RIIO-2 Cyber Resilience Plan and Re-opener Application Requirements: Version 0.1

Subject	Details
Publication date	29 June 2022 **Contact:** Cyber Security Team **Directorate:** Enforcement & Emerging Issues **Email:** RIIO2cyber@ofgem.gov.uk

This document is directed at gas and electricity transmission and distribution network companies (for the purposes of this document 'licensees').

The purpose of this document is to:

- Set out how the licensees must prepare their Cyber Resilience Plan for OT, IT and for any re-opener applications.
- Provide some guidance on the style and structure for Cyber Resilience Plans for OT, IT and for any re-opener applications.

Contents

1. Introduction

1.1 This document sets out our requirements for the Cyber Resilience OT Plan (OT Plan) and Cyber Resilience IT Plan (IT Plan) that must be submitted prior[1] to the start of the RIIO Price Control, and during a re-opener application window.

1.2 Re-openers are a type of RIIO uncertainty mechanism. Depending on their design, they allow Ofgem to adjust a licensee's allowances (in some cases up and in some cases down), outputs and delivery dates in response to changing circumstances during the price control period. Ofgem can do this by direction rather than by a statutory consultation. Re-openers may be cross sector, sector specific or bespoke to an individual licensee.

1.3 The Cyber Resilience OT and IT Licence conditions require that licensees prepare their Cyber Resilience Plans and re-opener applications in accordance with this Guidance. This is in addition to the specific re-opener requirements set out in the individual licence conditions.

1.4 This document sets out how the licensee must prepare its OT Plan, IT Plan and re-opener application for OT and IT cyber security resilience including:

- the level of detail required in each OT Plan, IT Plan and re-opener application
- requirements to publish each OT Plan, IT Plan and re-opener application
- when it is appropriate to make redactions in each OT Plan, IT Plan and re-opener application
- requirements to ensure senior leadership assurance of the OT Plan, IT Plan and re-opener application.

1.5 This document includes specific requirements for individual Cyber Resilience Plan and re-opener applications for both OT and IT. This document also covers the assessment methodology used when assessing the Cyber Resilience Plans or re-opener applications.

1.6 Licensees must ensure that their OT Plan, IT Plan and re-opener applications comply with this document and any other licence requirements prior to submission. Failure to

[1] These plans are submitted within the timelines for RIIO, normally greater than 12 months prior to the start of the price control period.

prepare an application in accordance with any of the relevant requirements may result in rejection of the application.

2. Cyber Resilience Plan and Re-opener Application Requirements

2.1 This section sets out the information that a licensee must provide when submitting its OT Plan and IT Plan or re-opener application (Submission[2]).

2.2 If a licensee considers it is not able to provide a piece of information set out in this section, it must, in its Submission, provide a reasonable explanation why. The rest of this section is in three parts:

- needs case
- options assessment
- and cost information.

Needs case

2.3 This section sets out the information that must be provided on the needs case for the proposed funding request.

Alignment with overall business strategy and commitments

2.4 Submissions must include details on organisational context, strategy, and business alignment.

2.5 The Submissions must include reference to the following when considering alignment to the business:

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

2.6 Submissions must include, but need not be limited to, a description of:

- the licensee's overall business strategy
- the licensee's cyber resilience strategy

[2] For the purposes of this document, Submission refers to either a Cyber Resilience Plan (IT/OT) or re-opener application.

- how the cyber resilience strategy aligns with its business strategy
- how the Submission aligns with previous/in-flight cyber resilience delivery (i.e. Improvement Plans or RIIO-1 activity)
- internal and external dependencies affecting the proposals set out in the Submission
- the current and targeted security state and/or maturity of the licensee (e.g. National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) self-assessment or similar maturity assessment aligned to NCSC's CAF.).

Demonstration of needs case

2.7 The Submission must include reference to the Network and Information Systems (NIS) Regulations 2018[3] and the measures taken to comply with regulations and associated security frameworks, for example, National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) outcomes.[4]

2.8 Submission must include, but need not be limited to, a description of:

- 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 will protect the network company from specific cyber threats
- relevant cyber risks and why current security and resilience control is insufficient
- the detailed risks posed to the network and consumers including details on threat, vulnerability, and impact
- the risk severity in terms of likelihood and impact for the inherent, residual (current), and target risk positions
- how the proposed project/site was prioritised
- the services, systems, sites and assets that relate to the identified risks
- the licensee's risk tolerability and risk response decisions
- how the licensee calculated the level of cyber risk

[3] https://www.legislation.gov.uk/uksi/2018/506/made
[4] 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

- how the proposed project represents value for money and is a proportionate solution.

Options Selection

2.9 This section sets out the information that must be provided on the options selection process.

Consideration of project options and methodology

2.10 Submissions must include, but need not be limited to, the following:

- the methodology and/or standards used to support security and resilience management and decision making
- the methodology and processes on how cyber risks are assessed, managed, and responded to
- the security and resilience controls required to reduce risks to tolerable levels (and options considered)
- the targeted solutions and projects required to develop and implement the identified security and resilience controls (and options considered).

Preferred option details

2.11 Submissions must set out, but need not be limited to, the following for each project:

- the project scope, including which sites and assets are in scope
- the proposed project/option, including a Cost Benefit Analysis (CBA)[5], general objectives of the project, sites applicability, and prioritisation
- site breakdown per project/work stream targeted for intervention within this Submission
- the security and resilience controls targeted for implementation as part of this project, and cross-referencing to the CAF outcomes or relevant standards
- project outputs, including the specific deliverables of each project (what specific products, solutions and technologies are being targeted for delivery)
- the security and resilience control links to current and targeted security state and/or maturity (e.g. CAF self-assessment).

[5] The CBA must include "do nothing" options

2.12 Submissions must include details of any site requiring funding, including:

- site function and purpose
- site criticality rating and justification
- overview of the technological architecture and assets.

Technical feasibility and consumer benefit

2.13 For Submissions the licensee must set out, but need not be limited to, the following:

- the relevant risks that will be influenced and mitigated through successful delivery of the project
- the inherent and residual (current) risk positions as well as the target risk positions for the end of the RIIO-2 period, based on successful delivery of the project
- a detailed list of project constraints, project risks and dependencies (i.e. dependence on IT Cyber/Business as usual (BAU) projects, alignment with broader site maintenance activities)
- details of any underpinning technical feasibility evidence relating to the project and description of how this reduces the delivery risks of the project. Technical feasibility evidence may include, but need not be limited to, research and development outputs, proof of concepts and demonstrations, and design work.

Project delivery and monitoring

2.14 Submissions must include, using the licensees own project delivery methodology, the following:

- a detailed project plan and timelines (e.g. Gantt chart)
- a detailed project schedule, including activity milestones for project delivery, personnel on-boarding, training, etc.
- the governance structure of each project, including project roles and responsibilities and number of resources required
- the organisational structure of the cyber security team and demonstration of capacity and capability to deliver the plan
- the fundamental components that are being used to measure delivery of the cyber resilience plan (i.e. risk reduction to the business/consumers/ stakeholders)

- a description of how project delivery will be assessed for targeted risk reduction and how assurances will be sought for the effectiveness of delivered security and resilience controls
- a description how project constraints, dependencies, priorities, risks and similar matters will be tracked/managed, for example whether they will be reflected in a prioritised backlog, risk and/or issues log
- a description of how performance will be monitored, including key performance indicators to be used to monitor the progress of the project.

Cost information

2.15 This section sets out the information that must be provided on costs.

Consideration of options

2.16 The licensee must provide information to justify the need and amount of allowance required per project, demonstrating consideration against the targeted risk reduction and site prioritisation.

2.17 The licensee must also provide a description of the various options that were considered (i.e. by performing cost benchmarking, previous tenders or contract information) and the rationale for the selection preferred option.

2.18 The licensee must provide information to demonstrate consideration of the expected lifetime of security and resilience controls in the context of a changing threat landscape.

Breakdown of costs of preferred option

2.19 Submissions must be set out in the accompanying costing templates, covering the following:

- the overall costs of implementing the proposals contained in the Submission
- source information used to build up the costs for each Submission
- a breakdown of the overall baseline costs for the Submission per year
- a breakdown of the capex and opex costs of the overall costs per year
- a breakdown of the capex and opex for the overall costs for each project

- for each project, a breakdown of the costs for each site which is in scope in terms of capex and opex costs and volume and unit costs (wherever applicable).

2.20 Submissions must set out, but need not be limited to, the following:

- the current overall Cyber IT/OT running costs as well a breakdown of the current Cyber IT/OT running costs for each site
- the future overall Cyber IT/OT running costs as a result of project implementation as well a breakdown of the future Cyber IT/OT running costs for each site
- where an agile delivery methodology is being used:
    - estimated team cadence e.g. who will be included on each project
    - estimated burn down charts
    - scrum team cadence costs and key external stakeholder costs.

Justification and efficiency of costs

2.21 The licensee must provide a description of the sourcing approach, such as procurement or tendering, to be adopted and demonstrate how this process supports cost efficiency.

2.22 For projects at an early stage of development that have not entered their sourcing approach, a Submission must include:

- source information for the baseline costs, supplemented with uncertainty costs based on assessed delivery risk
- source information for the licensee's approach to cost estimation, which may include a qualitative or quantitative explanation of a baseline cost element (e.g. probabilistic P50 value)
- a cost comparison analysis against the market or benchmarking
- a description of how and when cost uncertainty will be reduced as the project proceeds towards initiation and throughout delivery.