# Requirements

ofgem
Making a positive difference for energy consumers

## RIIO-3 - NIS-R Cyber Resilience Business Plan Assessment Methodology and Requirements

| | |
|---|---|
| Publication date: | 18 July 2024 |
| Contact: | Cyber Resilience – Competent Authority |
| Team: | Cyber Regulation |
| Email: | riio3cyber@ofgem.gov.uk |

This document is directed at electricity transmission, gas transmission and gas distribution network companies (for the purposes of this document collectively referred to as 'network companies'). It builds on the Appendix 4 RIIO-2 Cyber Resilience Re-opener Application Methodology and Requirements v3 (issued directly to the network companies in February 2023) and the sector feedback we have received on the RIIO-3 sector specific methodology consultation ('SSMC').[1]

The purpose of this document is to:

- Set out our assessment methodology for a NIS-R Cyber Resilience Business Plan ('CRBP') submission for both operational technology ('OT')[2] and information technology ('IT')[3] assets that are subject to the Security of Network and Information Systems Regulations 2018[4] ('NIS-R').
- Set out how a network company must prepare its CRBP in accordance with the requirements set out in this document, the NIS-R and National Cyber Security Centre's ('NCSC') Cyber Assessment Framework ('CAF').[5]
- Provide a glossary of terms to support the CRBP submission, Appendix 1.
- Provide further guidance to support the CRBP submission, Appendices 2, 3 and 4.

[1] RIIO-3 Sector Specific Methodology Consultation - Overview Document (ofgem.gov.uk)
[2] Operational Technology means a network company's operational technology network and information systems that interface with physical assets and processes of operations.
[3] Information Technology means a network company's information technology network and information systems that relate to the use of computers, software, hardware and other devices to perform business operations.
[4] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[5] NCSC CAF guidance - NCSC.GOV.UK The CAF provides guidance for organisations responsible for vitally important services and activities.

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

10 South Colonnade, Canary Wharf, London, E14 4PU.

# Contents

**RIIO-3 - NIS-R Cyber Resilience Business Plan Assessment Methodology and Requirements ..... 1**

**1. Introduction ..... 4**

**2. NIS-R Cyber Resilience Business Plan Assessment Methodology ..... 6**

Assessment methodology for a NIS-R Cyber Resilience Business Plan ..... 7
Needs case ..... 7
Alignment with business strategy ..... 7
Risk assessment ..... 7
Options analysis ..... 8
Proposed delivery ..... 9
Cost Assessment ..... 9
Determining baseline allowances ..... 10
Financial mechanisms for cyber resilience ..... 10
Conclusion ..... 11

**3. NIS-R Cyber Resilience Business Plan Requirements ..... 12**

Structure of the NIS-R Cyber Resilience Business Plan ..... 12
NIS-R Cyber Resilience Investment Document (CRID) ..... 14
Investment categories ..... 14
Needs Case ..... 16
Proposed Delivery ..... 17
Cost Assessment ..... 18

**Appendices ..... 20**

**Appendix 1 – Glossary ..... 21**

**Appendix 2 – Overarching principles for NIS-R Cyber Resilience Business Plans ..... 27**

**Appendix 3 – BPDT guidance ..... 29**

Electricity Transmission ..... 29
Gas Distribution ..... 29
Gas Transmission ..... 30

**Appendix 4 – CAF contributing outcome to project mapping ..... 31**

**Appendix 5 – RIIO-3 NIS-R Cyber Resilience Business Plan templates . 35**

NIS Self-Assessment and Improvement Report template ..... 35
NIS-R Cyber Resilience Investment Document (CRID) template ..... 35
NIS-R Cyber Resilience Detailed Costs (Detailed Costs) template ..... 35

**Appendix 6 - Authority directed new re-opener window request process 36**

# 1. Introduction

1.1 We consider there is a significant and continual need for network companies to invest, develop, and undertake activities to reduce risk, improve their cyber capabilities, and better align their organisation with the NIS-R requirements. To measure the implementation progress of NIS-R, the NCSC defined Cyber Resilience Outcomes in the CAF in 2018.[6] Network companies have a clear mandate to incorporate the current CAF profiles into their risk management activities and to adopt the current CAF profiles to assess cyber security resilience and ensure compliance with the NIS-R.

1.2 In RIIO-3, we will no longer require network companies to submit separate business plans for 'Cyber Resilience IT' and 'Cyber Resilience OT', companies should submit one NIS-R Cyber Resilience Business Plan ('CRBP'). This enables better alignment with the NIS-R, which are agnostic of IT and OT environments. We recognise that network companies review, plan and monitor cyber resilience IT and OT systems and activities holistically.

1.3 This document sets out in detail our requirements for a CRBP submission, for network and information systems that are subject to the NIS-R.

1.4 A network company must ensure its CRBP complies with this document, NIS-R and CAF. Failure to prepare a CRBP in accordance with any of the relevant requirements may result in the full or partial rejection of the submission.

1.5 Where a network company has identified a requirement to exceed a CAF profile, we would consider, review and assess these projects. We would require clear justification of the investment where a network company's risk assessment demonstrates this is required. See paragraph 1.18 in the NIS Supplementary Guidance for more information.[7]

1.6 Through the cyber resilience funding route for RIIO-3, we will assess all economic and efficient investments that network companies propose to improve cyber resilience of assets subject to the NIS-R.

1.7 For IT and OT assets that are not within the NIS-R scope, economic and efficient investments will be considered through alternative RIIO-3 funding routes e.g. IT and Telecoms, capex expenditure, asset health, engineering. However, where a network company can demonstrate a clear and well justified link for investment in an asset

[6] NCSC CAF guidance - NCSC.GOV.UK The CAF provides guidance for operators of essential services. Ofgem, as joint Competent Authority with DESNZ for the energy sector in GB, use the CAF to assess the extent to which a network company is mitigating and managing its cyber risks.
[7] Ofgem, August 2023, NIS Supplementary Guidance and CAF Overlay for DGE Sector (ofgem.gov.uk)

that is not subject to the NIS-R that will deliver risk reduction to assets subject to the NIS-R, we may consider this through the cyber resilience funding route, see Appendix 2 and Appendix 3 for more guidance.

1.8 We encourage the network companies to engage with us during their RIIO-3 Business Plan development process and to review the Ofgem NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB.[8]

[8] Ofgem, April 2022, NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB v2.0.pdf (ofgem.gov.uk)

# 2. NIS-R Cyber Resilience Business Plan Assessment Methodology

2.1 This chapter includes the methodology that will be applied to assess a CRBP submission to determine baseline allowances for the RIIO-3 price control period, 1 April 2026 to 31 March 2031.

2.2 Network companies have a clear mandate to incorporate the current CAF profiles into their risk management activities and to adopt the current CAF profiles to assess cyber security resilience and ensure compliance with the NIS-R. In our NIS Supplementary Guidance[9] we set out our expectations regarding the appropriateness and proportionality of security measures to assess compliance with the NIS-R.

2.3 A CRBP must demonstrate how network companies will reduce the risk of incidents on essential services, to ensure a safe and resilient network that is compliant with the NIS-R.

2.4 The CRBP should be based on the NIS Self-Assessment and Improvement Report submitted to Ofgem in Autumn 2022, updated to reflect any scope changes as reported in the NIS Annual Reports, submitted to Ofgem as part of their NIS-R reporting requirements, up to and including the report submitted in July 2024.

2.5 We expect general technology refresh or end of life replacements to form part of more general system investment plans, which should already include appropriate cyber security protection, rather than to be included as part of CRBP.

2.6 For network company business as usual IT and OT activities that include an aspect of cyber resilience e.g. licence upgrades for operating systems, we would expect these to be included in the wider RIIO-3 Business Plan. However, as we outline in Appendix 2 in our overarching principles, we will consider cases where there may be a crossover, where an associated cyber risk is highlighted, for example around the interconnection between business IT and NIS-R assets. In Appendix 3 we provide guidance on where business as usual and asset refresh allowance requests could be included in the sector business plan data templates ('BPDT').

2.7 Where available and appropriate to do so we will consider using historical unit costs to benchmark cyber resilience activities e.g. resource costs.

2.8 In carrying out our assessment of a CRBP, we also consider interactions and interdependencies between IT and OT environments.

[9] Ofgem, August 2023, NIS Supplementary Guidance and CAF Overlay for DGE Sector (ofgem.gov.uk)

## Assessment methodology for a NIS-R Cyber Resilience Business Plan

2.9 Our assessment methodology for a CRBP covers three broad components: **Needs Case, Proposed Delivery, Cost Assessment.** In carrying out our assessment, we consider interactions between the three components.

## Needs case

### Alignment with business strategy

2.10 We consider four key aspects in relation to business alignment when assessing a network company's CRBP. We assess whether:

i) it serves a clear purpose in supporting the organisation to achieve the overall business objectives set out in its RIIO-3 Business Plan (e.g., maintaining a safe and resilient network);

ii) it clearly articulates the linkage of key cyber risks to wider business risks, including how, and to what extent, its cyber resilience activities in its CRBP will reduce risk to the business;

iii) the immediate need for the proposed investment is clear and demonstrates how it will support NIS-R alignment, achieving CAF Contributing Outcomes and reducing risk; and

iv) aligns with any cyber resilience projects that the network company is currently undertaking.

### Risk assessment

2.11 We assess the following aspects in relation to the risk assessment in a network company's CRBP:

i) an accompanying cyber security risk assessment aligned to our NIS Guidance is provided;[10]

ii) the risk assessment reflects the risks, at an applicable level[11], that the network company is seeking funding to mitigate;

[10] NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB v2.0.pdf (ofgem.gov.uk) – see Chapter 4, paragraphs 4.5-4.16, and https://www.ofgem.gov.uk/sites/default/files/2023-06/NIS-R%20Reporting%20Templates.zip see the 'risk assessment results template' embedded in the NIS Annual Report Template v3.0

[11] We would expect network companies to align sub-programmes / grouped activities to deliver risk mitigation against the CAF Principles and CAF Contributing Outcomes.

iii) the consequences and impacts have been assessed and articulated as part of the rationale for the mitigation activities;

iv) risk mitigation activities will lead to a targeted risk reduction in line with the network company's risk appetite; and

v) acknowledgement and assessment of the impact cyber incidents may have on existing and future energy consumers.

2.12 We consider whether the network company demonstrates the overall business need for cyber resilience improvement project(s) and how it aligns to the NIS-R. Particular importance is placed on its inherent,[12] residual,[13] and target[14] risk position. These are used to gauge the reduction in risk, or the mitigation of risk impact from the proposed cyber resilience improvement project(s) and how these contribute to the attainment of CAF Contributing Outcomes.

2.13 We consider the targeted reduction in risk and attainment of CAF Contributing Outcomes as a benefit to the network company and consumers i.e. an advantage gained from the delivery of the output (deliverables) and wider outcome and benefits (business change and cultural shift for cyber security).

2.14 We consider proportionality[15] when assessing requested project costs and the anticipated benefits (i.e., level of risk reduction / mitigation) the project is expected to deliver. For example, we would expect high cost projects to deliver high levels of risk reduction / mitigation. Where this is not the case, we require clear justification on why the allowances are required and how it demonstrates good value for money for consumers.

### Options analysis

2.15 We consider whether the network company provides robust justification of the range of options analysed and clearly demonstrates how the preferred option(s) mitigate the risks identified by the network companies. Justification includes (but is not limited to):

[12] Inherent security risk is assessed to determine reasonable worst cases scenarios. This assessment is based on the assumption that no risk response or control is in place, or existing controls fail to counter the risk.
[13] Existing risk responses and controls are identified and considered within the context of the inherent risk position to develop the residual risk position (i.e., the current position).
[14] All risks, whether above or below tolerability, have a defined risk response. In addition, a target risk position should be presented for those risks with a response that is seeking to change the level of risk.
[15] When assessing the proportionality of those measures, due account shall be taken of the degree of the network company's exposure to risks, its size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

- what the alternative range of options were, and how these were identified and developed;
- how the alternative range of options were assessed and compared;
- why and how the preferred option was selected;
- how the preferred option will protect the network and information systems from specific cyber threats and the risk(s) identified; and,
- how the preferred option represents value for money for consumers and is an appropriate and proportionate solution to mitigate the risk(s) identified.

2.16 We assess whether the options are realistic and applicable to the activities. We will look to identify whether its associated costs are allocated appropriately and proportionally to achieve improvements in risk reduction and CAF Contributing Outcomes, aligning to the NIS-R.

## Proposed delivery

2.17 We consider what governance model a network company proposes to safeguard and effectively monitor project progress, delivery risks, delivery of defined outputs, overall outcome and spend against allowance.

2.18 We consider the approach the network company has taken to build its proposed project plan and the level of detail provided.

2.19 We assess how the network company has identified the level of resourcing required to ensure deliverability of the proposed activities and the associated justification.

2.20 We also consider how the network company proposes to measure the actual risk reduction, and benefits once activities are delivered.

## Cost Assessment

2.21 We assess if the requested baseline allowance as set out in a CRBP is appropriate, proportionate, economic, efficient, and represents value for money for consumers.

2.22 The requested baseline allowance is cross-checked to ensure that a network company's RIIO-3 Business Plan, CRBP and supporting documentation such as Business Plan Data Tables ('BPDT'), NIS-R Cyber Resilience Investment Documents ('CRIDs'), and any supplementary question responses are consistent, and provide clear justification for CRBP requested allowances.

2.23 We assess the approach used by the network company to determine the requested baseline allowance. We consider how the types of expenditure are distributed by

capital expenditure ('capex') and operational expenditure ('opex'). We also consider and compare requested allowance with historic 'Run the Business'[16] costs.

2.24 Where we disagree with the approach, assumptions used, or have found errors we may propose adjustments in the CRBP allowance at draft and final determination.

### Determining baseline allowances

2.25 To determine an appropriate and proportionate baseline allowance for each network company that represents value for money for consumers, we consider:

- if the annual allowances requested are appropriate and proportionate based on the scope of works provided;
- if the source of the cost estimates included in the CRBP are clear and well justified;
- if procurement / tendering has not been undertaken, what steps the network company has taken to determine the efficiency of costs;
- where uncertainty in cost estimates is indicated, how and when the network company proposes to have certainty on these costs e.g. when procurement will be completed; and
- cost benchmarking information where available.

### Financial mechanisms for cyber resilience

2.26 The majority of RIIO-3 CRBP baseline allowances will be awarded using the totex incentive mechanism ('TIM') and monitored through price control deliverables ('PCD').

2.27 Setting baseline allowances using TIM, will encourage companies to look for efficient and innovative ways to deliver cyber resilience and maintain compliance with NIS-R. This also enables better alignment with the wider RIIO-3 price control. Through the NIS Self-Assessment and Improvement Report completed in July 2022 and through NIS Annual reporting network companies have a clear improvement plan to ensure compliance with NIS-R. We expect alignment between the NIS-R improvement plan activities and the NIS-R Cyber Resilience investments requested in RIIO-3.

2.28 Where there is uncertainty in relation to the cost or the nature of the investment required, we will consider awarding allowances via two mechanisms:

i) The first is where a PCD can be set as the network company can justify the business need, the specific needs case, preferred option and schedule, but there is

[16] Run the Business costs are the day-to-day costs associated with operating a business. These are sometimes referred to as Business-as-Usual costs.

uncertainty over the estimated cost to deliver. In this case, allowances will be awarded via TIM and delivery will be monitored via a PCD. A network company must include details of the estimated cost range, lower and upper, and the basis of the estimate for us to assess.

ii) The second is where a PCD cannot be set as the network company can justify the overall business need and specific needs case for a proposed project, but there is uncertainty over the preferred option, schedule and cost. In this case, we will consider awarding a use it or lose it ('UIOLI') baseline allowance. However, this will be by exception and the needs case minimum requirements must be met. If we do award a UIOLI baseline allowance, it will be capped at 20% of a network company's total awarded TIM baseline allowance for cyber resilience and funding will initially only be awarded for years 1-3 of the RIIO-3 price control period. This will enable network companies to move forward at the beginning of RIIO-3 and then submit a mid-period re-opener application once more certainty has been gained. Where a PCD cannot be set and UIOLI is used, the benefits and outcomes will be reported annually and will be assessed ex-post.

2.29 CRBP TIM baseline allowances will be subject to ongoing monitoring in RIIO-3 as part of the outcome-based PCD Reporting process. The CRBP PCDs for RIIO-3 will be aligned to the 16 CAF Principles so all project delivery outputs such as: CAF Contributing Outcome improvements; risk reduction / mitigation; and cyber resilience improvements will be aggregated and mapped against the applicable CAF Principles.

2.30 If a network company identifies a significant emerging cyber threat between submitting their CRBP and the start of the RIIO-3 price control period in April 2026, we may consider directing a re-opener before the mid-period re-opener in 2028. In Appendix 6, we outline the process a network company should follow if it identifies a well justified need to request an Authority directed new re-opener.

## Conclusion

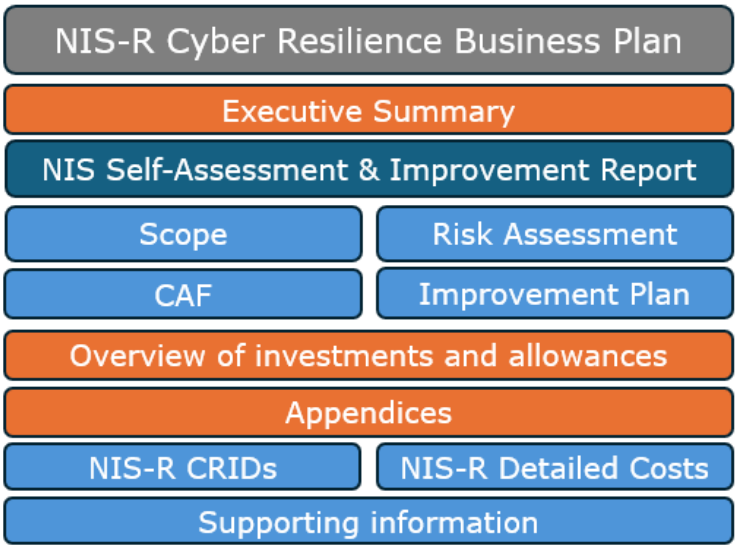
2.31 In conclusion, we will adopt this assessment methodology when reviewing the network companies RIIO-3 CRBP to ensure they represent value for money for the consumer, are economic and efficient and appropriate and proportionate in relation to targeted risk reduction.

# 3. NIS-R Cyber Resilience Business Plan Requirements

3.1 This chapter sets out the minimum requirements a network company needs to include in its CRBP. Figure 1 outlines the component parts a CRBP should include.

3.2 A network company's CRBP must provide us with a clear overview of its NIS-R Cyber Resilience programme and its investment requirements in RIIO-3, Figure 1.

Figure 1: CRBP component parts




3.3 If a network company is not able to provide any of the information set out in this chapter, an exceptions statement must be provided to support the exclusion of the requirement from its CRBP.

## Structure of the NIS-R Cyber Resilience Business Plan

3.4 The CRBP must include a concise executive summary which summarises the RIIO-3 investment requirements.

3.5 The network company must submit an updated version of its July 2022 NIS Self-assessment and Improvement Report. This provides the four key elements to support its RIIO-3 investment requirements:

- Overview & Scope;
- Risk Management;
- NCSC CAF; and
- Improvement Plan.

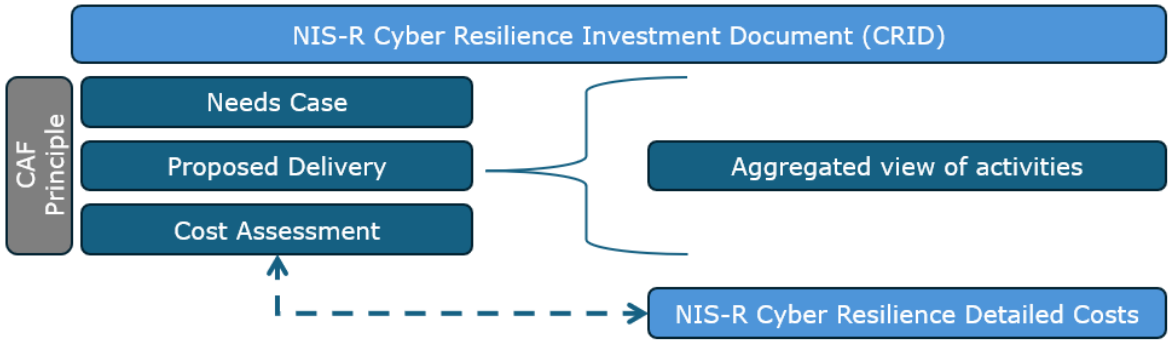
3.6 The network company should include a concise overview of its RIIO-3 investment requirements and the allowances being requested.

3.7 The CRBP Appendices must include the following standardised CRBP templates as a minimum: The NIS-R Cyber Resilience Investment Document (CRID) template and the NIS-R Cyber Resilience Detailed Costs (Detailed Costs) template. Any other supporting information a network company thinks is pertinent to its RIIO-3 investment requirements can also be included within the appendices e.g. Cyber Strategy. See Appendix 5 of this document for links to the CRBP templates.

3.8 The CRID should include details of the needs case, proposed delivery and the costings (see guidance in the following sub-chapter) either at a programme or project level depending on what is most appropriate for the network company to articulate its investment requirements.

3.9 We expect network companies to align each CRID to a primary CAF Principle. This should result in a maximum of 16 CRIDs being submitted, see Figure 2.

Figure 2: NIS- R CRID overview

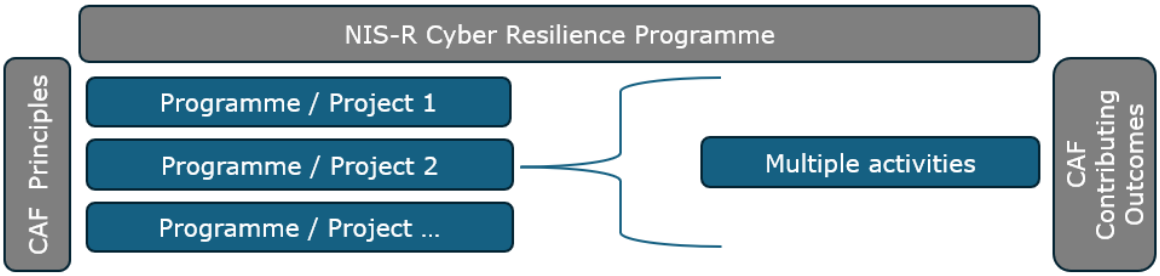



3.10 The Detailed Costs template is required to be populated per project and should align with each of the CRIDs. We expect network companies to align the Detailed Costs template to the primary CAF Principle as per the CRID, see Figure 3.

Figure 3: NIS-R- Detailed Costs overview


3.11 A network company's CRBP must provide a clear overview of its NIS-R Cyber Resilience programme and its investment requirements in RIIO-3, see Figure 4.

Figure 4: NIS-R Cyber Resilience Programme




3.12 The rest of this chapter outlines the minimum requirements for RIIO-3 NIS-R Cyber Resilience investments in the CRID and Detailed Costs.

## NIS-R Cyber Resilience Investment Document (CRID)

3.13 We recognise that some network companies have multi-year programmes spanning price control periods. We require a network company to re-submit documentation to support its RIIO-3 investment request. We expect the network company to review its risks, options, delivery schedule and costs to ensure they are appropriate, proportionate, economic and efficient. If there are no changes to the RIIO-2 submitted needs case, proposed delivery and/or costs this should be clearly stated along with an explanation of the process the network company has followed to confirm this is the case in the CRID.

3.14 Appendices 2, 3 and 4 provide guidance to support the development of the CRBP.

### Investment categories

3.15 For each programme and/or project included in a RIIO-3 CRID we consider that there are two investment categories:

- **Defined investments (TIM)**
    - For programmes and/or projects where there is a justified needs case, proposed delivery, cost to deliver and defined output to mitigate an identified risk as the proposed solutions are well understood and readily available.
    - A price control deliverable ('PCD') can be set to evaluate the success of the delivery in terms of benefits and outcomes.
- **Uncertain investments (UIOLI)**

- For small projects where the needs case has been identified but the solutions are in their infancy or are novel in nature and require allowances to support further development of detailed requirements, scoping and assessment of appropriate technologies to mitigate an identified risk.

- Where a PCD can't be set and UIOLI is used, the benefits and outcomes will be reported annually and will be assessed ex-post.

- As mentioned in paragraph 2.29, UIOLI will be by exception and the needs case minimum requirements must be met. If we do award a UIOLI baseline allowance, it will be capped at 20% of a network company's awarded TIM baseline allowance for cyber resilience and funding will only be awarded for years 1-3 of the RIIO-3 price control period.

3.16 Table 1 provides a summary of the minimum requirements by investment category.

Table 1: Investment category minimum requirements

| **Minimum Requirement** | | **Defined investments** | **Uncertain investments** |
|---|---|---|---|
| **Needs case** | Needs case overview | ✓ | ✓ |
| | Alignment with business strategy | ✓ | ✓ |
| | Risk Assessment | ✓ | ✓ |
| | Options Analysis | ✓ | - |
| **Proposed delivery** | Governance structure | ✓ | - |
| | Delivery model | ✓ | - |
| **Cost Assessment** | People costs (capex/opex) | ✓ | - |
| | Process costs (capex/opex) | ✓ | - |
| | Technology – software (capex/opex) | ✓ | - |
| | Technology – hardware (capex/opex) | ✓ | - |

3.17 In the sub-sections below, we lay out in more detail what the minimum requirements are for a programme and/or project documented in a CRID.

## Needs Case

3.18 This section sets out the needs case information that must be provided for each programme and/or project documented in a CRID. Central to this is the cyber security risk assessment aligned to the NIS Self-Assessment and Improvement Report format.

### Alignment with business strategy

3.19 A programme and/or project must include details of the organisational context, strategy, and business alignment, specifically:

- the network company's overall business strategy.
- the network company's cyber resilience strategy.

3.20 A programme and/or project must set out where there are dependencies with other programmes or projects.

### Risk assessment

3.21 In addition to updating the NIS Self-Assessment Risk Assessment template, [17] a programme and/or project must include the following:

- an overview of the business and cyber risk assessment process and methodology used to identify the current risks facing a network company's assets subject to the NIS-R and its consumers including details on threat, vulnerability, and impact as well as outlining the inherent, residual and target risk positions.
- how the consequences and impacts for the risks have been derived and are related to the assets in scope of NIS-R.
- how the network company calculated the level of cyber risk including the risk severity in terms of likelihood and impact and the scale used to quantify and qualitatively assess the risk.
- why the current security and resilience control/s are insufficient.
- how the network company's risk tolerance affected the response decision.

[17] NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB v2.0.pdf (ofgem.gov.uk) – see Chapter 4, paragraphs 4.5-4.16, and https://www.ofgem.gov.uk/sites/default/files/2023-06/NIS-R%20Reporting%20Templates.zip see the 'risk assessment results template' embedded in the NIS Self-Assessment and Improvement Report Template v3.0. This should be used unless an alternative risk assessment template was agreed with Ofgem as part of the NIS Self-Assessment submission in July 2022.

- how and why the specific project, once delivered, will impact on the inherent, residual and target risk positions as well as how this will be monitored during and after project delivery.

Options analysis and selection

3.22 This section sets out the options analysis information that must be provided in for a programme and/or project.

3.23 A programme and/or project must include:

- the problem statement being addressed.
- an overview of the range of options identified, evaluated and assessed. Where the options are limited for the chosen remediation, the network company should articulate the rationale for presenting a reduced set of options.
- the cyber resilience controls identified to address the needs case i.e., the options considered and preferred option.
- the methodology and/or standards used to identify the options considered and how these were shortlisted.
- feasibility assessments including deliverability in the network company's specific environments, any resource consideration including any third-party vendors and contractors' requirements.
- volume of sites where preferred option would be delivered and/or where new people resources are required to deliver.
- information to demonstrate how and why the preferred project has been prioritised for investment at this point in time and how it has been considered against the targeted risk position.
- how the preferred project represents value for money and why it is a proportionate solution that will best address the identified need.
- for uncertain outputs, network companies should include any feasibility evidence such as research and development output, technical studies, demonstrations, or design work.

### Proposed Delivery

3.24 This section sets out the governance and delivery model information that must be provided in for a programme and/or project.

Governance and delivery model

3.25 A programme and/or project must include:

- the governance structure, 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 the plan including how the outputs will be integrated into business as usual (where relevant).
- the scope, including its general objectives, site applicability, site criticality rating and justification and prioritisation.
- a detailed list of project constraints, project delivery risks and dependencies (i.e., dependence on other cyber / business as usual activities, alignment with broader site maintenance activities).
- programme and/or project output(s), including any specific sub-deliverables (what specific products, solutions and technologies are being targeted for delivery).
- programme and/or project plan and timelines (e.g., Gantt chart, excel or MS Project).
- a resource plan to demonstrate the number of resources required to deliver the project, the roles required, how the resources will be managed and if the resources are also involved in other projects.
- a description of how programme and/or project performance will be monitored, including key performance indicators including alignment of CAF Contributing Outcomes to the performance of the overarching cyber security management system and performance of risk mitigation delivered through PCDs.
- Defining year on year outputs for each year of funding.

**Cost Assessment**

Breakdown and justification of costs

3.26 A programme and/or project must include:

- Information to justify the allowance required.
- An explanation to demonstrate how programme and/or project costs have been derived, including any cost benchmarking where available and where efficiencies have been identified.

- Outline any cost uncertainties and how this will be managed / mitigated including a timeline for when cost certainty is expected.
- Information to demonstrate how the activities within the programme and/or project have been prioritised for investment at this point in time and how it has been considered against the targeted risk position.
- Explain how the programme and/or project costs demonstrates value for money for customers.
- Alongside the CRID, network companies must complete the Detailed Costs template. For each project network companies must provide:
- the baseline totex costs for the people, process and technology activities per year.
- a breakdown of the capex and opex costs for the people, process and technology activities per year.
- a breakdown of the capex and opex cost elements for each activity including volume and unit costs.
- supporting narrative to support the rationale for the requested investment.

3.27 Where agreed between a network company and Ofgem, the network company can apply customisation on the Detailed Costs template.

# Appendices

Index


| Appendix | Name of appendix | Page no. |
|---|---|---|
| 1 | Glossary | 23 |
| 2 | Overarching principles for NIS-R Cyber Resilience Business Plans | 29 |
| 3 | BPDT guidance | 31 |
| 4 | CAF contributing outcome to project mapping | 33 |
| 5 | RIIO-3 NIS-R Cyber Resilience Business Plans templates | 37 |
| 6 | Authority directed new re-opener window request process | 38 |

# Appendix 1 – Glossary

| Term | Description |
|---|---|
| Benefit | Measure of the advantage gained by the organisation through achieving the outcomes from the project |
| Business as usual | Routine activities and maintenance activities that form part of a normal series of business operations. These activities focus on the operation of the business. |
| Cyber Assessment Framework (CAF) | Means the Contributing Outcomes set out under the cyber security and resilience principles set out on the NCSC's website, titled 'Cyber Assessment Framework'. Current version can be found at Cyber Assessment Framework - NCSC.GOV.UK. |
| Consumer Outcome | Means the benefits to existing and future consumers in terms of maintenance of existing levels of, or improvements in the network's capability or resilience including cyber resilience, or benefits to consumers in terms of service quality, or reduction in risk delivered, that would have been delivered by the PCD output over the whole life of the PCD output as specified in the relevant licence condition. In the context of works delivered by the network company, this means the benefits to customers or consumers in terms of maintenance of existing levels of, or improvements in the network's capability or resilience including cyber resilience, or benefits to consumers in terms of service quality, or reduction in risk delivered, that can be attributed to the works delivered by the network company over the whole life of the works delivered. |
| Critical National Infrastructure (CNI) | Means those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), as designated by DESNZ, which the loss or compromise of which could result in: (a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; or (b) significant impact on national security, national defence, or the functioning of the state.<br>Note: DESNZ will designate sites as CNI via an official letter. |
| Essential Service | Means a service which is essential for the maintenance of critical societal or economic activities. An operator of essential service will be formally designated by DESNZ via an official letter.<br>See The Network and Information Systems Regulations 2018 (legislation.gov.uk) |
| Full-Time Contractor / Fixed Term Contractor (FTC) | An employment contract where there is a fixed end date for the contractor. The FTC would be calculated as an FTE i.e. 40 hours per week equates to 1 FTC. Labour costs include any form of payment, consideration or other benefit, paid or due to or in respect to temporary contractors, fixed term contracts or Agency Staff. |
| Full-Time Equivalent (FTE) | A full-time, permanent employee deployed to an activity or series of activities where the organisation has identified the number of FTE to service these activities. One full-time employee working ~40hours per week equates to 1 FTE. Labour costs include any form of payment, consideration or other benefit, paid or due to or in respect of full time employees. Gross salaries and wages of all employees with the cyber security program, including payments resulting from bonus and profit-related payment schemes. |
| Hardware | Hardware refers to the external and internal devices and equipment to perform functions such as input, output, storage, and communication.<br>Expenditure on new and replacement hardware used to support the operation of the assets subject to the NIS-R. These types of hardware support compliance activities within the CAF and address the needs of the organisation to minimise the impact of risk and incidents to its network and information systems. This hardware must have a NIS-R Cyber Resilience focus and not part of general IT appliances used by the network company. |
| Incident | Any event having an actual adverse effect on the security of network and information systems. |
| Inherent risk position | Inherent security risk is assessed to determine reasonable worst cases scenarios. This assessment is based on the assumption that no risk response or control is in place, or existing controls fail to counter the risk. |
| Innovation | Involves the application of technology, systems or processes that were not proven as at the time of submission of the Business Plan. |
| Information Technology | Means a network company's information technology network and information systems that relate to the use of computers, software, hardware and other devices to perform business operations. |

| Term | Description |
|---|---|
| License costs | Refers to costs associated with software licences. These costs may be split into different categories for different software vendors:<br>• Perpetual software licence model<br>• Subscription software licence model<br>• Consumptive software licence model<br>• Pay-per-use licence model |
| Network Security: Identity and Access Management | Systems used to control access to the organisation's NIS-R assets, commensurate with the risk to critical infrastructure and organisational objectives. Costs to develop, manage and enforce identity management capabilities for entities granted logical or physical access to the organisation's NIS-R assets. Technologies and methods to:<br>• Establish of identities and management of Authentication, Authorisation and Access controls for network and information systems;<br>• Control of Logical Access;<br>• Control of Physical Access. |
| Network Security: Network Monitoring | Hardware and Software solutions used to support collection, monitoring, analysis, alarming, reporting, and use of operational, security, and threat information for the purpose of detecting security incidents and reporting on security posture of NIS-R assets. Technologies and methods for:<br>• Malicious Code Detection;<br>• Network Traffic Analysis;<br>• Device Posture Assessment;<br>• Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing).<br>Costs associated with the deployment of technologies to provide network monitoring and logging for security information and events. Measures applied must have a NIS-R Cyber Resilience focus and not part of general IT systems, applications and services used by the network company. |
| Network Security:<br>Threat and Vulnerability Management | Acquisition of threat intelligence for NIS assets. Deployment of tooling to report upon vulnerabilities within the NIS operated and support for management / remediation through active vulnerability management. Technologies and methods for:<br>• Vulnerability Scanning;<br>• Automated Asset Discovery<br>• Hardware / Software Security Configuration Status posture assurance;<br>• Acquisition and deployment into the environment threat intelligence to assist with security posture assessment;<br>• Flaw Remediation and Patch Management Software.<br>Costs associated with hardware / software technologies used to detect, identify, analyse, manage, and respond to cybersecurity threats and vulnerabilities. Measures applied must have a NIS-R Cyber Resilience focus and not part of general IT systems, applications and services used by the network company. |

| Term | Description |
|---|---|
| Network Security: Security Architecture | Network Architecture Improvements. Network protections are defined and enforced for selected asset types according to NIS asset risk and priority. May include: -<br>• development of NIS cyber resilience through introduction of redundancy measures and service separation/reinforcement;<br>• introduction of security controls to harden devices, establish defence in depth protections.<br><br>Examples:<br>• Logical or physical segmentation of NIS assets into distinct security zones based on asset cybersecurity requirements;<br>• Implementation of micros segmentation and or application of zero trust architecture;<br>• Necessary architectural changes to NIS systems to support operational independence from IT systems so that NIS assets can be sustained during an outage of non-NIS systems;<br>• Establishment of network protections to support monitoring, analysis, and control of network traffic for selected security zones.<br><br>Addition of network monitoring to support: -<br>• Asset management, including discovering and inventorying devices connected to the network;<br>• Baselining typical network traffic, data flows, and device-to-device communications;<br>• Diagnosing network performance issues;<br>• Identifying misconfigurations or malfunctions of networked devices.<br><br>Additional protective Technologies: -<br>• Logging;<br>• Media Protection;<br>• Secure Remote Access Solutions;<br>• Secure remote connection;<br>• Data encryption solutions to handle data at rest and in transit;<br>• Deployment of time synchronisation services were these are relied upon for security monitoring and log correlation.<br><br>Costs associated with architectural changes required to support separation and segregation of NIS-R Assets and implementation of network protections based on security risk.<br><br>Measures applied must have a NIS-R Cyber Resilience focus and not part of general IT systems, applications and services used by the network company. |
| Secure Configuration: Physical Hardening / Device Hardening | Application of Security Controls to minimise the probability of inappropriate or unauthorised use of NIS-R assets or interference with the normal functioning of NIS-R assets.<br>Application of secure software and hardware configuration(s) (device hardening) for NIS-R assets. Physical hardening of NIS-R assets to prevent local interference and misuse. Such as asset marking, tamper protection, secure fixings, cabinets and storage locations. Improvements to security housing of NIS assets.<br><br>Costs associated with configuration hardening for both hardware and operating software. May include measures applied to prevent physical access to NIS assets to minimise local interference and abuse. Measures applied must have a NIS Cyber Resilience focus and not part of general IT systems, applications and services used by the network company.<br><br>Exclusions for RIIO-3 NIS-R Cyber Resilience funding: Physical security for buildings and locations where these are used to protect infrastructure assets holistically from multiple threat sources and are not specifically related to NIS-R assets. (NIS-R risk categorisation may raise additional requirements for protection over and above existing requirements and may still be in scope of RIIO-3 NIS-R Cyber Resilience funding). |
| Security Incident and Event management, Recovery and Response | Event and Incident Response and Recovery, Restoration. Secure Storage solutions for the purpose of managing data securely. Automated tooling to perform and verify the integrity of backups of NIS assets, configurations and related data sets for the purpose of recovery and restoration. Dedicated spares holdings for timely restoration and testing of recovery processes and procedures including integrity validation.<br><br>Mechanisms for communicating during incident response outside of normal channels should these be affected by the incident (emergency communications channels). An OES may already have provided for these measures through related business continuity planning for other types of incidents. Dedicated software or hardware for enactment of incident response processes and procedures for NIS-R assets were these are do not covered by general business continuity programmes.<br><br>Costs for development and deployment of infrastructure (hardware and software) to facilitate and manage backups and manual or automated recovery and restoration of NIS-R critical assets. Measures applied must have a NIS-R Cyber Resilience focus and not part of general IT systems, applications and services used by the network company. |

| Term | Description |
|---|---|
| NIS-R Critical Assets (assets within scope of the NIS-R) | Network and information systems on which the essential service relies, or which are used for the provision of an essential service, as per the definitions in the NIS-R.<br>Within the NIS-R (Regulation 2(1)), the term 'network and information systems' means:<br>(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003;<br>(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or<br>(c) digital data stored, processed, retrieved, or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance; |
| Non NIS-R Critical Assets (assets out of scope of the NIS-R) | Assets identified by the network company, in their role as an operator of essential service, which may support the operation or function of the NIS-R Critical Asset, but in itself is not critical to the delivery of the essential service documented by the network company.<br>Note: Whilst these assets may be treated as additional to the NIS Critical Asset, any technical dependencies between the two sets of assets should be reviewed to determine their inclusion or exclusion from scope. |
| Outcome | The direct impact to the organisation or key stakeholders as a result of the delivery of the output. |
| Output | The deliverables of the project from a people, process and technology viewpoint. |
| Operational Technology | means a network company's operational technology network and information systems that interface with physical assets and processes of operations. |
| People | High-level category used to summarise the people element of a cyber security program. The people element refers to those employees or contractors identified by the organisation to run the essential service.<br>Employees from a financial perspective are further classified as full-time equivalents (FTEs). These are permanent employees.<br>Contractors from a financial perspective are further classified as full-time contractors (FTCs). These are fixed term contracted employees. |
| Process | High-level category used to summarise the process element of a cyber security program. The process element refers to those management systems, procedures and policies required by an organisation to function correctly.<br>This may also extend to third party consultancy firms who are contracted by the organisation to support the delivery of assurance activities where or independent view is required by the organisation for its cyber security program. Or where a service is required to be performed by a third party service organisation to support the delivery of the cyber resilience program. |
| Professional Services | Services provided on a consultancy basis, typically items such as assurance and support activities in maintaining or achieving compliance with NIS-R. It represents costs incurred by contracting with organisations for the provision of services. |

| Term | Description |
|---|---|
| Programme | A NIS-R Cyber Resilience programme is a holistic set of projects (activities) which are aligned to business and security strategies that support the cyber security management of systems and assets, that are subject to NIS-R, at a network company. A NIS Cyber Resilience programme should deliver a clear outcome / or series of outcomes and should consist of the following:<br>• strategy<br>  ○ business.<br>  ○ cyber.<br>• governance model<br>  ○ cyber security teams and oversight and delivery boards.<br>• project management office<br>  ○ repeatable, defined process for the delivery of projects.<br>• dependencies<br>  ○ sub-programs or projects are deemed critical to the success of the programme or to allow another project to complete.<br>• outcomes and monitoring<br>  ○ the sum of the projects will deliver an outcome or series of outcomes within a certain timeframe.<br>  ○ these projects will be monitored for completion.<br>• costings<br>  ○ the total cost for the programme.<br>  ○ allowances requested in each year of the programme. |
| Project | A NIS-R Cyber Resilience project should deliver a clear output or set of outputs that contribute to the NIS Cyber Resilience programme outcome(s). There should be key performance indicators and milestones designed to support the delivery of the NIS Cyber Resilience programme. A project should have a design, implementation, delivery and review phases. |
| Residual risk position | Existing risk responses and controls are identified and considered within the context of the inherent risk position to develop the residual risk position (i.e., the current position). |
| Risk | Means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems |
| Run the business (RtB) | Normal day to day operations. In terms of costs these are the ongoing operational expenses incurred from running the business. |
| Scope (scope of the NIS-R network companies have identified) | The NIS Scope should set out full details of the network and information systems on which the essential service relies, or which are used for the provision of an essential service. The NIS-R define what ‘network and information systems’ and ‘essential service’ means, and these must be considered when developing the NIS Scope. |
| Security of network and information systems | Means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems. |

| Term | Description |
|---|---|
| Software | A set of instructions, data or programs used to operate computers or similar devices to perform specific tasks. Software can be further categorised into:<br>• Application<br>• System<br>• Middleware<br><br>Expenditure on new and replacement software used to support the operation of the assets subject to the NIS-R. These types of software support compliance activities within the CAF and address the needs of the organisation to minimise the impact of risk and incidents to its network and information systems. This software extending to, but not limited to, applications and systems must have a NIS-R Cyber Resilience focus and not part of general IT systems, applications and services used by the network company.<br><br>Any software whose primary function is to improve security or network resilience. Application of secure software lifecycle processes for proprietary software solutions. Support for migration of software solutions from obsolete operating systems onto a current (supported) operating system. This may include lifecycle upgrades to move between major versions of an OEMs core software application used for the essential service (e.g. energy management distribution systems) however these costs may be better directed via other RIIO funding schemes. |
| Target risk position | All risks, whether above or below tolerability, have a defined risk response. In addition, a target risk position should be presented for those risks with a response that is seeking to change the level of risk. |
| Technology | High-level category used to summarise the technology element of a cyber security program. The technology element refers to both hardware and software deployed by the organisation to supports its risk appetite and to support the integration of the people and process elements of a cyber security program. |
| Totex Incentive Mechanism (TIM) | The totex incentive mechanism (TIM) is applied in RIIO to incentivise companies to find cost efficiencies with the benefits of these efficiencies to be shared with consumers. The TIM applies a sharing factor which incentivises companies to be more efficient by enabling them to take a share of under and overspend, with the remainder passed to consumers. |
| Uncertain | In relation to costs only and not to mechanisms whereby network companies can present re-opener applications.<br><br>Where costs are unknown or are in their infancy e.g. a rigorous cost assessment has not been conducted due to several factors such as:<br>- lack of a supplier to deliver the innovation or control.<br>• timing issues to accurately scope the requirements of the project and therefore, a range of costs are presented. |
| Use-it-or-lose-it (UIOLI) | Uncertainty mechanism for allowances where the need for work has been identified, but the specific nature of work or costs are uncertain. |

# Appendix 2 – Overarching principles for NIS-R Cyber Resilience Business Plans

We have developed a set of overarching principles to guide CRBP submissions:

- **Principle 1- NIS-R Critical Assets**: Where cyber security risks have been identified on assets subject to NIS-R we would encourage network companies to includes this in its CRBP detailing the assessment of the risk, justification of the remediation activity to achieve a targeted risk reduction or attainment of CAF maturity which is appropriate and proportionate, economic and efficient and is underpinned by the benefit to the consumer.

    (1) Supporting comments for Principle 1a: We would expect network companies to review its assets that are within the NIS-R scope and cyber security risk assessments in preparation for its CRBP. We would expect network companies to provide clarity and rationale as to why the risk is beyond its organisational risk tolerance. We would also expect where a network company has identified a requirement to exceed the maturity within the CAF profile(s) (relative to attacker capability) then it can justify the basis of the investment. Detailing the risk posed to its network and information systems.

    (2) Supporting comments for Principle 1b: Where security improvements have been identified for assets within its NIS-R scope, requiring investment to the asset in terms of replacement and removal to mitigate vulnerabilities in underlying, hardware, software or within the supply chain, we would encourage the network company to review more applicable schemes within RIIO to submit requests for allowances.

- **Principle 2- Non NIS-R Critical Assets**: Where a network company threat assessment identifies a cyber security risk impacting assets that are not included within its NIS-R scope we would encourage network companies to engage with us as soon as possible to determine if this should be included in the CRBP or wider RIIO-3 Business Plan. If it is deemed suitable for inclusion in the CRBP, a network company will need to detail the assessment of the risk, justification of the remediation activity to achieve risk reduction or attainment of CAF maturity which is appropriate and proportionate, economic and efficient and is underpinned by the benefit to the consumer.

    (1) Supporting comments for Principle 2a: In addition to the supporting comments for Principle 1, we would expect network companies to be able to justify why these additional assets (non NIS-R critical assets) have not

been included within its declared NIS-R critical assets scope where they may be viewed as important to the security of the essential service provided.

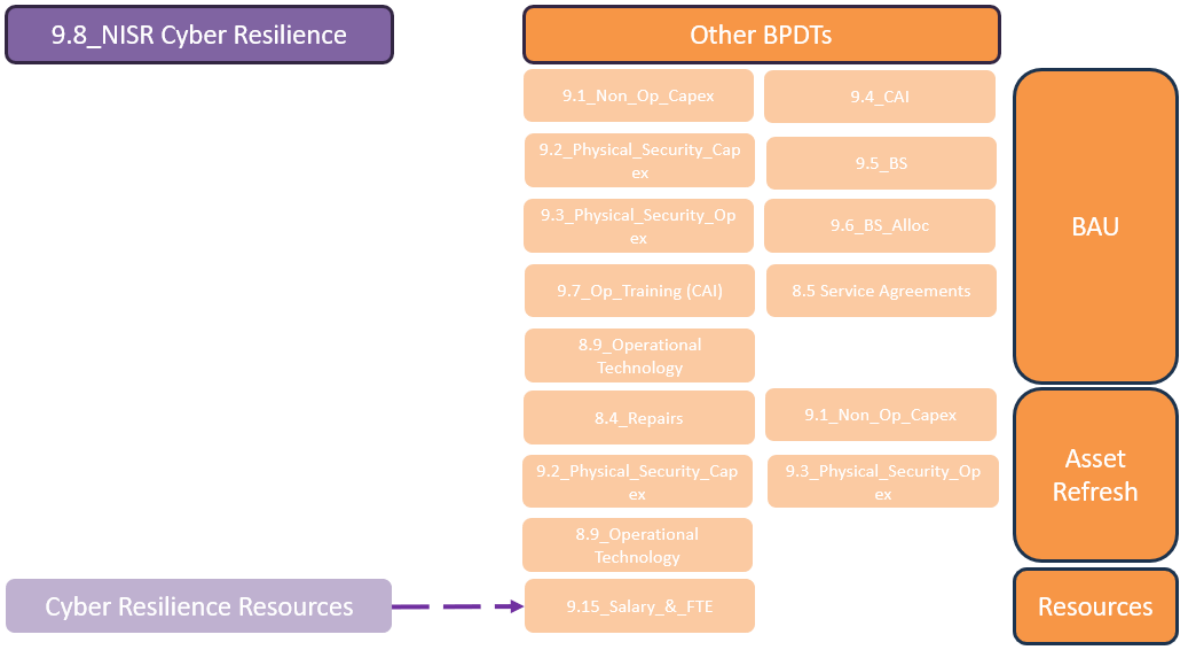
(2) Supporting comments for Principle 2b: We would expect network companies to demonstrate the threat modelling or attack path scenarios it has devised to support the justification of investment via its NIS-R Cyber Resilience Submission for assets that are not subject to NIS-R.

As mentioned in the principles outlined above, we will consider economic and efficient investment requests to improve cyber resilience of assets subject to the NIS-R. There are other funding routes for assets that are not subject to the NIS-R which we also outline in the introduction of this document.

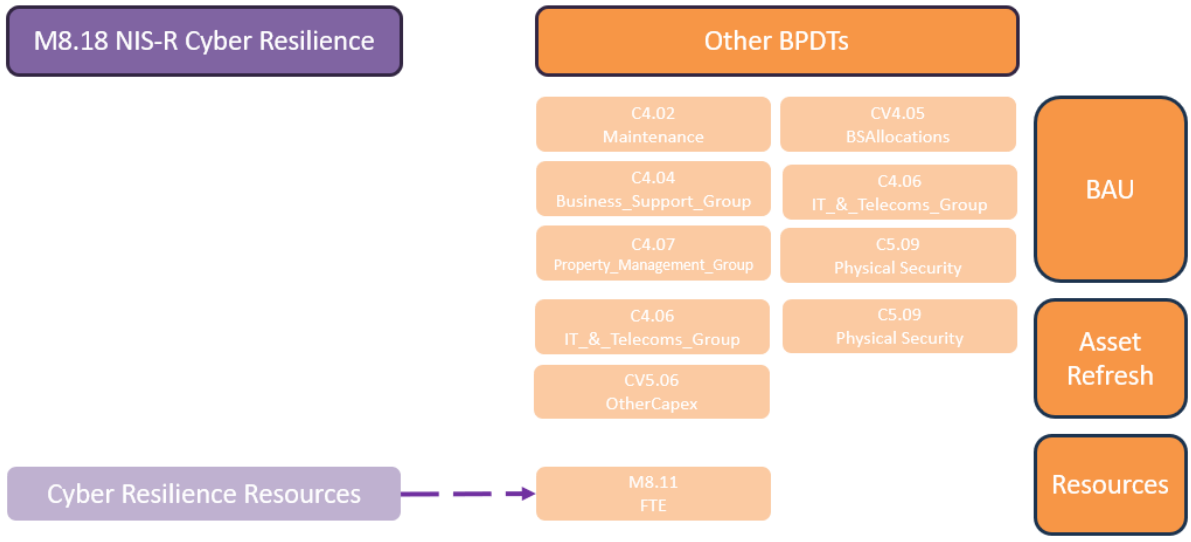
# Appendix 3 – BPDT guidance

In this appendix we provide indicative guidance on where business as usual, asset refresh and resource costs could be captured in the business plan data templates ('BPDT') for each sector. This is not a prescriptive list; we recommend that the companies review the Regulatory Instructions and Guidance ('RIGs') document for more detailed guidance.

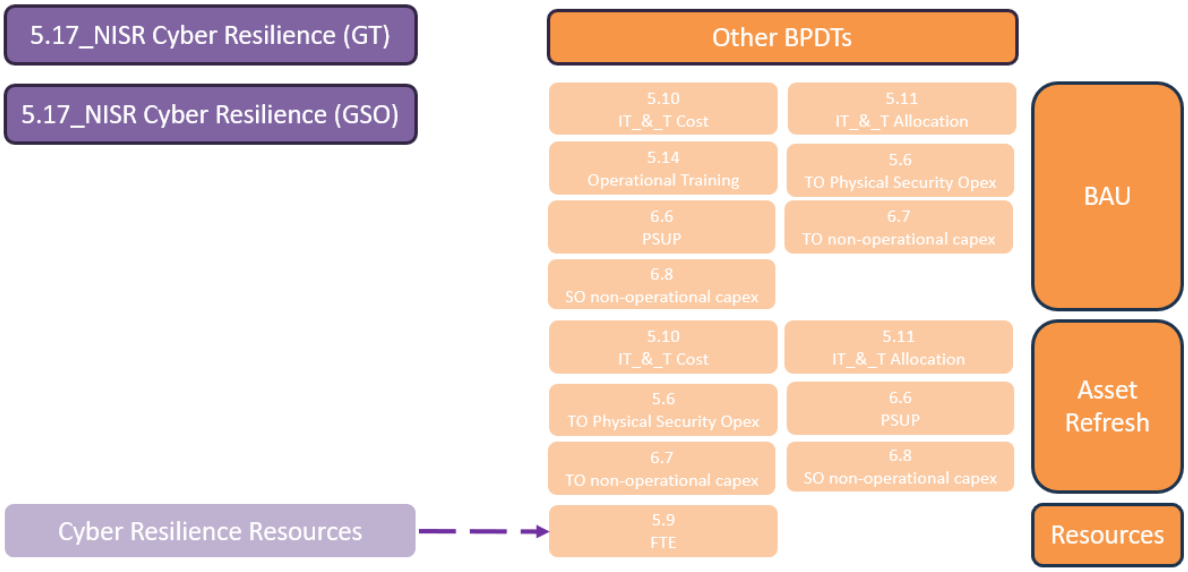
## Electricity Transmission




## Gas Distribution



## Gas Transmission



## Appendix 4 – CAF contributing outcome to project mapping

The table has been designed to support network companies in mapping activities they may conduct aligned to the CAF Principles and Contributing Outcomes. These example projects have been derived from NIS Supplementary Guidance and CAF Overlay for DGE Sector. Note that in Annex E of the NIS Supplementary Guidance there are project mappings of NIST CSF to CAF, Mitre Attack-ICS to CAF, Mitre Enterprise to CAF, ISO27002/19 to CAF, ISA/IEC 62443-2-1 to CAF and ISA/IEC 62443-3-3 to CAF.

This table is not a prescriptive list, nor is it intended to provide a checklist for network companies to submit requests for investments. Network companies are required to conduct a risk assessment to determine the need for the investment.

| CAF Objective | CAF Principle | CAF Contributing Outcome | Example Activities which may be included in a NIS-R CRID |
|---|---|---|---|
| **A** | **A1. Governance** | **A1.a Board Direction** | Cyber/Information Security Management System Development, Implementation and Review |
| | | | Governance and Reporting Structures |
| | | **A1.b Roles and Responsibilities** | Target Operating Model |
| | | | Resource Allocation – FTE and FTC |
| | | | RACI Matrix |
| | | | Skills/Capability Matrix |
| | | **A1.c Decision-making** | See A1.a; A1.b |
| | **A2. Risk Management** | **A2.a Risk Management Process** | Risk Management Methodology |
| | | | Risk Assessment Process and Review |
| | | | Business/Operational Impact Assessments |
| | | **A2.b Assurance** | Assurance Activity |
| | | | Audit and Inspection Preparedness |
| | **A3. Asset Management** | **A3.a Asset Management** | Asset Register |
| | | | Dependency mapping- Identification and Recording |
| | | | Asset Prioritisation exercises |
| | | | Obsolete Device Management |
| | **A4. Supply Chain** | **A4.a Supply Chain** | Supply Chain Assessments and Security Monitoring |
| | | | Supply Chain Mapping, Recording and Review |
| | | | Supply Chain Processes- Lifecycle management |
| | | | Information Asset Registers |
| | | | Security Requirements |
| **B** | **B1. Policies & Processes** | **B1.a Policy & Process Development** | Cyber Security Processes and Documentation |
| | | | Behavioural and Circumvention Risk Management activities |
| | | **B1.b Policy & Process Implementation** | Policy and Document Monitoring and Integration |
| | | | Policy and Document Compliance activities |
| | | | Policy and Document Communication and Awareness |

| CAF Objective | CAF Principle | CAF Contributing Outcome | Example Activities which may be included in a NIS-R CRID |
|---|---|---|---|
| | **B2. Identity & Access Control (IDAC)** | **B2.a Identity Verification, Authentication and Authorisation** | Access Review and Recertification exercises see B2.d |
| | | | Access Control Management e.g. Joiners, Movers and Leavers |
| | | | Pre-Employment Checks including verification of third parties |
| | | **B2.b Device Management** | Dedicated Device Management for General, Third Party and Privileged Access |
| | | | Certificate-based Device Identity Management |
| | | | Unknown Device Detection programme |
| | | **B2.c Privileged User Management** | Enhanced Authentication |
| | | | Dedicated Account Management for Privileged Access |
| | | | Privileged Access Management including 3rd party tracking, monitoring and review see B2.d |
| | | **B2.d Identity and Access Management (IdAM)** | Role-Based Access Control |
| | | | User Access tracking, monitoring and review (note: monitoring from a SIEM or similar for unauthorised access) |
| | **B3. Data Security** | **B3.a Understanding Data** | Data Understanding, Cataloguing and Flow mapping |
| | | **B3.b Data in Transit** | Data Protection Measures- in Transit |
| | | **B3.c Stored Data** | Data Protection Measures- at Rest |
| | | **B3.d Mobile Data** | Mobile device management |
| | | **B3.e Media / Equipment Sanitisation** | Data Sanitisation |
| | **B4. System Security** | **B4.a Secure By Design** | Network Security |
| | | | Enforcement Boundary |
| | | | Recovery Systems and Services e.g. Backups |
| | | **B4.b Secure Configuration** | Secure Configuration and Installation Management (includes hardening activities) |
| | | | Change Control and Approval |
| | | | See A3.a includes Patch Management |
| | | **B4.c Secure Management** | Unauthorized Software Management |
| | | | See B2.a, c & d |
| | | **B4.d Vulnerability Management** | Vulnerability Management |
| | | | Vulnerability Testing, Exercising and Remediation |
| | **B5. Resilient Networks & Systems** | **B5.a Resilience Preparation** | Business Continuity Management System |
| | | | Disaster Recovery |
| | | **B5.b Design for Resilience** | Network Security Architecture- Segregation |
| | | | See A2.b |
| | | | See B4.a |
| | | **B5.c Backups** | Backup Management |

| CAF Objective | CAF Principle | CAF Contributing Outcome | Example Activities which may be included in a NIS-R CRID |
|---|---|---|---|
| | | | Backup Management Processes including Testing |
| | **B6. Staff Awareness & Training** | **B6.a Cyber Security Culture** | Cyber Security Culture Programme |
| | | | Cyber Security Culture- Incident Reporting |
| | | **B6.b Cyber Security Training** | Cyber Security Training Programme |
| **C** | **C1. Security Monitoring** | **C1.a Monitoring Coverage** | Monitoring Strategy |
| | | | Intrusion Detection/Prevention |
| | | **C1.b Securing Logs** | Secure Log Management and Monitoring |
| | | | Protection of Logging Architecture |
| | | **C1.c Generating Alerts** | Alert Investigation and Analysis |
| | | | Alert Tuning and Log Enrichment |
| | | **C1.d Identifying Security Incidents** | Threat Intelligence Information Management |
| | | **C1.e Monitoring Tools & Skills** | Workflow definition |
| | | | See A1.b |
| | | | Tool Selection, Utilisation and Coverage |
| | **C2. Proactive Security & Event Discovery** | **C2.a System Abnormalities for Attack Detection** | Monitoring Programme Effectiveness |
| | | | System Abnormality Descriptions (link to A2.a) |
| | | | Advanced Detection Algorithms |
| | | **C2.b Proactive Attack Discovery** | Automated Monitoring and Prevention |
| | | | Optimisation of Monitoring Systems and Detection Capabilities |
| | | | Routine Exception Monitoring |
| **D** | **D1. Response & Recovery Planning** | **D1.a Response Plan** | Incident Response Management |
| | | **D1.b Response & Recovery Capability** | Incident Response and Recovery Management |
| | | | Playbook Design, Implementation and Review |
| | | | External Support Capabilities- Arrangement and Engagement |
| | | **D1.c Testing & Exercising** | Exercise Testing and Development |
| | | | Test/Attack Scenario Design, Implementation and Review |
| | **D2. Lessons learnt** | **D2.a Incident Root Cause Analysis** | Root Cause Analysis |
| | | **D2.b Using Incidents to Drive Improvements** | Lessons Learned Process |
| **E** | **E1. Physical security of network & information systems** | **E1.a Governance and risk management processes relating to physical security risks** | Development of Teams see A1.b |
| | | | Physical Security Risk Assessments and Breach reviews see A2.a |
| | | | Identify Zones, Areas and Facilities containing assets subject to NIS Scope see A3.a |
| | | **E1.b Designing and implementing physical security controls** | Review and Refresh of NIS Scope |

| CAF Objective | CAF Principle | CAF Contributing Outcome | Example Activities which may be included in a NIS-R CRID |
|---|---|---|---|
| | | | Advice and Guidance on Physical Security Measures and Controls |
| | | | Design, Implementation and Review of networks managing physical security systems |
| | **E2. Broader network and information systems resilience risks** | **E2.a Broader resilience risks** | Risk and Control Framework development for resilience measures |

# Appendix 5 – RIIO-3 NIS-R Cyber Resilience Business Plan templates

This appendix provides links to the templates we require network companies to use for the RIIO-3 CRBP.

## NIS Self-Assessment and Improvement Report template

Use the NIS Self-Assessment and Improvement Report template as the basis for the NIS-R Cyber Resilience Business Plan: [Network and Information Systems Regulations 2018: Ofgem Guidance for Operators of Essential Services | Ofgem]

## NIS-R Cyber Resilience Investment Document (CRID) template

Use the CRID word template.

## NIS-R Cyber Resilience Detailed Costs (Detailed Costs) template

Use the Detailed Costs excel workbook.

# Appendix 6 - Authority directed new re-opener window request process

If a network company identifies a well justified need such as a significant emerging cyber threat or change in the regulatory landscape during RIIO-3 it can request the Authority to direct a new re-opener window using the following steps:

| | |
|---|---|
| **Bi-lateral with Ofgem** | Required Ofgem Attendees: Cyber Regulation Director, Deputy Director and Head of Investment Delivery<br>**Agenda items to discuss the rationale to request an Authority directed Re-opener and materiality of cost associated with the Re-opener** |
| **Formal Letter requesting Authority directed new Re-opener window** | To be submitted to Ofgem Cyber Regulation Director, Deputy Director and Head of Investment Delivery<br>Content Must Demonstrate:<br>• Project Materiality<br>• Justification of request in absence of the established re-opener window or business plan submission window<br>• Timeline of re-opener activities<br>• Exploration of alternative internal opportunities that provide remediation without triggering a new re-opener<br>• Rationale for determining if the re-opener should be solely for the proposing network company or extend to the wider sub-sector. |
| **Re-opener Application** | Submit to Ofgem via a Secure Information Exchange ('SIE') link the Re-opener Application.<br>The Re-opener Application should follow the existing guidance and requirements for the price control period |