ofgem
Making a positive difference
for energy consumers

Consultation

Cyber Resilience Operational and Information Technology Plan Assessment Methodologies Annex - NON-CONFIDENTIAL

Publication date	09 July 2020	**Contact:**	RIIO Team
		Team:	Network Price Controls
Response deadline	4 September 2020	**Tel:**	020 7901 7000
		Email:	RIIO2Cyber@ofgem.gov.uk

We are consulting on our Draft Determinations for the RIIO-2 price control. Once the consultation is closed, we will consider all responses. We want to be transparent in our consultations. For cyber resilience OT and IT consultation responses, we expect responses to be confidential, as our company specific draft determinations set out issues relating to national security. If you want your response considered non-confidential – in whole or in part – please tell us in your response and explain why. Please clearly mark the parts of your response that you consider to be non-confidential, and if possible, put the non-confidential material in appendices separate from to your response. We will publish the non-confidential responses we receive alongside a decision on next steps on our website at Ofgem.gov.uk/consultations.

Please provide your consultation responses securely. Our preferred method is through Egress Switch. However, please contact us if you wish to use an alternative secure method.

If your response is confidential, please provide your consultation responses securely. Our preferred method is through Egress Switch. However, please contact us if you wish to use an alternative secure method.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at www.ofgem.gov.uk. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

Purpose of this document

1.1 This document sets out our assessment methodologies for Cyber Resilience Operational Technology (OT)[1] and Information Technology (IT)[2] Plans for the RIIO-2 price control. This price control will cover the five-year period from 1 April 2021 to 31 March 2026.

1.2 This document is intended to be read alongside the RIIO-2 Draft Determinations Core Document (Core Document), and the licensees' company specific RIIO-2 Draft Determinations for Cyber Resilience OT and IT, where applicable. A confidential version of this document was sent directly to network companies.

1.3 Please note that we no longer refer to 'Cyber Resilience' and 'Business IT Security', as we did in the RIIO-2 Sector Specific Methodology Decision (SSMD). We have decided to change our reference to provide clarity for non-expert readers. We now refer to these two terms as 'Cyber Resilience Operational Technology (OT)' and 'Cyber Resilience Information Technology (IT)'.

Introduction

1.4 We have assessed the Cyber Resilience OT and IT Plans that were submitted as part of the Business Plans for the RIIO-2 price control. Our methodologies for assessing each type of Plan are based on the guidance provided in the Business Plan Guidance document,[3] and our RIIO-2 Cyber Resilience Guidelines.[4]

1.5 Our assessment methodology for Cyber Resilience OT Plans covers three broad components. These are: business alignment, needs case, and costs. In carrying out our assessment, we considered interactions between the three components.

1.6 Our assessment methodology for Cyber Resilience IT Plans is different from, but similar to, our assessment methodology for Cyber Resilience OT Plans. The reason for the difference is that we consider that requirements for the cyber resilience IT area are relatively mature. This allows us to review historical costs because

[1] Operational Technology are network and information systems that are deemed necessary to the delivery of essential services, for example Supervisory Control and Data Acquisition Systems (SCADA).
[2] Information Technology are network and information systems that are used within business functions, for example word processing.
[3] https://www.ofgem.gov.uk/publications-and-updates/riio-2-business-plans-guidance-document
[4] https://www.ofgem.gov.uk/publications-and-updates/riio-2-cyber-resilience-guidelines

licensees should have already be investing in capabilities to mitigate IT cyber security risks as a business as usual activity.

1.7 In carrying out our assessment of both Cyber Resilience OT and IT Plans, we also considered interactions and interdependencies between these two domains.

Assessment methodology for Cyber Resilience OT Plans

1.8 As referred to above, our assessment methodology for Cyber Resilience OT Plans covers three broad components: business alignment, needs case, and costs.

Business Alignment

1.9 We considered two key aspects in relation to business alignment when assessing a network company's Cyber Resilience OT Plan. We assessed whether the Cyber Resilience OT Plan:

a) serves a clear purpose in supporting the organisation to achieve the overall business objectives set out in its Business Plan; and,
b) aligns with any cyber resilience projects that the network company is currently undertaking.

1.10 In regards to the first aspect, we assessed whether the proposed activities in the Cyber Resilience OT Plan supported the wider business objectives the Business Plan proposals (e.g. maintaining a safe and resilient network). We also assessed whether it clearly articulated linkage of key cyber risks to wider business risks, including how, and to what extent, its cyber resilience activities in its Cyber Resilience OT Plan will reduce risk to the business.

1.11 In regards to the second aspect, we assessed whether the Cyber Resilience OT Plan aligned with any projects included in the RIIO-1 cyber re-opener determination, or pre-existing cyber resilience programmes. We also assessed whether the plans reflect the risks the company has identified from its past cyber resilience activities.

Needs Case Assessment

1.12 We assessed two key aspects in relation to the needs case when assessing a network company's Cyber Resilience OT Plan. We assessed whether:

a) the overall business needs case is justified; and,

b) specific needs case of proposed projects is justified.

1.13 In regards to the first aspect, we considered whether the network company demonstrated the overall business need for cyber OT improvement on its network, in terms of its current risk position, when compared to the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) outcomes[5] and to its own acceptable business risk tolerances.

1.14 In regards to the second aspect, we considered whether the network company provided robust justification around its project specific needs case. Justification includes (but is not limited to):

- how the need for the specific project was identified through a methodical process;
- what the alternative project/options were, and how these were considered;
- how the proposed project/site was prioritised;
- why the project/option/site was selected;
- how the proposed project will protect the network company from specific cyber threats; and,
- how the proposed project represents value for money and is a proportionate solution.

1.15 Where possible, we assessed whether proposed specific projects were mapped, and whether its associated costs were allocated appropriately and proportionally to achieve improvements in CAF outcomes and risk reduction.

1.16 We also considered what safeguards and approach the company put in place to measure implementation, progress, risk reduction, and benefits of its proposed cyber resilience OT projects. This included considerations of whether resources are justified and adequate to ensure deliverability of proposed activities.

Cost Assessment

1.17 We undertook an assessment to understand the associated costs of the proposed projects set out in baseline and uncertainty categories of the Cyber Resilience OT Plan, as well as how these types of spend are represented by capital expenditure

[5] NCSC CAF outcomes are 14 cyber security and resilience principles. It specifies what operators of essential services (i.e. network companies) must achieve. More information can be found here: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

(capex) and operational expenditure (opex). The requested allowance amounts were cross-checked to ensure that Business Plans, Cyber Resilience OT Plans and supporting documentation such as Business Plan Data Tables (BPDT), Engineering Justification Papers (EJP), Cost Benefit Analysis (CBA), and any supplementary question responses were consistent, and provided justification for the project costs.

1.18 We assessed the methodology used by the network company to determine the project costs, and have proposed adjustments in its RIIO-2 Draft Determinations – Cyber Resilience Operational Technology (OT) document, where we disagreed with the approach, assumptions used, or found errors.

1.19 We assessed the trade-offs considered by the network company, between the costs of projects available, and the level of detail included in the cost breakdown of projects. The purpose of this task was to better understand the different the projects, cost options, the level of granularity considered, and what cost-benefit assessment was undertaken when selecting its proposed projects.

1.20 We considered proportionality when assessing requested project costs and the anticipated benefits (ie level of risk reduction) the project is expected to deliver. For example, projects with significant costs should deliver high levels of risk reduction. Where this is not the case, we considered any relevant justifications to reach our view on whether allowances should be provided.

Assessment methodology for Cyber Resilience IT Plans

1.21 As with cyber resilience OT, our assessment methodology for Cyber Resilience IT Plans covers three broad components: business alignment, needs case, and costs. In assessing these components, we considered many of the factors set out above in relation to our assessment methodology for Cyber Resilience OT Plans.

1.22 However, unlike for cyber resilience OT, our assessment of business alignment and needs case was combined because of the relative maturity of cyber resilience IT requirements.

1.23 As part of our assessment of Cyber Resilience IT Plans, we also considered and compared requested allowance with historic 'Run The Business'[6] costs.

[6] Run the Business costs are the day-to-day costs associated with operating a business.

Determining proposed allowance

Cyber Resilience OT

1.24 In coming to our proposed funding allowance for each licensee for cyber resilience OT projects, we have also considered:

- the nature of cyber resilience OT as a new policy area for licensees;
- the need for continued investment to support achieving CAF outcomes and managing risk;
- the risks and consequences of potential cyber resilience OT incidents on existing and future energy consumers; and,
- the limited reporting and cost benchmarking information available.

1.25 We consider it appropriate to provide an allowance for cyber resilience OT activities to a licensee where it has demonstrated the overall business need for cyber resilience OT improvement on its network, in terms of its current risk position, when compared to the CAF outcomes, and to its own acceptable business risk tolerances.

1.26 Where a company has justified both the overall business need and specific needs case for its proposed projects, we propose to provide allowances for these projects. Where we disagreed with elements of a proposed project (eg cost proposals or deliverability), we have proposed adjustments to outputs and allowances to reflect our rationale.

1.27 We consider that there is a need for network companies to continue to invest, develop, and undertake activities to manage measured risk, cyber maturity and CAF outcomes, and align its organisation with the Security of Network & Information Systems Regulations (NIS) Regulations 2018[7] requirements at the start of RIIO-2.

1.28 Where a network company has demonstrated the overall business need, but has not justified the specific needs cases for its proposed projects, we propose to provide an allowance amount, less than the amount the network company requested. We consider that our proposals provide an appropriate way for network

[7] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

companies to seek, and to ensure timely investment and implementation of cyber resilience OT projects in view of the considerations set out in paragraph 1.24.

1.29 Due to the relatively new nature of cyber resilience OT as a policy area, and the uncertainty around scope and cost of cyber resilience OT enhancements, we decided in the RIIO-2 Sector Specific Methodology Decision (SSMD),[8] that cyber resilience OT allowances would be provided on a 'use-it-or-lose it' basis.

1.30 In the Core Document, we set out how we propose to consider whether use-it-or-lose it allowances are used appropriately, proportionally, and efficiently.

1.31 Cyber resilience OT allowances are also subject to ongoing monitoring as part of outcome based Price Control Deliverables (PCDs).[9] In the Core Document, we set out our proposal to require the delivery of outputs such as: CAF outcome improvement; risk reduction; and cyber maturity improvement. We would welcome views on this proposal in the Core Document.

1.32 We are also proposing two re-opener windows for network companies to request adjustments to their outputs, delivery dates, and associated allowances.

1.33 We propose to require that all companies submit new Cyber Resilience OT plans during the first re-opener window at the start of RIIO-2.

1.34 Where a company did not submit a Cyber Resilience OT Plan as part of its Business Plan in December 2019, we do not propose to provide any allowance.

Cyber Resilience IT

1.35 We consider it appropriate to provide an allowance for cyber resilience IT outputs to a licensee where it has demonstrated the overall business need for cyber resilience IT improvement on its network, in terms of its current risk position, and when compared to its own acceptable risk tolerances.

1.36 Where a company has justified both the overall business need and specific needs cases for its proposed projects, we propose to provide allowances for these projects. Where we disagreed with elements of a proposed project (eg cost

[8] Paragraph 6.108 in the RIIO-2 Sector Specific Methodology Decision (SSMD)- https://www.ofgem.gov.uk/system/files/docs/2019/05/riio-2_sector_specific_methodology_decision_-_core_30.5.19.pdf

[9] SSMD Core document paragraph 6.108 https://www.ofgem.gov.uk/publications-and-updates/riio-2-sector-specific-methodology-decision

proposals or deliverability), we have proposed adjustments to outputs and allowances to reflect our rationale.

1.37 Where a network company has demonstrated the overall business need, but has not justified the specific needs case for its proposed projects, we propose to provide the company an allowance based on RTB costs, determined using historical costs, provided by the company. This is intended to enable the company to continue to invest, develop, and undertake activities to demonstrate a reduction in measured risk on its network and information services, and milestone achievements.

1.38 In the SSMD,[10] we decided that for cyber resilience IT, baseline allowances will be provided subject to the Totex Incentive Mechanism. We consider that requirements for cyber resilience IT are relatively mature. Licensees should already be investing in capabilities to mitigate IT cyber security risks as a business as usual activity.

1.39 Cyber resilience IT allowances are also subject to ongoing monitoring as part of outcome based PCDs. In the Core Document, we set out our proposal to require the delivery of outputs such as: CAF outcome improvement; risk reduction; and cyber maturity improvement. We would welcome views on this proposal in the Core Document.

1.40 We are proposing two re-opener windows for companies to request adjustments to their outputs, delivery dates, and associated allowances.

1.41 We are also proposing to require that all companies submit new Cyber Resilience IT Olans during the first re-opener window at the start of RIIO-2.

Conclusion

1.42 In conclusion, we have adopted this assessment methodology when reviewing the network companies RIIO-2 Cyber Resilience OT and IT Plans to ensure that they represent value for money for the consumer.

[10] Paragraph 6.107 in the RIIO-2 Sector Specific Methodology Decision (SSMD)- https://www.ofgem.gov.uk/system/files/docs/2019/05/riio-2_sector_specific_methodology_decision_-_core_30.5.19.pdf