ofgem
Making a positive difference
for energy consumers

Guidance

Appendix 1 Cyber Resilience IT and OT Re-Opener Application Guidance

Publication date	09 October 2020	**Contact:**	RIIO Team
		Team:	Network Price Controls
		Tel:	020 7901 7000
		Email:	RIIO2@ofgem.gov.uk

This governance document is directed at gas and electricity network companies and their stakeholders. It provides information to be included in companies' re-opener applications during RIIO-2, and requirements network companies must undertake in relation to its re-opener applications.

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

Cyber Resilience IT and OT re-opener application Guidance

The purpose of this Appendix is to set out information that must or should be included in a network company's RIIO-2 cyber resilience information technology (IT)[1] and operational technology (OT)[2] re-opener applications (hereon referred to as "IT applications" and "OT applications" respectively) and other requirements that must be fulfilled in making those applications. This Appendix provides additional guidance as to the types of evidence and level of detail that licensees must include when submitting Cyber Resilience IT and OT re-opener applications.

As regards OT applications, where a network company cannot provide the information required below, it must explain why such information is unavailable and submit any relevant alternative information. We will consider such explanations/submissions on a case-by-case basis. We acknowledge that cyber resilience in relation to OT is an evolving area and there could be uncertainty in areas such as cost benchmarking. There may be some projects/solutions where network companies will not be able to provide the necessary level of details listed within this section.

Needs Case

Alignment with overall business strategy and commitments

1.1 IT and OT applications must include details on organisational context, strategy, and business alignment.

1.2 IT and OT applications must include, but need not be limited to, a description of:

- The licensee's overall business strategy;
- The licensee's cyber resilience strategy;
- How the cyber resilience strategy aligns with its business strategy;
- How the IT and OT applications align to previous/in-flight cyber resilience delivery (i.e. The Security of Network and Information Systems Regulations 2018 (NIS) improvement plans[3][4], RIIO-1 activity, etc.);

[1] Information Technology are network and information systems that are used within business functions, for example word processing.
[2] Operational Technology are network and information systems that are considered necessary to the delivery of essential services, for example Supervisory Control and Data Acquisition Systems (SCADA).
[3] NIS Improvement Plans are relevant only for OT re-opener applications.
[4] For those assets that have been identified as enabling the delivery of essential services.

- Internal and external dependencies affecting the proposals set out in the IT and OT applications, and;
- The current and targeted security state and/or maturity of the organisation (e.g. National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)[5] self-assessment[6]/Standard(s) assessment results).

Demonstration of needs case

Problem Statement

1.3 For IT and OT applications the licensee must set out, but need not be limited to, the following:

- A description of 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;
- The services, systems, sites and assets that relate to the identified risks;
- The network company's risk tolerability and risk response decisions; and,
- How the licensee calculated the level of risk (i.e. the rationale behind cyber risk assessment results).

Options Selection

Consideration of project options and methodology of how preferred project option was selected

1.4 For IT and OT applications the licensee must set out, but need not be limited to, the following:

- The methodology and/or standard(s) used to support security and resilience management and decision making;
- The methodology and processes on how cyber risks are assessed, managed, and responded to;

[5] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
[6] CAF self-assessment are relevant only to OT re-opener applications.

- The security and resilience controls (and considered options) required to reduce risks to tolerable levels; and,
- The targeted solutions and projects (and considered options) required to develop and implement the identified security and resilience controls.

Preferred option details (per project)

Description

1.5 For IT and OT applications the licensee must set out, but need not be limited to, the following:

- The project scope, including which sites and assets are in scope;
- The proposed project/option, including general objectives of the project, site(s) applicability, and prioritisation;
- Site breakdown per project/work stream targeted for intervention within this re-opener application;
- The security and resilience controls targeted for implementation as part of this project/sites in scope, and cross-referencing to the CAF outcomes or relevant standard(s);
- Project outputs, including the specific deliverables of the project (what specific products, solutions and technologies are being targeted for delivery); and,
- The security and resilience control links to current and targeted security state and/or maturity (e.g. CAF alignment & assessment/ Standard(s) alignment and assessment).

1.6 The IT and OT applications should include a table listing sites related to the application, including:

- Site function and purpose;
- Site criticality rating and justification; and,
- An overview of the technological architecture and assets of each site.

Technical feasibility and consumer benefit:

1.7 For IT and OT applications 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;
- Detailed list of project constraints, project risks and dependencies (i.e. dependence on IT Cyber/BAU projects, alignment with broader site maintenance activities, etc.); and,
- Details of any underpinning technical feasibility evidence relating to the project and description of how this evidence 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

1.8 For IT and OT applications the licensee must set out, but need not be limited to, the following:

- Detailed project plan and timelines (e.g. Gantt chart);
- Detailed project schedule, including activity milestones for project delivery, personnel on-boarding, training, etc.;
- Governance structure of each project, including project roles & responsibilities and number of resources required;
- The organisational structure of the cyber security team and demonstration of capacity and capability to deliver cyber resilience IT or OT re-opener application 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;
- Key performance indicators to be used to monitor the progress of the project

1.9 For IT and OT applications that make use of agile delivery methods, the licensee should set out, but need not be limited to, the following:

- Description and use of a mature agile methodology/process that allows all stakeholders to understand how they will contribute to the successful delivery of a product, service, project or software with clear milestones. An example of

this would be the Governments Digital Service (GDS) Standard and/or Scaled Agile Framework (SAFE) with guidance for governance and Cyber Physical/Industrial security;

- Clearly defined phases, such as Discovery, Alpha, Beta and Live with milestones/time boxed in line with RIIO plan submissions;
- Sufficiently time boxed sprints with clear definitions that include security;
- All relevant sprint goals include security;
- Description of the governance structure of the teams (e.g. SCRUM team), and how these teams interface with other stakeholders or teams such as legal, governance, scrum of scrum, etc. are also known;
- The sprint tracking methodology e.g. KANBAN with a delivery train mapped out to the phases, such as Discovery, Alpha, etc.)
- Description of how monitoring, lessons learned and improvements will be tracked e.g. retrospectives, show and tell, sprint planning, etc.
- Description of how performance will be monitored, including real users of the service whether external or internal;
- Description how project constraints, dependencies, priorities, risks and similar will be tracked/managed for example will these be reflected in a prioritised backlog;
- Description of how those items that cannot be fixed in sprint are tracked on an issues log such as JIRA or other suitable products;
- Assurances that Product Owners are aligned with the RIIO Team to ensure delivery milestones across the RIIO-2 period are in sync; and,
- Description of key methods, procedures and plans are available and documented on a shared repository such as a wiki, confluence or similar.

Cost information

Breakdown and justification of costs

Consideration of options

1.10 The licensee must justify of the need and amount of allowance required per project, demonstrating consideration against the targeted risk reduction and site prioritisation, to support assessment of consumer value.

1.11 The licensee must also provide a description of the various options that were considered (e.g. by performing cost benchmarking, previous tenders or contract information, etc.), and rationale for the preferred option to be presented.

1.12 The licensee must demonstrate consideration of the expected longevity of security and resilience controls in the context of a changing threat landscape.

Breakdown of costs of preferred option(s)

1.13 For IT and OT applications the licensee must set out, but need not be limited to, the following:

- The overall costs of the IT and OT applications;
- A breakdown of the overall baseline costs for the IT and OT applications 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(s) which are in scope in terms of capex and opex costs & volume and unit costs (wherever applicable);

1.14 For IT and OT applications the licensee should set out, but need not be limited to, the following:

- The current overall running costs as well a breakdown of the current running costs for each site(s);
- Shows the future overall running costs as a result of project implementation as well a breakdown of the future running costs for each site;
- Where an agile delivery methodology is being used the following:
    - 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

1.15 A licensee should provide a description of the procurement/tendering process to be adopted and description of how this process supports cost efficiency;

1.16 For projects that have not entered procurement or tendering processes, a re-opener application must include:

- Best effort view of baseline costs supplemented with uncertainty costs based on assessed delivery risk;
- Cost comparison analysis against the market or benchmarking; and,

- Description of how and when cost uncertainty will be reduced as the project proceeds towards initiation and throughout delivery.