|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| NIS Self-Assessment and Improvement Report Template | | | |
| **Publication date:** | 17 May 2023 | **Contact:** | Cyber Security Team |
| **Team:** | Infrastructure and Security of Supply |
| **Email:** | cybersecurityteam@ofgem.gov.uk |

© Crown copyright 2021

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [**Open Government Licence**](http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/).

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

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**](http://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](mailto:psi@nationalarchives.gsi.gov.uk)

|  |  |  |
| --- | --- | --- |
| Version number | Date Published | Summary of amendments |
| Version 1 | Issued on 4 October 2021, Call for Input only | Not Applicable. |
| Version 2 | 01 April 2022 | Post consultation closure on 01 Dec 2021 with DGE sector incorporating the responses. |
| Version 2 | Issued on 14 Feb 2023, Call for Input only | Section 1, clause 1.3 added; clause 4.4 embedded document updated; Section 5 clause 5.2 embedded document updated;  Section 7, clause 7.1 added. |
| Version 3 | Issued on 28 Apr 2023 | Contents updated; Section 7 updated. |

**Contents**

[1. Executive Summary 5](#_Toc131024318)

[Self-Assessment & Improvement Approach 5](#_Toc131024319)

[Risk Assessment Significant Findings 5](#_Toc131024320)

[Cyber Assessment Framework Summary 6](#_Toc131024321)

[2. NIS Reporting Requirements Part A: Overview and Scope 8](#_Toc131024322)

[OES Overview 8](#_Toc131024323)

[NIS Scope 8](#_Toc131024324)

[Essential Service Viewpoint 8](#_Toc131024325)

[Functional Viewpoint 8](#_Toc131024326)

[System Viewpoint 8](#_Toc131024327)

[Sites Viewpoint 9](#_Toc131024328)

[Dependencies Viewpoint 9](#_Toc131024329)

[3. NIS Reporting Requirement Part B: Risk Management 11](#_Toc131024330)

[Risk management process 11](#_Toc131024331)

[Risk identification, assessment, and prioritisation 11](#_Toc131024332)

[Threat identification and assessment 11](#_Toc131024333)

[Vulnerability identification and assessment 11](#_Toc131024334)

[Impact identification and assessment 11](#_Toc131024335)

[Inherent risk 11](#_Toc131024336)

[Control identification 12](#_Toc131024337)

[Residual risk 12](#_Toc131024338)

[Risk response 12](#_Toc131024339)

[Risk tolerance 12](#_Toc131024340)

[Risk treatment and tracking 12](#_Toc131024341)

[Risk assessment results 12](#_Toc131024342)

[4. NIS Reporting Requirement Part C: NCSC Cyber Assessment Framework 13](#_Toc131024343)

[Gap Analysis with Respect to the CAF Target Profile 13](#_Toc131024344)

[Identification of Existing Controls 13](#_Toc131024345)

[Gap Analysis Results 13](#_Toc131024346)

[Target Profile Achievement Date 13](#_Toc131024347)

[Other Framework Data 14](#_Toc131024348)

[5. NIS Reporting Requirement Part D: Improvement Plan 15](#_Toc131024349)

[6. NIS Incident Reporting 16](#_Toc131024350)

[7. Self-Assessment and Improvement Report Approval 17](#_Toc131024351)

[8. References 19](#_Toc131024352)

[A. OES NIS Roles and Responsibilities 20](#_Toc131024353)

1. Executive Summary
   1. Ofgem’s ‘NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain 2.0’ (“the Guidance”) [1] should be used to guide the completion of this template.
   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]](#footnote-2). This should be high-level for which further detail can be provided in the **Part A Overview & Scope** section of this document.]
   3. [Also provide a statement for each part of report whether a change has been made for any section when compared to the last submission, alternatively please declare the report name and submission date post which no further changes have been made for this current submission for all the following four parts.]

Part A: Overview and Scope Updates –[Declaration statement]

Part B: Risk Management Updates –[Declaration statement]

Part C: NCSC Cyber Assessment Framework Updates –[Declaration statement]

Part D: Improvement Plan Updates –[Declaration statement]

Self-Assessment & Improvement Approach

* 1. [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. [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. [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.]

|  |  |
| --- | --- |
| **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** |  |

1. NIS Reporting Requirements Part A: Overview and Scope
   1. Use the overview and views below to develop your Executive Summary description here. Use Section 3 **‘Part A: Overview & Scope**’ from the Guidance document to guide the development of scope.

OES Overview

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

NIS Scope

Essential Service Viewpoint

* 1. [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

* 1. [Provide 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].

System Viewpoint

* 1. [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, in addition security zones and conduits may also be presented. 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

* 1. [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. Logical groupings may be used to manage situations where large site numbers are present (e.g., presenting a windfarm as a site rather than as a series of individual wind turbine sites, or presenting several thousand pole-mounted transformers more generally rather than listing names and locations for each). Consider representing by using site inventories and lists, and geographical network diagrams.]

Dependencies Viewpoint

* 1. [Considering the OES and its essential service as an open system that interacts with the broader subsector and beyond, this view presents the various external dependencies required to enable the OES to deliver its essential service and functions. 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 services; and interdependence on other OES or sector participants. Consider representing by using ‘Black-box’ diagram, context diagram, dependency mapping diagrams.]

1. NIS Reporting Requirement Part B: Risk Management
   1. Use Section 4 **Part B: Risk Management** from the Guidance document to guide the completion of this section.

Risk management process

* 1. [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

* 1. [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

* 1. [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

* 1. [Describe the impacts of realised threat events.]

Inherent risk

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

Control identification

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

Residual risk

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

Risk response

Risk tolerance

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

Risk treatment and tracking

* 1. [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

* 1. [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.]



1. NIS Reporting Requirement Part C: NCSC Cyber Assessment Framework
   1. Use Section 5 **Part C: NCSC Cyber Assessment Framework’** from the Guidance document to guide the completion of this section.

Gap Analysis with Respect to the CAF Target Profile

* 1. [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

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

Gap Analysis Results

* 1. [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[[2]](#footnote-3) to complete your assessment and reattach it.]



Target Profile Achievement Date

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

Other Framework Data

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

1. NIS Reporting Requirement Part D: Improvement Plan
   1. Use Section 6 **Part D: Improvement Plan** from the Guidance document to guide the completion of this section.
   2. See attachment for suggested improvement plan and Gantt chart formats.



1. NIS Incident Reporting
   1. See Section 8 **NIS Incident Reporting** from the Guidance document for guidance on the completion of this section.
   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.
2. Self-Assessment and Improvement Report Approval
   1. This condition requires the licensee to send to the Authority an annual assurance statement in relation to the NIS Reporting template and sets out the form of that statement.
      1. The OES must by 31 July in each Year starting from 1 April 2023, send to the Authority an assurance statement that NIS Self-Assessment and/or NIS Annual report:

(a) has been approved by resolution of the OES’s board of directors or, where it is appropriate, by the OES’s most relevant senior management body;

(b) is signed by a director of the OES, or, where it has none, by its appropriate senior manager, pursuant to that resolution in sub-paragraph (a);

* 1. The prescribed form for the assurance statement is as follows:
     1. In accordance with the NIS reporting requirements, the Directors of [OES] ("the designated operator”) hereby certify that for NIS Reporting Year YYYY, in their opinion:

(a) the submitted report represents a fair interpretation of the OES’s NIS obligation as shown in the in the OES’s Self-Assessment /Annual Report;

(b) [OES] have met the Basic Profile or commit to Basic Profile attainment by [DD/MM/YYYY] as set out in section 4.5 of this NIS Self-Assessment and Improvement Report submission.

| **Board Member or Director of the OES** | | | |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

* 1. The NIS Responsible Officer (NRO) named below confirms 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 Responsible Officer (NRO).

| **NIS Responsible Officer** | | |
| --- | --- | --- |
| **Name** | **Signature** | **Date** |
|  |  |  |

1. 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>

1. OES NIS Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Named Contact** |
| CEO |  |
| CIO |  |
| CISO |  |
| NIS Responsible Officer (NRO) |  |
| Deputy NIS Responsible Officer (DNRO) |  |
| Cyber Operational Lead (OT) |  |
| Cyber Operational Lead (IT) |  |

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). [↑](#footnote-ref-2)
2. Based on version 3.0 of the NCSC CAF found here www.ncsc.gov.uk/guidance/nis-guidance-collection [↑](#footnote-ref-3)