APPENDIX 4: **IMPLEMENTING A CYBERSECURITY REGULATION** THE OFGEM APPROACH

Appendix to **Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators**

Project Title:	Europe and Eurasia Cybersecurity Partnership
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Cooperative Agreement #:	AID – OAA-A-16-00049
Recipient:	National Association of Regulatory Utility Commissioners (NARUC)
Date of Publication:	May 2020

Author: CNR-IRCrES, The National Research Council of Italy, Research Institute on Sustainable Economic Growth[1]

[1] The present document has been prepared by Daniele Benintendi and Alberto Stefanini, under the supervision of Elena Ragazzi.

This appendix presents a case study of the real approach adopted by a European Regulator to tackle the problem of the cybersecurity stance of the power system.

EU countries (and the individual states in the U.S.) have adopted different regulatory strategies; some of them are still in an early phase of initial prospection on the problem. In that context, the Ofgem (UK) experience is a very interesting example, because its process to establish a comprehensive regulatory approach for cybersecurity is at a very advanced state. The Office of Gas and Electricity Markets (Ofgem), supporting the Gas and Electricity Markets Authority (GEMA), is the government regulator for the electricity and downstream natural gas markets in Great Britain. We will review here some recent updates concerning cybersecurity. As Ofgem is still working on the legislation for the next regulatory period (called RIIO-2[2] starting in 2021 for all the sectors except Electricity Distribution which will start in 2023), our analysis covers the main principles used and the process of consultation with the stakeholders.

As stated in the conclusion of the guidelines, several tools and approaches may be adopted while designing a cybersecurity regulation, but it must be clear that no turnkey solutions are available. The guidelines suggest that the contents and features of the regulation should be defined not through a one-step decision, but through a process, including for each step the collection of information, the consultation of relevant stakeholders, and time for internal reflection. For this reason, we deem it interesting to show an example of this process, even though it is not yet concluded.

[2] RIIO-2 is the next price control for network companies running the gas and electricity transmission and distribution networks. RIIO (Revenue=Incentives+Innovation+Outputs) is designed to encourage network companies to:

- Put stakeholders at the heart of their decision-making process.
- Invest efficiently to ensure continued safe and reliable services.
- Innovate to reduce network costs for current and future consumers.
- Play a full role in delivering a low carbon economy and wider environmental objectives.

1 Principles behind the Ofgem regulatory approach

Ofgem's concern starts with the objective to provide consumers with a safe, reliable, and affordable supply of energy. It also defines the current situation as a phase of transition towards a system that will use cleaner energy sources.

> *The energy networks sit at the heart of our energy system and the RIIO-2 price controls will have a critical enabling role. Within the context of Ofgem's wider integrated strategy for network regulation, RIIO-2 will need to be sufficiently flexible and agile to respond to a range of exciting future possibilities. This approach will ensure that networks can connect and manage the low carbon technologies required to meet climate change targets, maintain high levels of reliability, at the same time as ensuring that network capacity is not increased unnecessarily or at high cost.*[3]

This will imply investments in new, more flexible, solutions, better use of data and innovative contracting schemes between demand and generation. In the long term, a higher degree of interoperability between transmission and distribution to further lower the system costs and better integrate RES generation is envisioned.

The Ofgem approach is to have an output-based incentive framework with rewards and penalties, with the aim to have an innovative system that will reduce the costs of investing in the networks. Moreover, there are special schemes to promote innovation for large demonstration projects and smaller-scale initiatives.

The overall objective is to develop a regulatory strategy that considers the system as a whole, introducing mechanisms that facilitate the coordination of expenditures between networks to support a more decentralized energy system. Great importance is given to the opinion of consumers in setting outputs and shaping and assessing business plans of network operators; these are encouraged to define the objectives with their clients to jointly define the business strategy.

For this new regulatory period, Ofgem defines three output categories and three output types. The output categories are:

- Meet the needs of consumers and network users
- Maintain a safe and resilient network
- Deliver an environmentally sustainable network

The output categories are quite standard as they follow the current EC priorities. The output types are instead specific of the UK system:

- *License Obligations.* They set minimum standards to be achieved with the baseline funding. No further coverage is foreseen. If these are not met, there is a clear system of penalties or enforced actions. During the regulatory period, Ofgem can revise the standards.
- *Price Control Deliverables* (PCDs) are specific deliverables with funding attached.
- Service level improvements incentivized through *Output Delivery Incentives* (ODIs). They set dynamic incentives for network operators to improve the quality of service.

[3] (Ofgem RIIO Team, 2019, p. 5) – Clause 1.11

PCDs are used where the output is funded through the price control and cannot be transferred to a different one. The conditions of PCDs are defined clearly upfront, examples are large one-off capital projects with specific budget and timing conditions or a commitment to connect a certain quantity of MW. This instrument can be used to accommodate a change of policy by the government or other special events that occur during the regulatory period. Ofgem recognizes the concern that pre-defined conditions could limit the ability of operators to innovate, and will take adequate measures in the definition of terms to avoid this risk.

Network operators are expected to identify potential PCDs as part of their business plans. They also must identify the possible use of uncertainty mechanisms (these are also called reopeners, and indicate the possibility to re-discuss the terms of the engagements) and assess the consequences for the consumers of any delay or failure to deliver.

ODIs are connected to improvements in the quality of service that come for activities not included in license obligations. For a specific activity, it is calculated ex-ante how to share the benefits of an improved performance between operators and consumers. ODIs will have upper and lower limits, because companies could have financial issues in case of a bad performance and because after a certain level further improvements are not marginally productive.

Ofgem suggests the possibility of bespoke ODIs that can be proposed by operators also using the feedback from their customers. The concern has been raised that bespoke measures could reduce the level of cooperation between operators, as they would face different conditions.

2 Terms of reference of the decision process on cybersecurity regulation

The EU directive on security of network and information systems (2016/1148) (NIS Directive) was transposed into UK law as the "Network and Information Systems Regulations 2018" (NIS Regulations) and came into force on May 10, 2018 for the water, health, transportation, digital, and energy sectors.

The NIS Regulations impose new duties on Operators of Essential Services (OES) and give relevant Competent Authorities (CAs) new powers and responsibilities to ensure OES are meeting those duties. Ofgem has been designated in the NIS Regulations as a joint CA with the Department for Business, Energy, and Industrial Strategy (BEIS), for the downstream gas and electricity sectors in Great Britain.[4]

OES are those gas and electricity operators which are **determined by thresholds defined in the NIS regulations** and **those determined by BEIS.** Under the NIS regulations, network companies must take appropriate and proportionate technical and organizational cybersecurity measures to manage risks posed to the security of the network and information systems on which their essential service depends and to prevent and minimize the impact of incidents on these essential services.

In 2017, the UK National Cyber Security Centre[5] developed a sector-agnostic Cyber Assessment Framework (CAF) to assist operators covered by the NIS regulations to perform self-assessments.[6] The process for this self-assessment is described in section four.

Table 1: The 14 NCSC cloud security principles[7]

1. Data in transit protection
User data that is transitioning between networks should be protected against any interference.
2. Asset protection and resilience
User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
3. Separation between users
If a user of a service is compromised by malicious software, this should not affect the service or data of another user.
4. Governance framework
A security governance framework should be followed by the service provider in order to internally coordinate its management of the service.

[4] (Ofgem, 2018, p. 1)

[5] The National Cyber Security Centre (NCSC) is the UK independent Authority established by the United Kingdom Government to provide advice and support for the public and private sector in how to face computer security threats. Based in London, it became operational in October 2016.

[6] (Ofgem RIIO Team, 2019, p. 42) – Clause 6.97.

[7] https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

5. Operational security
In order to prevent and detect attacks, the service must be operated securely. Adequate security shouldn't require complex or expensive processes.
6. Personnel security
Service provider personnel should be thoroughly screened, followed by in-depth training to reduce the likelihood of accidental or malicious compromise.
7. Secure development
Services should be designed with security in mind.
8. Supply chain security
Service providers should ensure that their supply chain adheres to the same security principles.
9. Secure user management
Service providers should ensure that end-users have the relevant tools to securely manage the use of their services. Management interfaces must prevent unauthorized access to data, making them a vital part of the security barrier.
10. Identity and authentication
Access to the service interfaces should only be granted to specific individuals and should all be guarded by adequate authentication measures – two-party authentication if possible.
11. External interface protection
Any external or less trustworthy service interfaces must be identified and defended appropriately.
12. Secure service administration
If a cloud service is compromised through its administration system, important company data could be stolen or manipulated. It is vital that these services are secure.
13. Audit information for users
A service provider should supply their customers with the audit recorded needed to monitor the service and who is able to access your data. This is vital, as it gives you the means to identify inappropriate or malicious activity.
14. Secure use of service
Service providers have the responsibility to ensure the service is used properly, to ensure their data is kept safe and protected.

3 The process

3.1 The first step: consultation of the stakeholders

Ofgem recognized that network companies are increasingly dependent on business IT systems and operational technology, which will only increase as networks become smarter, more automated, and more digitized. Network companies must ensure these systems are protected and can withstand an ever-evolving cyber-risk landscape. In December 2018, Ofgem launched a consultation asking the OES to comment on a proposal of regulation to deal with the cost associated with this protection.
Ofgem proposed to consider cyber resilience costs, which are:

(1) efficiently incurred as a direct result of the introduction of the Network and Information Systems (NIS) Regulations 2018, and
(2) above 'business-as-usual' activities[8]

Ofgem also proposed an exemplary list of the systems under inquiry:

Table 2: Ofgem's proposed list of systems under inquiry[9].

Examples of critical network and information systems
• Distributed control system
• Supervisory control and data acquisition systems
• Gas turbine control system
• Steam turbine control system
• Water treatment plant system
• Cooling water makeup system
• Common services (auxiliary) system
• Coal plant system
• Generator protection systems
• Fire safety systems
• Emergency shutdown systems
• Switching system
• Engineering systems
• Communication systems
• Plant information systems
• Remote terminal units
• Programmable logic controllers
• Plant-based heating ventilation and air conditioning
• IT Systems deemed critical by the business for the delivery of essential services
• Trading systems

To respond to the consultation, network companies in all sectors (including electricity distribution and the Electricity System Operator, or the British TSO) develop and submit strategic investment plans for cyber resilience setting out the steps they proposed to take during the RIIO-2 period and beyond to comply with the NIS Regulations.[10] OFGEM expected that costs associated with these strategic investment plans would form part of the RIIO-2 Business Plan submissions, and suggested that deviation from the

[8] (Ofgem RIIO Team, 2019, p. 40) – Clause 6.79
[9] This is not an exhaustive list but indicates some of the systems an OES may deem critical for the provision of the essential service they provide (OFGEM, 2018, p. 11).
[10] (Ofgem RIIO Team, 2019, p. 40) – Clause 6.80

plans without Ofgem's approval may result in a 'clawback' of the associated funding.[11] OFGEM also indicated that in their role as joint Competent Authority (CA), they expected to publish detailed guidance to inform the development of these strategic plans by June 2019.[12]
Ofgem recognized that cybersecurity is an evolving area, and operators may require further guidance and time to clarify their needs and appreciated that some operators could not be ready to submit their cyber resilience plans by December 2019.[13] Some operators took the opportunity to informally share draft proposals with the competent authority, ahead of the December submission, to enlist guidance and direction with the development of these plans.

3.2 December 2018 consultation outcome

Ofgem received 17 responses to the consultations, including the ones from the 12 network operators, two suppliers, citizens advice,[14] and the RIIO-2 challenge group.[15] A number of respondents agreed with the Ofgem proposal for the scope of costs, i.e. those efficiently incurred as a direct result of the introduction of the NIS regulations, and above 'business-as-usual' (BAU) activities. However, some respondents highlighted the difficulty in separating 'BAU' activities from 'above BAU' activities given the rapidly changing landscape and called for greater clarity on how this is being defined. Others suggested that all cyber costs should be treated the same. Some respondents also suggested that business plans should identify initiatives to deal with known risks/threats, with an uncertainty mechanism used to deal with the unknown.[16] Moreover, some respondents noted that cyber investment goes beyond the NIS regulations, which only cover operational systems rather than business systems, and the scope should be widened to include all such costs.[17] One respondent suggested differentiating between NIS costs and BAU costs, rather than above BAU costs, while another suggested that cyber resilience costs should not be treated separately as they are an integral part of the business plan. One respondent suggested that only costs above BAU should be funded under this category. Finally, the majority of respondents supported the use of a **re-opener mechanism** to deal with *uncertainty around requirements, unknown and emerging risks/threats, new regulatory requirements, and technology changes. Some suggested this should operate mid-term, two to three years into the control, and others suggested a low or zero - materiality threshold. One respondent proposed a logging-up mechanism to deal with costs resulting from new requirements that emerge during RIIO-2.*[18]

[11] (Ofgem RIIO Team, 2019, pp. 40-41) – Clause 6.84
[12] (Ofgem RIIO Team, 2019, p. 40) – Clause 6.81. The Consultation outcome is fully documented by (Ofgem, 2019).
[13] (Ofgem RIIO Team, 2019, p. 42) – Clause 6.101. A reopener mechanism will be available to deal with this possibility, see section 3 hereinafter.
[14] Citizens Advice is a network of 316 independent charities throughout the United Kingdom that give free, confidential information and advice to assist people with money, legal, consumer and other problems.
[15] (Ofgem RIIO Team, 2019, p. 41) – Clause 6.85. Ofgem have established RIIO-2 Challenge Group for all RIIO-2 price controls to strengthen the voice of consumers in the process of setting price controls for energy network companies (Ofgem, 2019).
[16] (Ofgem RIIO Team, 2019, p. 41) – Clause 6.87
[17] (Ofgem RIIO Team, 2019, p. 41) – Clause 6.87
[18] (Ofgem RIIO Team, 2019, p. 41) – Clause 6.85 and 6.86

3.3 Ofgem conclusion: separate the normal business plan and cyber resilience

In the end, Ofgem decided to separate the normal business plan from cyber resilience measures. These are given a separate allowance that could be re-discussed (re-opener mechanism) and adapted if circumstances might change due to the continuously evolving cyber risk landscape.[19]

In the consultation process, most operators preferred a unique scheme for IT security included in the general regulation or specific projects with well-defined outputs. The decision of Ofgem for this regulatory period is more prudent; this period seems to be considered as an opportunity to gather more information as there is not enough evidence/knowledge to commit to something specific. Companies apparently do not seem to favor having the Regulator doing micro-management of their projects, and for this reason, prefer to be monitored on outputs and not process. The ex-ante allowances will be based on the presentation of the plans for cybersecurity. The plans should be integrated into the overall business plan of the company and document well the options chosen.

The decisions

- Network companies should develop and submit business IT security plans as part of their RIIO-21 business plans. Funding for IT will be provided as part of normal regulatory allowances.
- Network companies should develop and submit cyber resilience plans. A separate 'use-it-or-lose it' allowance which will be provided to increase cyber resilience of operational technology requirements is considered appropriate, proportionate, and efficient, together with a re-opener mechanism to deal with uncertainty.

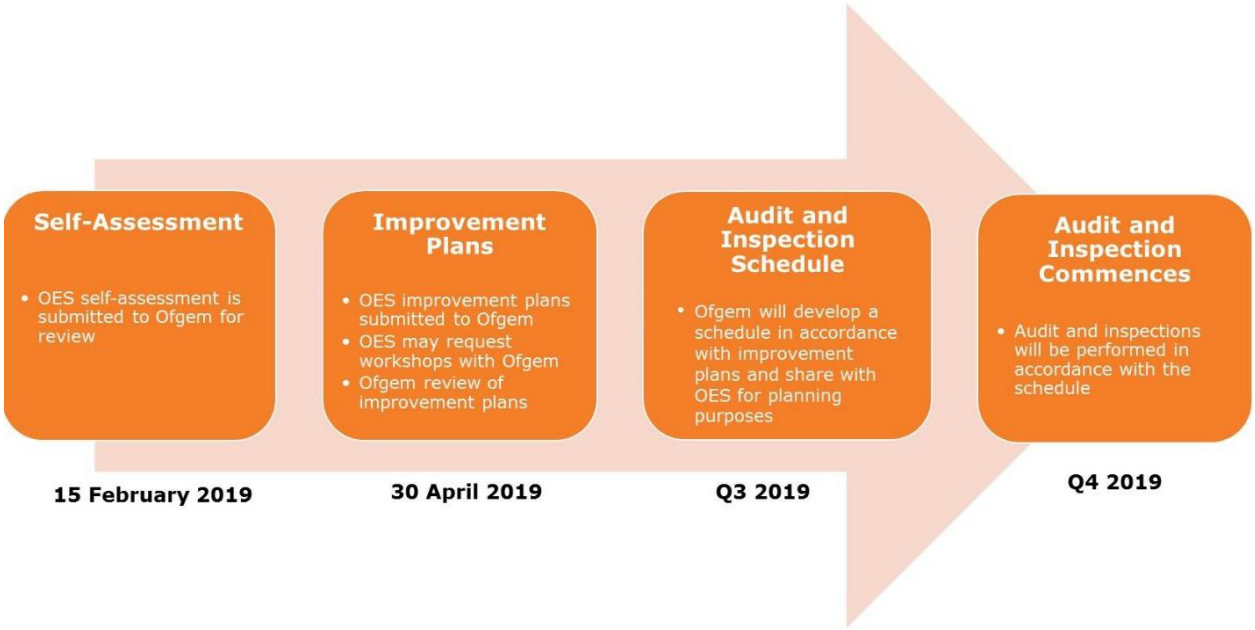
Operators should follow a robust risk-based approach to assess the investments. Current risks, vulnerabilities, threats, and mitigation options are expected to be documented, together with the relative benefits of the options considered.

[19] (Ofgem RIIO Team, 2019, p. 40): 'Network companies should develop and submit cyber resilience plans. A separate 'use-it-or-lose it' allowance which will be provided to increase cyber resilience of operational technology requirements considered appropriate, proportionate, and efficient, together with a re-opener mechanism to deal with uncertainty.'

4 2019 OES self-assessment

The NIS Regulations ask, among other duties, to Operators of Essential Services (OES) to run a self-assessment. The National Cyber Security Center developed a sector-agnostic Cyber Assessment Framework (CAF); its application came into force in early 2019 and was completed within the year, as depicted in Figure 1.

Figure 1 - Schedule of OES self-assessment cycle



Source: (OFGEM, 2018, p. 7)

Self-assessments to Ofgem comprises of two Parts:[20]

- **The OES Self-Assessment Report**: this provides a high-level overview of the complete self-assessment, any significant risks identified, and any initial proposals for risk treatment.
- The **NCSC CAF spreadsheet** with **supporting evidence to validate the self-assessment.** Evidence is required for areas identified as 'not achieved' or 'partially achieved'. A high-level justification should, however, be provided within the CAF self-assessment spreadsheet as to why an item is deemed to be 'achieved'. There may be instances where an OES may be mostly 'achieved' and only parts of the OES are 'not achieved' or 'partially achieved'.

Following the process for submission of part one and part two submissions set out above, the OES have to develop their improvement plans. Improvement plans will build upon the OES's self-assessments, identifying risks in accordance with their own risk management and risk methodology. The improvement plans will set out the cyber-security countermeasures the OES intend to take where the risk is above their own risk tolerance levels. Improvement plans may cover both short-term measures or longer-term strategic measures, for which budget needs are to be sought through business planning.[21] Ofgem may,

[20] (Ofgem, 2018, p. 8)
[21] (Ofgem, 2018, p. 9)

where it is deemed to be required, review the improvement plans with the OES in order to assist them with prioritization and risk mitigation planning.[22]

[22] (Ofgem, 2018, pp. 13-14, 20)

References

Ofgem. (2018, Nov. 30). *Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain.* Retrieved from https://www.ofgem.gov.uk/ofgem-publications/144069: https://www.ofgem.gov.uk/system/files/docs/2018/11/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf

Ofgem. (2018, November 30). *Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain.* Tratto da Ofgem_CA-Guidance: https://www.ofgem.gov.uk/system/files/docs/2018/11/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf

Ofgem. (2019, Nov. 19). *RII0-2 Challenge Group* . Retrieved from https://www.ofgem.gov.uk/system/files/docs/2018/11/riio-2_challenge_group_terms_of_reference.pdf

Ofgem. (2019, September 13). *RIIO-2 Cyber Guidelines Draft Consultation.* Tratto da Ofgem: https://www.ofgem.gov.uk/publications-and-updates/riio-2-cyber-guidelines-draft-consultation

Ofgem RIIO Team. (2019, May 24). *Decision - RIIO-2 Sector Specific Methodology – Core document.* Retrieved from RIIO-2 Sector Specific Methodology Decision: https://www.ofgem.gov.uk/system/files/docs/2019/05/riio-2_sector_specific_methodology_decision_-_core_30.5.19.pdf