![ofgem - Making a positive difference for energy consumers]

NIS Annual Report

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

Contents

1. Summary of Changes

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.   **Reporting period:** April [YEAR] to March [YEAR]

1.3.   [Provide an overview of any major changes that will be detailed within this report. For example, if there is an update on scope, state it here at a high level]

2. NIS Reporting Requirment Part A: Overview and Scope Updates[1]

Scope Declaration

2.1.   [Confirm whether i) there have, ii) will be, or iii) have not been a change to scope. Where there has been or will be changes to scope, complete the relevant section below. Otherwise, state N/A for each section.

Scope Change

2.2.   The below section details changes in NIS scope since the last reporting period.

2.3.   [Include changes to scope e.g., from acquisition or merger, sale, addition, decommissioning, descoping. Provide the timelines associated with the change, any impact to compacity, consumers server, rationale for change to scope and any further supporting information.]

NIS Scope

2.4.   [Provide your current NIS scope. You should utilise the essential service, functional, system, site and context viewpoints that were developed for the self-assessment[2]. Include full details of any new or additional network and information systems within the NIS scope.]

[1] Part A: Overview and Scope. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain*, Section 3, Page 13 - 22.
[2] NIS Reporting Requirements Part A: Overview and Scope. NIS Self-Assessment and Improvement Report Template, Section2, Page 7 - 9.

3. NIS Reporting Requirment Part B: Risk Management Updates[3]

Risk Management Process Changes

3.1.   [Confirm whether i) there have or ii) have not been any changes to your Risk Management process as described in your self-assessment or previous annual report. Where there is a change, provide details of what this is, the rationale, and state what the impact has been on previous risk assessments performed.]

Risk Tolerance Level Changes

3.2.   [Confirm whether i) there have or ii) have not been any changes to the risk tolerance levels. Provide details of what these changes are and supporting rationale for these changes and how this impacts any identified risks]

Risk Assessment Results

3.3.   [Confirm whether i) there have or ii) have not been any new risks identified. Where new risks have been identified provide a high-level explanation of these and any recommended treatment plans.]

3.4.   Use the attached spreadsheet to detail the risks relating to the security of the network and information systems on which your essential service relies, together with details of any risk response decisions. This should include newly identified risks and all previously identified risks.]

Risk Assessment
Results Template_v1.x

---

[3]   Part B: Risk Management. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain,* Section 4, Page 23 - 28

4. NIS Reporting Requirment Part C: NCSC Cyber Assessment Framework Updates[4]

Target Profile Achievement Date

4.1.   The original target date for reaching the target profile was [ENTER DATE].

4.2.   We are on track for meeting the target date / The new target date is: [ENTER DATE].

4.3.   The target date has changed because [enter reason for change in date or delete].

CAF Gap Assessment Update

4.4.   [Use the attached to provide an update on your progress against the CAF target profile. Add in a column for each subsequent reporting year.]

CAF Gap Analysis
High Level Results.xls:

Other Framework Data

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

---

[4]   Part C: NCSC Cyber Assessment Framework. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain*, Section 5, Page 29 – 30.

5. NIS Reporting Requirment Part D: Improvement Plan Updates[5]

5.1.   Provide an update on your improvement plan, clearly highlighting any new or additional initiatives that have been identified since the last report.

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

Improvement Plan
Examples_v1.pptx

---

[5] Part D: Improvement Plan. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain*, Section 6, Page 31 – 32.

6. NIS Incident Reporting[6]

6.1.   [Confirm whether i) there have or ii) have not been any NIS incidents since the last reporting period.

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.]

[6] NIS Incident Reporting. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain*, Section 8, Page 39 – 41.

7. Sub-threshold Incident Reporting[7]

7.1.   [Confirm whether i) there have or ii) have not been any sub-threshold NIS incidents since the last reporting period.

7.2.   Provide details of any sub-threshold NIS incident. Sub-threshold NIS incidents are incidents that affect the security of network and information system(s) that in turn affects the delivery of essential services however fall below the reportable thresholds[8].

7.3.   Please also refer to the relevant section of BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [2] for further information.]

---

[7] NIS Self-Assessment. *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain,* Section 7.7, Page 35.
[8] Otherwise known as 'Non-NIS Incidents' within BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations

8. NIS Annual Report Approval

8.1.   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

9. 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. Roles and Responsibilities[9]

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

---

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