ofgem
Making a positive difference
for energy consumers

Cyber Resilience Investment Document (CRID) template

CRIDs must follow the format below, remain concise with a maximum length of 30 pages (excluding annexes), and focus on information that demonstrates the requirements below. Please remove the guidance text in each section and replace it with the requested content. Supporting documents such as procurement forms or cost benchmarks may be included as an appendix where necessary, but narrative or explanatory text should be incorporated within the CRID. This template should be used for both Defined (PCD) and Uncertain (UIOLI) Investments. The information to include for both investment types is set out in the Cyber Resilience Business Plan Guidance.

Summary table

Table 1: Summary table

Title section	Summary
Name of programme	*[Working title of the programme / project including a unique reference that links back to the CAF principle eg A1 – Cyber Security Board Training. This should align with the name used on the Business Plan Data Table (BPDT).]*
Investment driver	*[eg NIS-R compliance, CAF outcome, cyber risk outside tolerance]* *Provide a high-level overview in this table of the key project driver; where there are multiple drivers, please list them here and explain in more detail later on.]*
Primary CAF contributing outcome	*[eg A1.a Board Direction]*
Secondary CAF contributing outcomes	*[eg A2.b Assurance; E1.a Governance and risk management processes relating to physical security risks]*
Investment category	*[Price Control Deliverable or Use-it-or-lose-it]*

Title section	Summary
Current and target risk level	*[Provide an aggregated, qualitative assessment of this risk level eg Moderate]*
Outputs	*[List the key output(s) to be delivered]*
Delivery year and key milestones	*[The year the project will be completed. If this is a staged project, please provide any interim key delivery milestones.]*
Historic funding interactions	*[Detail all interactive (either as direct named assets, or as portfolios) funding provided to date.* *Please highlight if there have been any deferrals of works.]*
Interactive programmes	*[Please outline any interactions, direct and indirect, with other NIS-R cyber programmes of work or broader network company programmes of work.]*

Table 2: Spend apportionment over the price control period

Spend apportionment within price control (£m)	Year 1 (m)	Year 2 (m)	Year 3 (m)	Year 4 (m)	Year 5 (m)	Total

Needs: part 1 - summary and alignment with business strategy

All programmes must include information on:

- how it supports the organisation to achieve the overall business objectives set out in its ED3 Business Plan, with a clear articulation of the linkage of key cyber risks to wider business risks
- how it supports the organisation's cyber resilience strategy

Needs: part 2 - risk assessment

All programmes must include:

- an overview of the business and cyber risk assessment process and methodology used to identify the current risks facing the company's assets subject to the NIS-R. Including how risks have been prioritised. Risk assessment process and methodology are only required to be submitted once
- how the consequences and impacts for the risks have been derived and are related to the assets in scope of NIS-R
- how the level of cyber risk was calculated, 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 controls are insufficient
- how the companies' risk tolerance affected the response decision
- how the specific project would impact on the inherent, residual and target risk positions as well as how this will be monitored during and after project delivery

To support the risk assessment, DNOs should include an accompanying cyber security risk assessment aligned to our NIS Guidance. We expect this the risk assessment to reflect the risk, at an applicable level, that the DNO is seeking funding to mitigate. This should include:

- the consequences and impacts have been assessed and articulated as part of the rationale for the mitigation activities
- an explanation of how risk mitigation activities will lead to a targeted risk reduction in line with DNOs risk appetite
- acknowledgement and assessment of the impact cyber incidents may have on existing and future energy consumers

Needs: part 3 - options analysis and selection

Each PCD investment programme must include:

- an overview of the range of options identified, evaluated and assessed, with a clear presentation of the preferred option (where the options are limited for the chosen remediation, DNOs should articulate the rationale for presenting a reduced set of options)
- the methodology and/or standards used to identify the options considered and how these were shortlisted
- 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

- for uncertain outputs, network companies should include any feasibility evidence such as research and development output, technical studies, demonstrations, or design work

Delivery

Each PCD investment programme must include:

- the governance structure, including roles, responsibilities and number of resources required
- a resource plan and 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 activities (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
- programme outputs including any specific sub-deliverables (what specific products, solutions and technologies are being targeted for delivery)
- programme plan and timelines, such as a Gantt chart, with defined year on year outputs
- a description of how performance will be monitored, including key performance indicators and alignment with CAF Contributing Outcomes

Costs: part 1 - qualitative explanation of value for money

Each PCD investment programme must include:

- information to justify the allowance requested, including the split between opex and capex
- a demonstration of how programme/project costs have been derived, including any cost benchmarking where available and where efficiencies have been identified
- information on any procurement and tendering processes (and where these have not been untaken competitively, what steps DNOs has taken to determine the efficiency of costs)
- an outline of any cost uncertainties and how this will be managed and/or 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
- explanation of how the programme and/or project costs demonstrates clear value for money for customers

Costs: part 2 - quantitative totex breakdown

Each PCD investment programme must include:

- a breakdown of the costs in the Cyber Resilience BPDT (see the BPDT Guidance for more information on breaking down the costs within the template)
- a proposed PCD for our review, which can be used to track allowances and outputs throughout the price control period, see Table 3

Table 3: Proposed PCDs and costs

Outputs	Delivery Dates	28/29 (£m)	29/30 (£m)	30/31 (£m)	31/32 (£m)	32/33 (£m)	Total (£m)
[Proposed deliverable]	[DD Month YY]	0.00	0.00	0.00	0.00	0.00	0.00