ofgem
Making a positive difference
for energy consumers

NIS Self-Assessment and Improvement Report Template

Publication date:	4th October 2021	**Contact:**	Cyber Security Team
		Team:	Enforcement & Emerging Issues
		Email:	cybersecurityteam@ofgem.gov.uk

Contents

1. Executive Summary

1.1. Ofgem's 'NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain' ("the Guidance") [1] should be used to guide the completion of this template.

1.2. [Provide relevant background and context for the Operator of Essential Service ("OES"); name of legal entity(ies) forming part of the OES,details of essential service OES provides; details of basis for designation as OES[1]. This should be high-level for which further detail can be provided in the Part A Overview & Scope section of this document.]

Self-Assessment & Improvement Approach

1.3. [This should describe how you performed the self-assessment. This should include the stages of an OES's self-assessment methodology. It should include how scope was identified, stakeholders involved, risk methodology used (this will be described further in the Part B Risk Management section of this document) and any engagement with Government agencies such as Ofgem, BEIS, NCSC, or other organisations.]

Risk Assessment Significant Findings

1.4. [Provide a high-level executive view of risks identified and any recommended treatment plans. These can be expanded further down in **Part B Risk Management** section of this document.]

Cyber Assessment Framework Summary

1.5. [Provide a high-level executive view of the major findings against the Cyber Assessment Framework. These can be expanded further down in **Part C Cyber Assessment Framework** section of this document.]

[1] If a 'deemed designation' under Regulation 8(1), please provide details of the threshold the OES satisfies (Reg 8(1)(b) and Schedule 2).

CAF Objective & Principle	High-level Statement
Objective A: Managing security risk	
Principle A1 - Governance	
Principle A2 - Risk management	
Principle A3 - Asset management	
Principle A4 - Supply chain	
Objective B: Protecting against cyber-attack	
Principle B1 - Service protection policies and processes	
Principle B2 - Identity and access control	
Principle B3 - Data security	
Principle B4 - System security	
Principle B5 - Resilient Networks and Systems	
Principle B6 - Staff Awareness and Training	
Objective C: Detecting cyber security events	
Principle C1 - Security monitoring	
Principle C2 - Proactive security event discovery	
Objective D: Minimising the impact of cyber security incidents	
Principle D1 - Response and recovery planning	
Principle D2 - Lessons learned	

2. NIS Reporting Requirements Part A: Overview and Scope

2.1. Use the overview and views below to develop your Executive Summary description here. Use Section 3 **'Part A: Overview & Scope'**[2] from the Guidance document to guide the development of scope.

OES Overview

2.2. [Provide relevant organisational details including legal structure of organisation, license details, any relevant team structures, governance approaches etc[3].]

NIS Scope

Essential Service Viewpoint[4]

2.3. [Provide a viewpoint that describes the essential service the OES provides at a high-level. It should identify the relevant subsector (i.e. downstream gas or electricity), and service-type provided (e.g. generation, transmission, system operation, etc.). This view should also consider the OES's operational role within the respective subsector and identify, where possible, the regions and customers served. In addition any wider aspects that make the OES's essential service important to consumers (e.g. electricity restoration capability) should be detailed. Consider representing by using descriptive text and an overview diagram.]

Functional Viewpoint[5]

2.4. [Provid a breakdown of the OES's essential service into the various functions that enable delivery. It should identify the high-level functions, and the relationships between those functions, to provide an overview of the approach an OES takes to delivering their essential service. Consider representing by using capability taxonomy / mapping diagrams, functional breakdown diagrams, Process flow diagrams].

[2] Part A: Overview and Scope. *The Guidance*, Section 3, Page 13 - 22.
[3] OES Overview. *The Guidance*, Section 3.3, Page 13.
[4] Essential Service Viewpoint. *The Guidance*, Section 3.9, Table 2, Page 15.
[5] Functional Viewpoint. *The Guidance*, Section 3.9, Table 2, Page 16.

System Viewpoint[6]

2.5. [Provide a view that identifies the relevant network and information systems required to deliver the OES's functions and essential service. This view should provide a formal description of the system architecture that is employed by the OES to deliver the essential service and should be aligned to a reference architecture model such as the Purdue Enterprise Reference Architecture. This viewpoint should clearly identify the groups of network and information systems required to deliver the essential service and those that do not - including connectivity across those boundaries. In addition, internal and external access points into the OES's network and information systems should be captured. Consider representing by using system architecture diagrams, network diagrams, asset inventories, zone, and conduit diagrams]

Sites Viewpoint[7]

2.6. [Provide a view that identifies all the relevant sites that are related to the delivery of the essential service. This view should articulate whether any given site belongs to a certain class or type with relevant description. This view should seek to describe the interconnectedness and/or interdependence of sites, for example in a transmission or distribution network, supplemented with other information sources that describe the criticality of sites when considering risks to the provision of essential services. Consider representing by using site inventories and lists, and geographical network diagrams.]

Context Viewpoint[8]

2.7. [Considering the OES and its essential service as an open system that interacts with the broader subsector, provide a view that presents the various external inputs and outputs required to enable the OES to deliver its essential service and function. In terms of inputs, this view should document all dependencies required to enable the provision of the essential service. This could include product or service suppliers; integration, operation and maintenance providers; third party systems and interdependence on other OES or sector participants. In terms of outputs, this view should articulate what the OES contributes to the

[6] Systems Viewpoint. *The Guidance*, Section 3.9, Table 2, Page 16 - 17.
[7] Sites Viewpoint. *The Guidance*, Section 3.9, Table 2, Page 17.
[8] Context Viewpoint. *The Guidance*, Section 3.9, Table 2, Page 17 – 18.

wider subsector; this is likely to link back to the Essential Service view. Consider representing by using 'Black-box' diagram, context diagram, dependency mapping diagram]

3. NIS Reporting Requirement Part B: Risk Management

3.1. Use Section 4 '**Part B: Risk Management**[9]' from the Guidance document to guide the completion of this section.

Risk management process

3.2. [Describe your Risk Management process and how this links into your self-assessment methodology described in the Executive Summary and the scope identified. Describe the risk assessment process including how often and when risk assessments are conducted on the security of the network and information systems within your NIS scope. Describe where these risks are captured and maintained e.g. in a certain application?]

Risk identification, assessment, and prioritisation

Threat identification and assessment

3.3. [List the identified threats to the security of those network and information systems within your NIS scope and how they have been ranked. Detail how the threats were identified.]

Vulnerability identification and assessment

3.4. [Describe how vulnerabilities are identified for those network and information systems within your NIS scope and how they feed into your risk assessment process.]

Impact identification and assessment

3.5. [Describe the impacts of realised threat events.]

Inherent risk

[9] Part B: Risk Management. *The Guidance*, Section 4, Page 23 - 28

3.6. [Describe how inherent risk is calculated e.g., likelihood and impact. Include any matrices used to determine this and relevant descriptors.]

Control identification

3.7. [Describe how controls are identified and applied, and how these feed into your risk calculations. Describe any linkage to the CAF outcomes]

Residual risk

3.8. [Describe how residual risk is calculated. Include any matrices used to determine this and relevant descriptors.]

Risk response

Risk tolerance

3.9. [Describe risk tolerance and appetite levels, and how these were decided.]

Risk treatment and tracking

3.10. [Describe how risks are prioritised for treatment. Define and describe the risk treatment responses. Describe how all risks are reviewed and tracked.]

Risk assessment results

3.11. [The attached spreadsheet sets out the risk information that should be provided. This information presents the risks relating to your essential service and risk response decisions. Use the attached spreadsheet or attach another with the relevant details.]

Risk Assessment Results Template_v1.x

4. NIS Reporting Requirement Part C: NCSC Cyber Assessment Framework

4.1. Use Section 5 **'Part C: NCSC Cyber Assessment Framework'**[10] from the Guidance document to guide the completion of this section.

Gap Analysis with Respect to the CAF Target Profile

4.2. [Describe how you performed a gap analysis process against the CAF and how you link this back to your risk assessment process.]

Identification of Existing Controls

4.3. [How were existing controls identified and verified, and applied to the processes described above.]

Gap Analysis Results

4.4. [For each of the CAF outcomes, provide detail on whether **Achieved, Partially Achieved**, **Not Achieved**, **Not Relevant**, **Not Yet Assessed**. You must provide rationale and evidence for the assessment status of each CAF contributing outcome. Use the attached template[11] to complete your assessment and reattach it.]

NCSC_CAF.xlsx

Target Profile Achievement Date

4.5. The target date for reaching the target profile is [ENTER DATE].

Other Framework Data[12]

[10] Part C: NCSC Cyber Assessment Framework. *The Guidance*, Section 5, Page 29 – 30.
[11] Based on version 3.0 of the NCSC CAF found here www.ncsc.gov.uk/guidance/nis-guidance-collection
[12] Part C: NCSC Cyber Assessment Framework. *The Guidance*, Section 5.6 – 5.7, Page 30.

4.6. [Add in any comparable outcome-based frameworks such as the National Institute of Sandards and Technology (NIST) Cyber Security Framework where appropriate].

5. NIS Reporting Requirement Part D: Improvement Plan

5.1. Use Section 6**. 'Part D: Improvement Plan'**[13] from the Guidance document to guide the completion of this section.

5.2. See attachment for suggested improvement plan and Gantt chart formats.

Improvement Plan Examples_v1.pptx

[13] Part D: Improvement Plan. *The Guidance*, Part 6, Page 31 – 32.

6. NIS Incident Reporting

6.1. See Section 8 **'NIS Incident Reporting'**[14] from the Guidance document for guidance on the completion of this section.

6.2. Please also refer to the relevant Annex of BEIS's Policy Guidance on the Implementation of the Network and Information Systems Regulations [2], for the Incident Reporting Template.

[14] NIS Incident Reporting, *The Guidance*, Section 8, Page 39 – 41.

7. Self-Assessment and Improvement Report Approval

7.1. The NIS Accountable Officer (NAO) and NIS Responsible Officer (NRO) named below confirm that:

- all guidance released by BEIS, NCSC and Ofgem, relating to the NIS Regulations has been circulated and made available to the relevant individuals and third parties involved in the delivery of the essential service.

- the details in this self-assessment have been reviewed and approved by the relevant responsible individuals including the NIS Accountable Officer (NAO) and NIS Responsible Officer (NRO).

NIS Responsible Officer		
Name	**Signature**	**Date**

NIS Accountable Officer		
Name	**Signature**	**Date**

8. References

[1] Office of Gas and Electricity Markets (2021), NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain.

[2] Department for Business, Energy and Industrial Strategy (2018), Security of Network and Information Systems Regulation 2018 Implementation in the Energy Sector for GB (current version), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

A. OES NIS Roles and Responsibilities[15]

Role	Named Contact
CEO	
CIO	
CISO	
NIS Accountable Officer (NAO)	
NIS Responsible Officer (NRO)	
Deputy NIS Responsible Officer (DNRO)	
Cyber Operational Lead	

[15] OES NIS Roles and Responsibilities. *The Guidance,* Section 2, Page 12.