ofgem Making a positive difference for energy consumers

Safety, Resilience, and Reliability Working Group – Workforce Resilience

26/03/2020

Agenda

- Introductions and actions review (13-13:15)
- Workforce resilience metrics (13:15-14:30)
- AOB, Actions, and close (14:30-15:00)

Conference call details:

Dial: 0800 376 8224

PIN: 82957238#

- Based on previous discussions and material presented, we have put together initial thoughts on potential metrics to cover workforce resilience.
  - These are not finalised or decided; they are to promote some discussion.

- How these would be reported/recorded are still to be decided.

- Two elements:
  1. Workforce satisfaction sur vey with consistent questions across the industry.
  2. DNO-specific questions/measures developed in accordance with workforce's preferences.

- Consistent reporting of workforce characteristics across the industry.
  - E.g. Male/Female proportions, BAME proportion, pay equality/pay gap

- Associated narrative setting out key steps taken (or to be taken) to improve all metrics.

- Three elements:
  1. Number of reportable incidents/HSE notices/Investigations
  2. Staff survey results
  3. Working hours lost due to work-related absence/illness

- Reporting of common measures around workforce mental health.
- Associated narrative setting out a summary of the policies/processes that are in place to support staff

ofgem Making a positive difference for energy consumers

Our core purpose is to ensure that all consumers can get good value and service from the energy market. In support of this we favour market solutions where practical, incentive regulation for monopolies and an approach that seeks to enable innovation and beneficial change whilst protecting consumers.

We will ensure that Ofgem will operate as an efficient organisation, driven by skilled and empowered staff, that will act quickly, predictably and effectively in the consumer interest, based on independent and transparent insight into consumers' experiences and the operation of energy systems and markets.

www.ofgem.gov.uk

ofgem Making a positive difference for energy consumers

Introduction to Cyber Security in RIIO-2

27/03/2020

Purpose and Key Messages

What are we doing / what do we want to achieve?

For RIIO-2, we want to ensure Network companies maintain and prepare the systems so that they are protected, and can withstand an ever-evolving cyber-risk landscape.

Through this, we decided in the SSMD:

1. Each network company is to perform self-assessment against the Cyber Assessment Framework (CAF), using a risk based approach to do so.
2. Each network company drafted a short-to-medium term cyber-security improvement plans based on self-assessments during RIIO-1. This will inform RIIO-2 Business Plans.
3. Each company to submit a **a) Business IT Security Plan (above BAU)** and **b) Cyber Resilience Plan (in response to NIS Regulations)** as part of their Business Plans

Why are we doing this?

Ensure companies develop and submit strategic investment plans for cyber resilience setting out the steps they propose to take during the RIIO-2 period and beyond to comply with the Network and Information Systems (NIS) Regulations

How are we doing this?

As joint Competent Authority (CA) with BEIS, Ofgem's Cyber Team will review BPs and work with the RIIO team to ensure:

1. costs are appropriate, proportionate, and justified;
2. comply with NIS Regulations; and,
3. assure agreed level of cyber resilience in RIIO-2

Context of interlinking legislation

Network and Information Systems (NIS) Regulations introduced in 2018.

The aim of the NIS Regulations is to increase the overall cyber security and cyber resilience of Operators of Essential Services (OES). The NIS regulation sets out:

- What is an OES and the Competent Authorities (CA) for each EU country;
- Security duties of OES;
- Enforcement and investigative powers of the CA (including penalty amounts)

The National Cyber Security Centre ('NCSC') developed a sector-agnostic Cyber Assessment Framework ('CAF')

The purpose of the CAF is to OES in achieving compliance by demonstrating they meet an appropriate level of cyber resilience. Companies undertake a self assessment.

CAF helps identify what needs to be done for RIIO-2. BP submissions for RIIO-2 would be in addition to improvements identified against the CAF. The Cyber team will assess CAF self-assessment, improvement plans, and BP submissions.

As joint CA, it is Ofgem's role to ensure that companies comply with the NIS Regulations, and that their BP submission deliverables and costs are appropriate, proportionate, and well justified.

What we've said – SSMD May and BP Guidance

Transmission, Gas Distribution and the ESO may submit cyber resilience plans along with BPs in December 2019* covering the RIIO-2 Period

Business IT Security Plan	Cyber Resilience Plan
Primarily focussed on **Information Technology (IT)** security for business systems. Submissions are for projects **above** BAU.	Primarily focussed on **Operational Technology (OT)** in response to the NIS Regulations
Funding for IT will be provided as part of **normal regulatory allowances**. Subject to TIM. BAU IT projects will be submitted separately within BP.	Funding will be provided using a separate "**use-it-or-lose-it"** allowance which will be provided, should Cyber Resilience plans requirements be considered appropriate, proportionate and efficient.
A **mid period** re-opener mechanism will be applied to account for uncertainty. There will be no re-opener at the beginning of RIIO-2, as requirements for this area are relatively mature	A re-opener mechanism will be applied to account for uncertainty at the **beginning**, and **mid period** of RIIO-2, as we recognise companies may not be ready to share detailed plans in Dec.

Cyber Resilience Plan submitted in December will be assessed against the minimum requirements for quality. Omission of a Cyber Resilience Plan in December Business Plans will not be considered incomplete

***Companies are not required to submit their cyber security plans in Dec 2019. We have in place a re-opener for companies to submit plans when they are well prepared and justified.**

Operational Technology (OT) Scope

Developing an OT Replacement Business Case

- Draft guidance was developed to assist with OT cyber resilience planning, based on Cyber Assessment Framework (CAF)
- Draft guidance proposed is not a compliance benchmark for companies; overall management of risks and associated mitigation planning are the sole responsibility of the network companies.

- Network companies should be able to identify and cost the appropriate split on shared IT and OT services. There can be no overlap of these costs.
- Major upgrades, their benefits, and opportunities must be justified

- Network companies should have explored and documented **all other options**, before considering OT replacement
- A business case should include (but not limited to):
  - Business Strategy & Direction
  - Asset/ OT classification, OT life, OT risk assessment
  - Mitigation Options
  - Define specifications
  - Prioritisation and Planning
  - Budget
  - CBA
  - Delivery Reporting

The Cyber team will be assessing companies' BP submissions against the guidance we published.

The RIIO team will be facilitating, and keeping the Cyber team up to date.

The cyber team is responsible for:

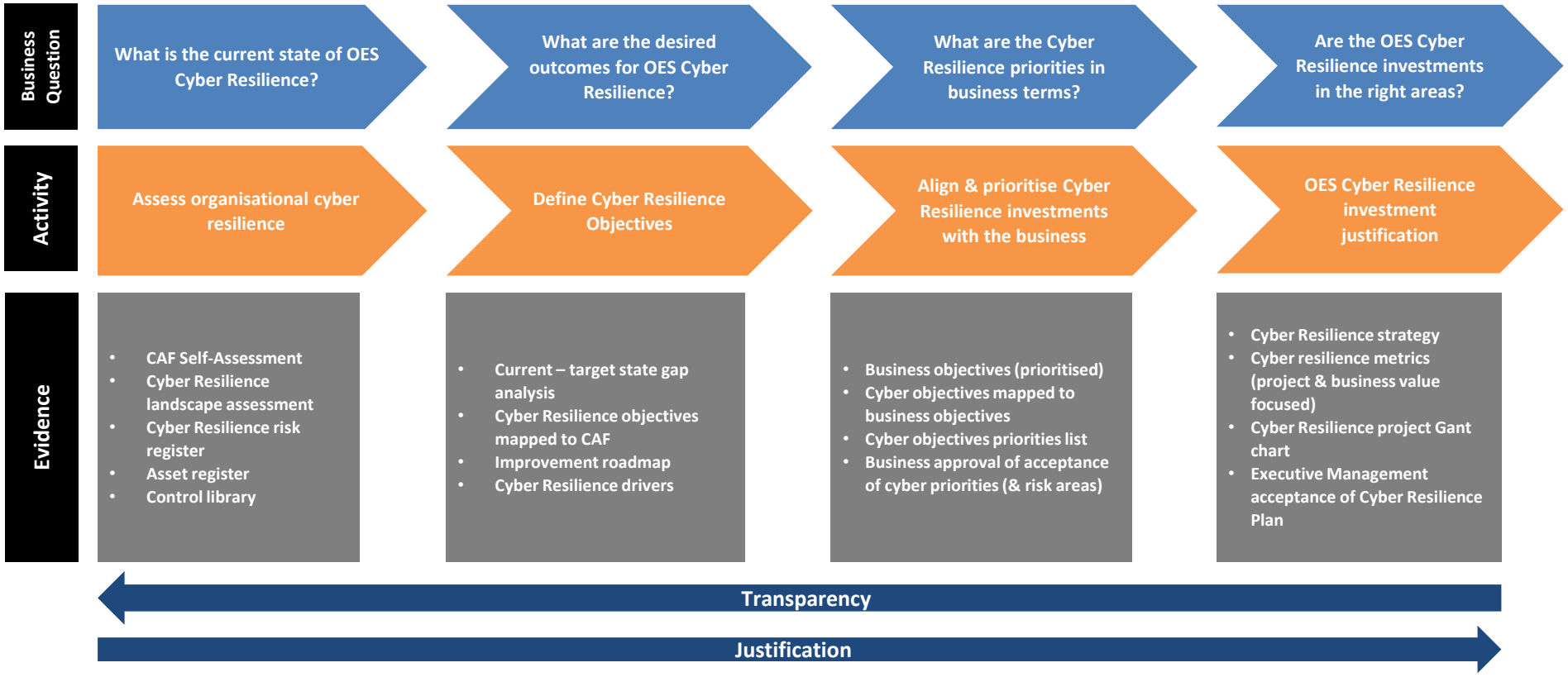
- Allocating work between own team and consultants
- Assessing Cyber submission to ensure costs are appropriate, proportionate, and justified.
- Review OT plans and ensure no IT costs are included
- Procuring third party consultancy support in their assessment
- Engage with companies (9 workshops planned)

The RIIO team is responsible for:

- Ensuring Cyber team understand RIIO-2 and principles
- Ensuring Cyber team are considering RIIO-2 principles (evidence based justifications, CBA, etc) when assessing business plans
- Ensuring alignment between Cyber team assessment and RIIO-2 timelines
- Licence drafting
- Facilitating decision making with senior leadership

ofgem Making a positive difference for energy consumers

We have developed a methodology to analyse the submissions



What does cyber investment look like
Example – MADE UP VALUES

	RIIO2 Cyber Resilience Request	RIIO3 Cyber Resilience Request
IT	£7m	£6m
OT	£169m	£94m
Total	**Approx. £176m**	**Approx. £100m**

Example of IT Outputs

- Anti-malware
- Multi-factor authentication
- Secure file transfer
- Back up and recover

Example of OT Outputs

- Replacement of digital Protection & Control devices/systems and substations
- Retrofitting existing assets

Engagement Plan and Next Steps (indicative timings)

Sprint	Date	Action	Owner
Sprint 1 Delivery	Oct – Dec 2021	Continued engagement with companies to discuss plans, as Challenge Groups do not see Cyber and IT plans	Cyber team RIIO team
	April 2022	Complete and engage in licence drafting working groups	RIIO team
	Dec 2021	Assess December Business Plans	Cyber team RIIO team
Sprint 2 Delivery	Jan 2022	Identify 'easy win' decisions and receive early steer on difficult areas Identify issues for Open Hearings	Cyber team RIIO team SLT
Sprint 3 Delivery	Apr 2022	Recommended decisions to COA Continued drafting	Cyber team RIIO team SLT
Sprint 4 Delivery	May 2022	RIIO GEMA Board Meeting	SLT

ofgem Making a positive difference for energy consumers

Our core purpose is to ensure that all consumers can get good value and service from the energy market. In support of this we favour market solutions where practical, incentive regulation for monopolies and an approach that seeks to enable innovation and beneficial change whilst protecting consumers.

We will ensure that Ofgem will operate as an efficient organisation, driven by skilled and empowered staff, that will act quickly, predictably and effectively in the consumer interest, based on independent and transparent insight into consumers' experiences and the operation of energy systems and markets.

www.ofgem.gov.uk