA, Oil & Gas UK
Other	Stakeholders that are not defined in other segments

## Appendix 3: 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: <ul style="list-style-type: none"> <li>keep you informed</li> </ul>	We will: <ul style="list-style-type: none"> <li>Keep you informed</li> <li>Listen to and acknowledge concerns and aspirations</li> <li>Provide feedback on how you have influenced our decision</li> <li>Seek feedback on drafts and proposals</li> </ul>	We will: <ul style="list-style-type: none"> <li>Work with you to ensure that your concerns and aspirations are directly reflected in alternatives developed</li> <li>Provide feedback on how you have influenced our decisions</li> </ul>	We will: <ul style="list-style-type: none"> <li>Work together with you to formulate solutions and incorporate your advice and recommendations into the decisions to the maximum extent possible</li> </ul>	We will: <ul style="list-style-type: none"> <li>Implement what you decide</li> </ul>

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

## Appendix 4: 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

## Appendix 5: Decision making framework checklist

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