NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v2.0

Publication date:	1st April 2022	**Contact:**	Cyber Security Team
		Directorate:	Enforcement & Emerging Issues
		Email:	cybersecurityteam@ofgem.gov.uk

This guidance is for Operators of Essential Services (OES), as defined by the Network and Information Systems Regulations 2018 (NIS Regulations), with undertakings in Downstream Gas and Electricity[1] in Great Britain. This guidance sets a process to assist OES in performing their regulatory duties and in continually managing security and resilience with respect to the network and information systems on which their essential services rely, or which are used for the provision of an essential service. This guidance fulfils the duties of the Gas and Electricity Markets Authority laid out at regulation 3(3) of the NIS Regulations [1] and OES must have regard to this guidance for the purposes of Regulations 10(4) and 11(12) of the NIS Regulations. This guidance is effective from the publication date above until otherwise directed by Ofgem.

[1] Downstream Gas and Electricity refers to those OES providing essential services within the Electricity subsector or the Gas subsector as defined within the NIS Regulations, except for those OES that provide essential services specified in Schedule 2, paragraph 3, sub-paragraphs (5) to (8).

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**. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

1. Introduction

1.1. This guidance is for Operators of Essential Services (OES), as defined by the Network and Information Systems Regulations 2018 (NIS Regulations) [1] with undertakings in the Downstream Gas and Electricity (DGE) subsectors in Great Britain. It may be used as a point of reference by the Office of Gas and Electricity Markets (Ofgem[2]) - in its role as joint Competent Authority (CA) with the Department for Business, Energy and Industrial Strategy (BEIS), under the NIS Regulations. This guidance fulfils the duties of the Gas and Electricity Markets Authority (GEMA) laid out at regulation 3(3) of the NIS Regulations and OES must have regard to this guidance for the purposes of Regulations 10(4) and 11(12) of the NIS Regulations.

1.2. This guidance is intended to be read alongside BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [1], and Ofgem's NIS Enforcement Guidelines. Further details of associated policies and guidance can be found within Appendix **Error! Reference source not found.**.

Background

1.3. The NIS Regulations[3] provide legal measures to maintain and improve the level of security (both cyber and physical resilience[2]) of network and information systems relied upon or used for the provision of essential services. Accountability for compliance with the NIS Regulations lies with the OES. The security duties assigned to OES within the NIS Regulations are detailed in Regulation 10 as follows:

- Regulation 10(1) - An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies. [1]
- Regulation 10(2) - An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services. [1]

[2] Ofgem is the Office of Gas and Electricity Markets. Ofgem is a non-ministerial government department governed by GEMA. GEMA is the body referenced in the NIS Regulations. The terms "Ofgem" and the "Gas and Electricity Markets Authority" are used inter-changeably in this guidance.

[3] Reference to the NIS Regulations is to the Network and Information Systems Regulations 2018 as amended from time to time. This guidance will also be interpreted by Ofgem in accordance with any amendments made to the NIS Regulations from time to time.

- Regulation 10(3) - The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed. [1]
- Regulation 10(4) - OES must have regard to any relevant guidance issued by the relevant CA when carrying out their duties imposed by paragraphs (1) and (2). [1]

1.4. OES also have a duty to notify Ofgem as the designated CA in writing about, any incident which has a significant impact on the continuity of the essential service which the OES provides (a NIS Incident). An "incident" means any event having an actual adverse effect on the security of network and information systems. Further details on incident reporting can be found within Section 7 of this guidance. The incident notification duties assigned to OES within the NIS Regulations are detailed in Regulation 11.

1.5. The first iteration of this guidance was focussed on the initial implementation of the NIS Regulations, specifically around establishing the relationship between the CA and OES community and introducing the concepts of self-assessment, improvement planning and incident reporting. This version supersedes the previous guidance and is issued to support OES with on-going compliance with the NIS Regulations. This document is intended as relevant guidance within the meaning of Regulations 10(4) and 11(12) of the NIS Regulations, though OES should not rely solely on this guidance for the purposes of achieving compliance with their duties under the NIS Regulations.

1.6. The purpose of this guidance is to outline Ofgem's expectations for OES, and it underpins the collaborative engagement approach sought between the CA and OES community to ensure compliance with the NIS Regulations. OES should engage with the CA when interpreting this guidance to seek clarifications and support where needed.

1.7. To encourage effective engagement between the CA and OES, it is expected that this guidance will be circulated and made available to all necessary individuals within the OES's organisation, as well as relevant third parties involved in the delivery of the essential service.

Approach

1.8. To achieve the aims of the NIS Regulations (i.e. securing those network and information systems that are critical to the delivery of essential services), OES are required to actively manage the security and resilience of their network and information systems whilst also demonstrating compliance with the NIS Regulations to Ofgem through reporting and engagement.

1.9. OES should consider the various steps required to achieve and maintain compliance with the NIS Regulations. In general, these relate to the implementation of a management system for security and resilience which:

1. Employs appropriate processes for identifying and managing the scope of the network and information systems that are relied upon or used for the provision of the essential service. This may include, but is not limited to considering: sites, assets, systems, components, interfaces, services, processes, people, and third-party suppliers.
2. Employs appropriate processes for managing risks posed to the security of network and information systems on which an essential service relies or which are used for the provision of the essential service, including those risks that originate from outside of the organisational boundary of an OES as a result of third party dependencies;
3. Actively manages security and resilience during system design and throughout the engineering lifecycle, including by ensuring requirements are considered in the procurement process for products and services.
4. Delivers essential services in a resilient manner, having the capability to detect, respond and recover from network and information system incidents, ensures levels of essential service continuity during an incident, and conducts timely and accurate incident reporting.

1.10. To support the implementation of the NIS Regulations it is expected that OES will have regard to this guidance and BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations, as well as the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) and associated guidance [3], and any other associated policy or technical direction issued by BEIS and/or Ofgem.

1.11. The landscape of security solutions and best practice is constantly evolving. The measures taken by OES in fulfilling their security duties under Regulation 10(1) of the NIS Regulations must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risks posed. Where appropriate, this includes:

- Aligning with recognised industry standards and generally accepted best practice;
- Considering the applicability of any available security solutions across the people, process, and technology domains to manage security risks, and;
- Considering the effectiveness of available security solutions to the network and information systems on which an essential service relies, or which are used for the provision of an essential service (e.g. Operational Technology (OT) environments)

1.12. OES are encouraged to engage with Ofgem, BEIS's industry collaboration teams and the NCSC, to explore options for advice and support.

Reporting

1.13. This guidance sets out an approach to assist OES in reporting their compliance with the NIS Regulations. This reporting should allow for the demonstration of effective security and resilience management in relation to the essential service. Notwithstanding any specific request, it is expected that OES will regularly report to Ofgem the status of their compliance through self-assessment and status reporting at regular intervals[4], in addition to responding to events such as incidents, inspections, or revocations. Further details on compliance reporting can be found within Section 7. In addition, Ofgem has issued a number of templates to support reporting. To encourage consistency, OES are expected to make use of any templates provided when conducting compliance reporting activities.

1.14. The content of OES ongoing reporting is expected to be based on self-assessment and self-improvement. This guidance sets out the expectations for OES in this regard in the form of a four-part set of NIS Reporting Requirements[5], as described below:

[4] Status reporting includes an annual report and an interim 6-monthly report.

[5] These were referred to as the NIS Self-Assessment Parts 1 & 2 in the last version of our guidance but nomenclature has been changed to emphasise that this concept is wider than, and incorporates, the CAF Self-Assessment amongst other things.

- **Part A: Overview & Scope (Section 3)** - This provides a high-level overview of the essential service and the key functions, sites and network and information systems on which the essential service relies, or which are used for the provision of an essential service;
- **Part B: Risk Management (Section 4)** - This describes the security risk management approach, risk information and decisions, including prioritised risks, risk response decisions and associated risk mitigation plans;
- **Part C: NCSC CAF (Section 5)** - The CAF Self-Assessment demonstrates the current and target states of CAF outcomes with supporting evidence that has been assessed using expert judgement;
- **Part D: Improvement Plan (Section 6)** – Improvement planning articulates identified risk mitigations and CAF deficiencies as security and resilience requirements, which are in turn aligned to projects and/or initiatives. These plans can be used to measure progress made by an OES, as well as to set future programmes of work.

1.15. Figure 1, below, highlights the key relationships between the four parts of the NIS Reporting Requirements. The overall premise is that, for a defined scope reflective of the essential service, the identification of intolerable risk and CAF deficiencies against a target profile drive the development of security and resilience requirements. These requirements are then delivered through a programme of work and ongoing security operations. Ongoing assurance activities enable OES to assess whether these requirements have been met and whether the necessary improvements in risk positions or CAF statuses have occurred. The relationships between scoping, risk management, position against the CAF and improvement plans are key when considering whether certain measures are appropriate and proportionate – and hence in determining OES compliance with their regulatory duties.

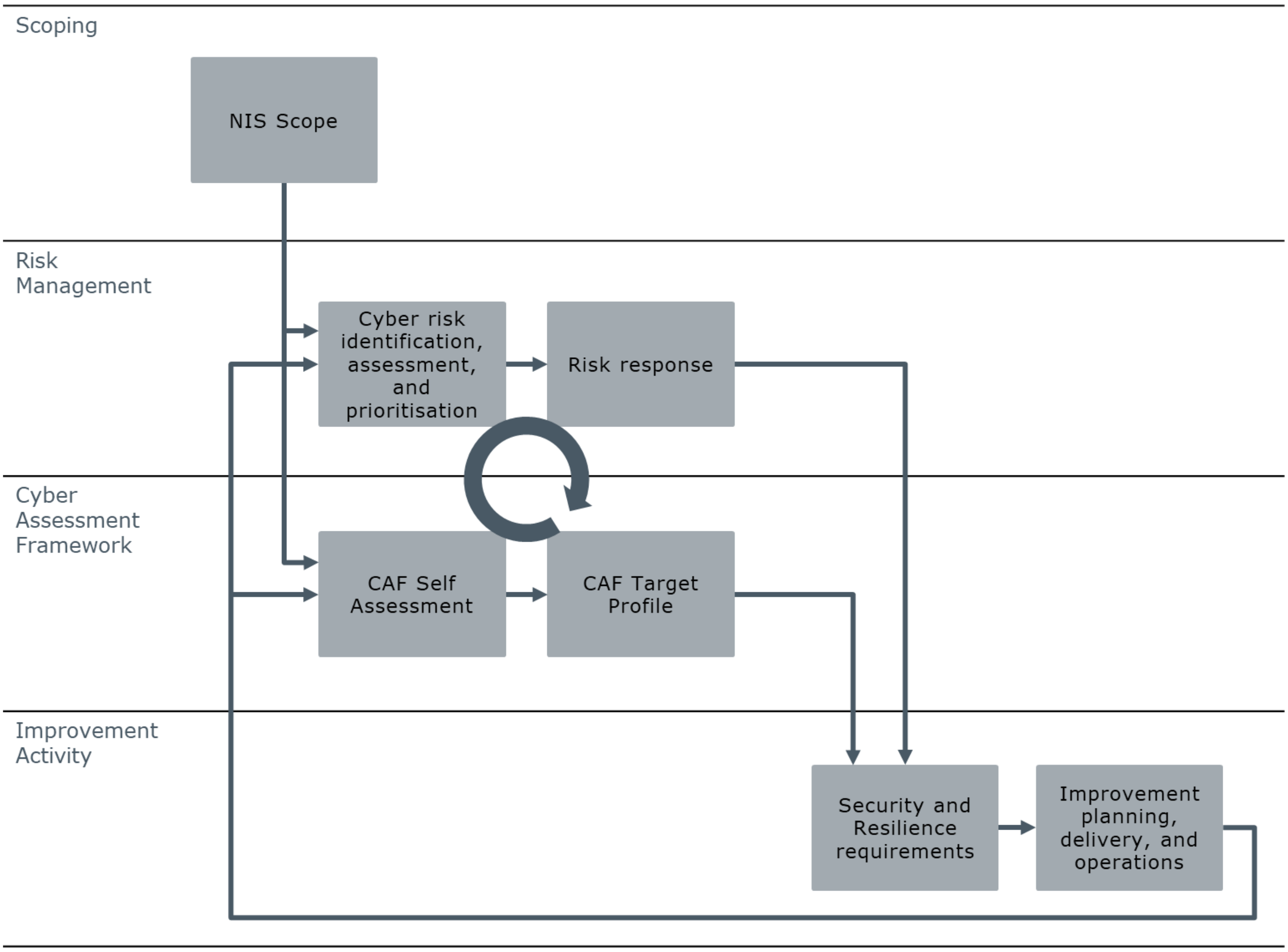

Scoping
NIS Scope
Risk Management
Cyber risk identification, assessment, and prioritisation
Risk response
Cyber Assessment Framework
CAF Self Assessment
CAF Target Profile
Improvement Activity
Security and Resilience requirements
Improvement planning, delivery, and operations

Figure 1: Key relationships between parts A-D of the NIS Reporting Requirements

Information provided by OES

1.16. Ofgem relies on the information submitted by OES as being a true reflection of their status. As such, any information provided to Ofgem must be accurate, reliable, transparent, well evidenced, and delivered in a timely and secure manner. Any information provided to Ofgem, in whatever form, may be used for the purposes of enforcement action, in accordance with Ofgem’s regulatory and statutory duties.

1.17. Ofgem’s receipt of information from OES, or any other party, should not be taken as tacit approval or endorsement of any conduct described therein. In addition, any reviews or associated commentary Ofgem may provide in relation to the same are advisory in nature and do not represent Ofgem’s approval or endorsement of an OES’s conduct, solutions, or decisions, unless expressly stated in writing. Any such reviews or associated commentary are issued without prejudice to Ofgem’s right to take enforcement action should this be considered appropriate.

1.18. Ofgem requests that information provided by OES are made directly to their respective advisor and to Ofgem’s Cyber Security Team mailbox (CyberSecurityTeam@ofgem.gov.uk) via agreed secure communication methods.

Status of this Guidance

1.19. This guidance sets out Ofgem’s interpretation of certain relevant obligations under the NIS Regulations and Ofgem’s expectations associated with the same. It is not a substitute for independent legal advice and each OES is responsible for seeking such legal (or other professional) advice as it considers appropriate to ensure compliance with its obligations.

1.20. This guidance represents Ofgem’s interpretation of current and developing standards for security and resilience predominantly for (but not limited to) OT. It does not cover protection of personal data or intellectual property considerations for OES.

1.21. This guidance may be updated and expanded in future as required, when appropriate and including based on continued partnership and collaboration with industry.

1.22. This document does not provide detailed guidance on security and resilience aspects across the engineering lifecycle, from design, development, factory or site acceptance testing, commissioning, operation, maintenance, decommissioning or disposal.

1.23. OES which are part of the ‘Revenue Using Incentives to deliver Innovation and Outputs’ framework (“RIIO-2”) should have regard to associated guidance, published by Ofgem[6].

[6] https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/network-price-controls-2021-2028-riio-2

2. OES Roles and Responsibilities

2.1. To facilitate engagement between the OES and Ofgem, OES are expected to appoint a NIS Responsible Officer (NRO) and a Deputy NRO, as described in Table 1.

Table 1: OES NIS Roles and Descriptions

Role	Role Description
NIS Responsible Officer (NRO)	The NRO is a single point of contact acting on behalf of the OES to ensure compliance with the NIS Regulations and to facilitate engagement with the CA. The NRO is expected to act as the general liaison for all compliance matters ranging from compliance reporting through to inspections. The NRO is also expected to attest to the accuracy and completeness of all NIS compliance reports. The NRO should be responsible for the security of network and information systems on which the essential service relies.
Deputy NIS Responsible Officer (DNRO)	The DNRO is expected to act as an appropriate deputy to the NRO supporting the fulfilment of the NRO responsibilities and promoting continuity when resource changes occur.

2.2. The NRO and DNRO role holders, and their contact details should be kept up to date, with any changes being submitted in writing to BEIS and Ofgem as soon as reasonably practicable to ensure communication continuity.

2.3. Ofgem's engagement with OES will not be limited to the NRO and DNRO, and OES are free to define additional roles. Ofgem does not require notification of these additional roles on an on-going basis. Additional roles could include persons responsible for the essential service operations, or perhaps a third-party supplier lead. It is expected that an OES will develop a team that is capable of implementing and maintaining a management system for security and resilience, and in order to demonstrate compliance.

2.4. Sections 3 - 6 set out the information required to satisfy the NIS Reporting Requirements introduced in paragraph 1.14, although Ofgem reserves the right to request additional or alternative information.

3. Part A: Overview and Scope

3.1. The following section describes Part A of the NIS Reporting Requirements covering the OES Overview and Scope. The purpose of scoping is to identify those network and information systems on which the essential service relies, or which are used for the provision of an essential service so that subsequent risk, security, and resilience management is framed appropriately.

3.2. In order to support BEIS and Ofgem's engagement with OES regarding the NIS Regulations, it is expected that OES will provide as part of their reporting a comprehensive background and description of the essential service they deliver. This may include the provision of details relating to the organisation, the network and information systems on which the essential service relies, or which are used for the provision of an essential service, its policies and processes, and its personnel, in addition to details on the OES's wider role within the DGE subsectors, and the energy sector as a whole. Details should also be provided on the OES's strategy and approach towards security and resilience.

OES Overview

3.3. Ofgem requires background organisational details of the OES to facilitate effective communications. It is expected that OES should provide an overview of organisational details within Part A of the NIS Reporting Requirements covering aspects such as:

- The legal structure of the OES providing the essential service in Great Britain, including any parent or subsidiary organisations;
- Any relevant Gas or Electricity licence details for any licensable activities related to the essential service; and
- Relevant organisational team and governance structures of those team(s) responsible for the oversight of an OES's duties under NIS Regulations.

NIS Scope

3.4. The NIS Reporting Requirements will require OES to provide details of what essential services, functions, systems, and sites are within the scope of the NIS Regulations. 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

Regulations define what 'network and information systems' and 'essential service' means, and these must be considered when developing the NIS Scope.

3.5. Within the NIS Regulations (Regulation 2(1)), the term 'network and information systems' means:

(a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003 [1];
(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 [1]; or
(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; [1]

3.6. 'Essential service' is defined as a service which is essential for the maintenance of critical societal or economic activities [1]. The essential services within the DGE sector are further set out in Schedule 2 of the NIS Regulations. OES are expected to consider the nature of their services with regard to Regulation 8(1) (with reference to Schedule 2's threshold requirements) to identify the essential services they provide. This is not just a matter of generation or network capacities but also the potential to impact certain numbers of consumers.

3.7. OES should use a consistent approach in defining and maintaining their NIS Scope. It is recommended that OES align to recognised and generally accepted good practice for scoping (e.g. the *approach* presented within 'ISA 62443-3-2 Security Risk Assessment and System Design Standard' to develop the 'System under Consideration', notwithstanding the fact that a NIS Scope may include additional network and information systems than what would typically be included in a 'System under Consideration' which focuses on industrial automation and control systems) [4]). Any scoping decisions must be well documented with an accompanying rationale and assumptions.

3.8. OES may also participate in periodic Critical National Infrastructure (CNI) reviews under existing engagements with BEIS. This requires data returns on both systems and physical assets critical to the delivery of essential functions. There is likely to be overlap in terms of the NIS scope and the network and information systems of the CNI return. BEIS and Ofgem will work closely to avoid any unnecessary duplication of efforts when developing such returns.

Scope viewpoints and mapping

3.9. Identifying the network and information systems on which the essential service relies or which are used for the provision of an essential service is a complex process that needs to consider many facets of how an OES operates. To support OES in explaining their NIS Scope, the NIS Scope should be presented using a series of viewpoints. These viewpoints are set out below and further expanded within Table 2:

- Essential service view;
- Functional view;
- Systems view;
- Site view;
- Dependencies view.

Table 2: NIS Scope Viewpoints

Essential Service Viewpoint	
Description	
This viewpoint 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.	
Purpose	Representation options
• To provide an overview of an OES's essential service and to provide context to subsequent scoping views. • To provide an indication of the operational role the OES plays within its subsector. • To indicate the inherent criticality of the OES.	• Descriptive text • Overview diagram
	Requirements
	• Subsector • Service-type and description • Considerations with regard to Regulation 8(1). Nature of essential service under Schedule 2 and (if relevant) details of which threshold requirements apply. • Geography • Number of customers served

Functional Viewpoint	
Description	
This view provides 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.	
Purpose	Representation options
• To provide an overview of the OES's essential service from a functional perspective. • To support the identification of in-scope network and information systems, and sites within those respective viewpoints. • To provide context to criticality and impact assessments.	• Capability taxonomy/mapping diagram • Functional breakdown diagrams • Process flow diagrams
	Requirements
	• Breakdown of high-level functions enabling the essential service • Description of relationships between functions

Systems Viewpoint	
Description	
This view 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 on which the essential service relies, or which are used for the provision of an essential service and those that are not - including connectivity across those boundaries. In addition, internal and external access points into the OES's network and information systems should be captured.	
Purpose	Representation options
• To provide details of the OES's system architecture. • To identify those network and information systems on which the essential service relies, or which are used for the provision	• System architecture diagrams • Network diagrams • Data flow diagrams • Asset inventories • Zone and conduit diagrams
	Requirements

of the essential service or that could directly impact it if an incident occurred. • To identify the boundary between network and information systems used for the provision of essential services and those that are not.	• Architecture diagram • Includes networks, information systems, and data • NIS scope boundaries and interfaces • Linkage to functional viewpoint

<table>
<tr><th colspan="2">Sites Viewpoint</th></tr>
<tr><th colspan="2">Description</th></tr>
<tr><td colspan="2">This view 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).</td></tr>
<tr><th>Purpose</th><th>Representation options</th></tr>
<tr><td rowspan="3">• To provide an overview of the OES’s physical estate.
• To identify those sites used for the provision of the essential service
• To provide indications of the criticality of certain sites.</td><td>• Site inventories/lists
• Geographic network diagram</td></tr>
<tr><th>Requirements</th></tr>
<tr><td>• Definition and description of site types/classes and their tiers/criticality
• Number of sites per type/class and tier/criticality
• Inter-site relationships</td></tr>
</table>

<table>
<tr><th>Dependencies Viewpoint</th></tr>
<tr><th>Description</th></tr>
<tr><td>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</td></tr>
</table>

product or service suppliers; integration, operation, and maintenance providers; third party systems and services; and interdependence on other OES or sector participants.	
Purpose	Representation options
• To provide details on an OES’s dependence on external products and services when delivering an essential service.	• ‘Black-box’ diagram • Context diagram • Dependency mapping diagram
	Requirements
	• Dependencies required to enable the essential service. • OES position in the sector including where applicable: ○ Relationship ‘downstream’ ○ Relationship ‘upstream’

3.10. OES are expected to map the various viewpoints to provide an understanding of the essential service’s dependency on functions, systems, sites, and the broader relationship with the gas or electricity subsector. Figure 2 highlights a number of viewpoint relationships which should form the basis of any mapping between them.

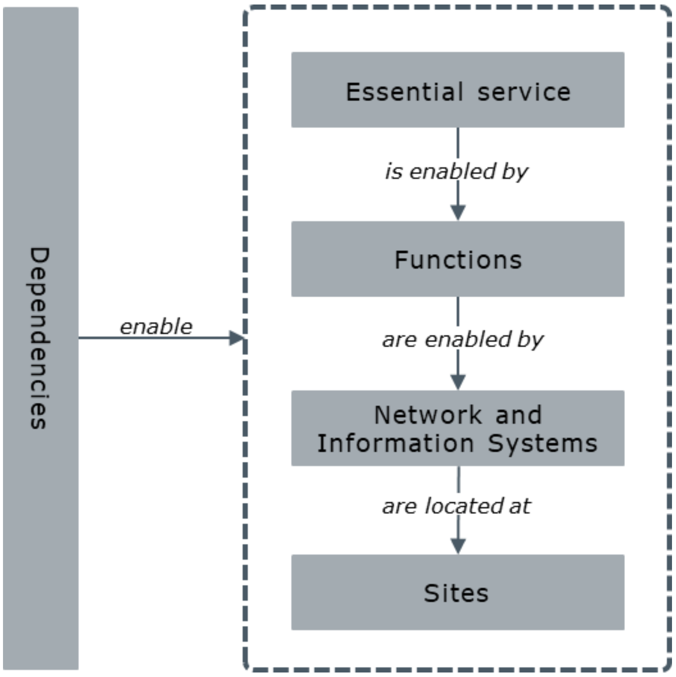


Figure 2: Key relationships between viewpoints

3.11. Two approaches are presented below to illustrate mapping between viewpoints, in particular between the Systems View and the Sites View:

- An OES that operates a large number of sites (e.g. a network operator) is not expected to provide a detailed system description of each of those sites, though the Systems View should capture key site-types. For example, a network operator that uses variants of substations based on vendor or technology-type may choose to capture these variances within a single Systems View with subsequent mapping to the Sites View with site-specific information.
- A generation OES may choose to develop several Systems Views to account for the variances across a fleet of power stations. These would then have subsequent mapping with the Sites View which covers aspects such as criticality.

Scope principles

3.12. The following principles are expected to be followed by OES when identifying their NIS Scope:

- Any network and information system must be included in the NIS Scope if the system, sites and network and information systems on which the essential service relies, or which are used for the provision of an essential service.
- Any network or information system must be included in the NIS Scope if the system could suffer an incident that would result in a significant impact on the continuity of the essential service which the OES provides.
- Network and information systems that are not owned or operated by an OES may nevertheless pose risks to the essential service that the OES provides. Third party dependencies on which the essential service relies, or which are used for the provision of an essential service must be identified within the NIS Scope.
- Network and information systems which only temporarily connect to an OES's networks must still be in the NIS Scope if they enable the provision of the essential service that the OES provides or if they could suffer an incident that results in a significant impact on the continuity of the essential service which the OES provides.
- Network and information systems related to maintenance, integration, security, or similar activity, that might not necessarily be required during immediate

essential service operations but are required for the long-term provision of the essential service, should be included within the NIS Scope.

- For those OES that are designated as a result of exceeding a cumulative or total capacity threshold requirement under Schedule 2 of the NIS Regulations, all sites and systems relevant to meeting said threshold requirement should be detailed within the NIS Scope.
- OES must not use the incident reporting thresholds, that they are to have regard to when notifying incidents under Regulation 11, when defining the functions, sites or network and information systems within their NIS Scope.

Scope examples

3.13. Examples of the types of network and information systems that are likely to support the provision of an essential service are presented below. This is not an exhaustive list, but indicates the types of systems an OES may consider a part of the NIS Scope:

- Operations management systems;
- Supervisory control and data acquisition systems (SCADA);
- Distributed control system (DCS);
- Local controllers (e.g. programmable and electronic controllers);
- Safety instrumented systems (SIS) and safety-related systems;
- Protection systems;
- Intelligent electronic devices;
- Remote terminal units (RTUs);
- Physical plant and sensing equipment;
- Data centre and cloud systems (e.g. cloud SCADA);
- Demand management and balancing systems;
- Real Time Operation Systems;
- Critical communications including wireless networks; and
- IT Systems deemed critical by the business for the delivery of essential services.

3.14. Examples of ancillary systems that may be in scope include:

- Utility systems (e.g. Heating, Ventilation, and Air Conditioning (HVAC); Power supply; chilled water, Instrumentation air, etc.);
- Trading systems and interfaces;
- Backup control centres;
- Backup systems;
- Remote access solutions;
- OT configuration management;
- Change management systems;
- OT asset management systems;
- Cloud/on premise-based monitoring or management systems;
- Building management systems; and
- Physical and cyber security systems.

3.15. When considering the NIS scope, OES should have regard to all functions, sites and network and information systems on which the essential service relies, or which are used for the provision of an essential service;

This may include functions related to:

- Physical process controls;
- Operational control and monitoring;
- Operational preparation, planning and management;
- Relevant business planning, maintenance and logistics;
- Operational confidence and assurance (including safety and security);
- Environmental protection; and
- Business policy and regulatory compliance.

Scope boundaries and interfaces

3.16. Network and information systems that the OES owns, operates, maintains, or has some level of involvement with and that are deemed to be out of the NIS Scope should be identified if they:

- interface with the network and information systems on which the essential service relies, or which are used for the provision of an essential service, or;
- interface with network and information systems that could otherwise suffer an incident that results in a significant impact on the continuity of the essential service which the OES provides.

3.17. These network and information systems should be included within scope descriptions or diagrams (e.g. the Scope Viewpoints) with necessary use of boundaries, interfaces, and system groupings to illustrate these cases.

4. Part B: Risk Management

4.1. The following section describes Part B of the NIS Reporting Requirements covering Risk Management.

4.2. Effective risk management supports decision-makers in determining what actions should be taken in response to risks that an organisation, or stakeholder group such as consumers, is exposed to. The process of risk management requires the analysis of many information sources ranging from potentially harmful scenarios and their likelihood and impacts, through to the security and resilience controls that are deployed or planned to be deployed across a system. For the purposes of this guidance, three key constructs are defined with the aim of supporting OES to communicate risk, security, and resilience with Ofgem. These are:

- Risk: Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;[7] [1]
- Security and resilience outcomes: The overarching result of an OES delivering security and resilience improvements. This is typically described within the CAF. (e.g. a risk management outcome could be described as effective management of risks posed to the essential service); and
- Security and resilience outputs: The description of specific details related to security and resilience controls, that lead to tangible changes. This is typically described within a security control framework or through requirements. (e.g. for the risk management outcome above, outputs could include: risk methodology selected, risk assessment conducted, risk response decisions made with seniors etc.).

4.3. Ofgem does not mandate the use of any specific methodology for risk management. However, OES must use a consistent risk management methodology that covers the entirety of their NIS scope. OES must explain their risk management methodology and should align to industry good practice and risk management standards where practicable. Example risk management standards include, but are not limited to, the ISA 62443-3-2 Security Risk Assessment and System Design standard [4], National Institute of Standards and Technology's (NIST) Risk Management Framework [5], ISO27005 [6] and Information

[7] Regulation 1(2) of the NIS Regulations.

Security Forum's IRAM2 methodology [7]. In addition to the standards detailed above, OES are encouraged to consider the risk management guidance published by the NCSC [8]. For the purposes of this guidance, risk management has been broken into two areas common amongst many risk management standards: identifying, assessing and prioritising risk; and responding to risk.

4.4. OES must implement a system for the management of security and resilience (often known as a security management system or similar) in order to facilitate effective risk management decisions and risk responses. This management system must be sponsored by someone suitably accountable for such risks within the OES's organisation, and formalised through policy. The system must articulate an operating model for security and resilience covering people, process, and technology. The performance of the management system must be periodically assessed, making use of key performance indicators, with appropriate improvements made to rectify any issues.

Risk identification, assessment, and prioritisation

4.5. Identifying, assessing and prioritising risk is fundamental to an OES's ability to make risk-based decisions regarding security and resilience. Although Ofgem does not mandate a specific risk management methodology, it is expected that OES will ensure:

- Security risks to specific network and information systems on which the essential service relies, or which are used for the provision of an essential service are identified and described in terms of threat or hazard, vulnerability, and consequence;
- Security risks are assessed based on some combination of threat/ hazard, vulnerability and consequence, generally in terms of likelihood and impact, or similar;
- 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;
- 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);
- Security risks are prioritised based on the severity of residual risk positions;

- Security risks are fed into wider enterprise risk management processes and governance structures; and
- An accurate risk register is maintained and communicated to stakeholders and relevant third parties who are engaged in the delivery of essential services. In addition, all risks must have an assigned owner at a suitable level of seniority with a record of ownership and risk response decisions.

Identifying risk

4.6. OES should consider all relevant threats and hazards that could lead to a reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems. Regarding threats, OES should consider a broad threat landscape including un-targeted and targeted attacks by actors employing commodity and bespoke capabilities across all stages of a cyber-attack (i.e. Survey, Delivery, Breach, Affect) [11].

4.7. OES should monitor and act upon credible emerging threat and vulnerability intelligence, and wider resiliency considerations when assessing risk and must take appropriate and proportionate action to mitigate against potential threats or resilience issues materialising if it is prudent to do so. OES must document and communicate to Ofgem any changes to improvement plans as a result of emerging risks.

4.8. When identifying risks associated with deployed or field-based sites or assets, OES may adopt a representative sampling approach to conduct their investigations. Any representative sampling approaches must be documented with rationale as to why any given sample is sufficiently representative of a wider body of sites or systems.

Describing risk

4.9. Risks need to be sufficiently detailed as to allow them to be assessed and for risk response decisions to be made. As previously stated, risks must be related to network and information systems that enable the delivery of the essential service and should be described in terms of threat/hazard, vulnerability, and impact (or similar). Referring to NCSC guidance on risk management these terms could be defined as follows:

Impact - the consequences or harm of a risk being realised. [8]

Vulnerability - the weakness within a system that if exploited could enable an impact to be realised. [8]

Threat - the individual, group, or circumstance which causes a given impact to occur. [8]

Asset - 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 Regulations [1].

4.10. The following risk statements provide examples of the level of detail that should be captured. These risks are illustrative only and do not reflect known risks to OES.

> There is a risk that the delivery of malware to a **control system's workstation**, as a result of poor physical security and lack of removable media controls, leads to denial of centralised control and monitoring of distribution services, and ultimately the need to deploy personnel to substations to conduct local control. Leading to minor service disruptions whilst local control is implemented.
>
> There is a risk that compromised **controllers** procured through the supply chain are deployed to various substations as a result of poor supplier vetting and hardware security testing, leads to a coordinated incident where sporadic shutdowns/restarts of controllers trigger the activation of substation protection systems, leading to wider network instability and ultimate loss of service to consumers.
>
> There is a risk that poor security awareness leads an authorised employee to accidently reveal a **control system's** credentials to an adversary through a phishing or watering hole attack. This results in the bypass of authentication controls and direct access to control systems of which presence is maintained to gather further information.

4.11. When considering hazard-driven risks, the above can be tailored to meet the specifics of the types of hazards and the types of perceived resilience issues that may occur.

4.12. It is appreciated that when assessing risk, it is often difficult to assign individual risk components to one another and that in many instances the mapping of risk components involves many-to-many relationships (e.g. a certain threat event or vulnerability may apply to several assets). Where required, OES should map risk components (e.g. list threat and vulnerability combinations for an asset within a table), as well as additional means such as attack paths or bow-tie diagrams to support risk descriptions.

Risk response

4.13. Once an understanding of priority risks has been developed, risk response decisions must be made to identify appropriate and proportionate measures to be taken. It is expected that OES will ensure:

- Risk tolerance is defined to a suitable level of detail as to allow risk response decisions to be made, and that these tolerances are regularly reviewed in the light of organisational change;
- Risk response types are defined (e.g. Avoid, Mitigate, Accept, Transfer) and that the measures that drive selection of any given risk response are explained;
- 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;
- All risk responses must be considered over both the short and long term with appropriate and proportionate measures taken to manage risk at all times. Risks that are due to be mitigated over the longer term through strategic-level interventions must also have an accompanying risk response over the short-term. Short-term risk mitigation could be achieved through compensating controls such as manual processes, enhanced security operations, or temporary risk acceptance;
- Risk response decisions that identify the need to reduce risk through security and resilience enhancements (e.g. mitigate) must document the relevant outcomes and outputs needed to achieve such a reduction. Outcomes must be considered in the context of the CAF, whilst outputs should be considered in the context of any adopted security control frameworks. This is discussed further in Section 5. Outcome and output objectives must be articulated within improvement planning and where relevant articulated as requirements which are assigned to projects or initiatives. This is discussed further in Section 6.
- OES should consider relevant guidance regarding security and the sector when planning risk reduction activity as these provide details on how industrial automation and control systems should be designed, built, operated, and managed on a continuous basis. In addition to NCSC CAF Guidance [3], relevant other guidance includes, but is not limited to, ISO 27019 [9], the ISA 62443 standards [4] and the NIST 800-82 [10] controls set.

- OES must assess and assure ongoing delivery results in expected risk reduction, and risks must be monitored regularly for change.

Managing sector-level risk

4.14. OES within DGE form part of a complex system-of-systems which is composed of other OES and sector participants. NIS Incidents may affect numerous OES or sector participants through mechanisms such as cascading impact, the exploitation of common dependencies, or coordinated threat activity. OES are expected to ensure that:

- The impact of realised risks to essential services are identified, and that any potential disruptions that may occur as a result of incidents to essential service dependencies are also captured. OES should where possible articulate the potential impact on consumers.
- OES must consider any identified risks that originate from beyond their organisational boundary yet could still affect the delivery of their essential services. In addition, risks that are identified or assessed via an external party including BEIS, Ofgem, NCSC, or other relevant stakeholder such as suppliers or other OES, must also be considered.

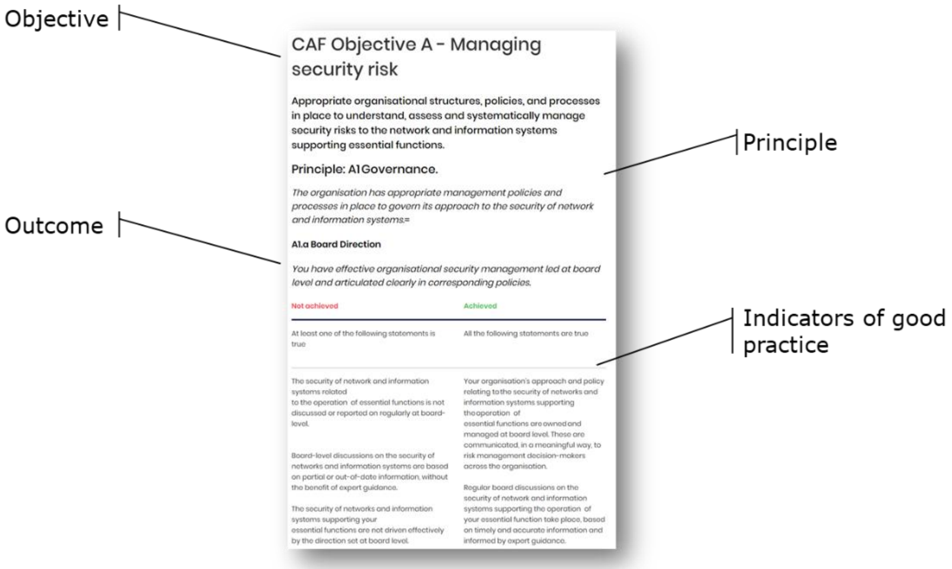
4.15. In addition to OES tolerance-based decision-making on risk, an OES is expected to actively engage with any relevant parties such as those within the supply chain or other OES to ensure that risks that span or originate externally to their organisational boundary are identified and understood.

4.16. Considering the interconnected and interdependent nature of participants within the DGE subsectors it may become apparent, for this reason or similar, that some form of coordinated effort to manage risks to essential services is of benefit to OES. In these instances, OES must have regard to:

- Any policy or technical guidance, referenced or issued by BEIS, Ofgem, or NCSC;
- Any CAF target profiles issued by BEIS and Ofgem;
- Any proposed risk appetite statements/limits, or frameworks to develop such understanding, made and/or cascaded by BEIS and Ofgem.

5. Part C: NCSC Cyber Assessment Framework

5.1. The NCSC have developed the CAF guidance collection [3] which is composed of 14 security and resilience principles, associated guidance, and the assessment framework itself. Distributed across four overarching objectives, the CAF's 14 security and resilience principles are broken down into 39 contributing outcomes. The contributing outcomes are further explained by associated indicators of good practice (IGPs).



CAF Objective A - Managing security risk

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

Principle: A1Governance.

The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.=

A1.a Board Direction

You have effective organisational security management led at board level and articulated clearly in corresponding policies.

Not achieved	Achieved
At least one of the following statements is true	All the following statements are true
The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level.	Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.
Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.	Regular board discussions on the security of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.
The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level.	

Figure 3: Illustration of CAF terms

5.2. Within Part C of the NIS Reporting Requirements, OES are expected to conduct and maintain an accurate positional report against the CAF. OES must have regard to the guidance issued by NCSC when conducting these assessments. OES must also consider relevant NCSC guidance to inform which security and resilience changes to make, and how to make them.

5.3. When conducting an assessment against the CAF, an OES must assess the 39 contributing outcomes and assign one of the following statuses:

- Achieved;
- Partially Achieved[8];
- Not achieved;
- Not relevant, or;

[8] The following CAF outcomes cannot be assessed as partially achieved as per CAF guidance: A1.a, A1.b, A1.c, A2.b, A3.a, B3.e, C2.a, C2.b, D1.b, D1.c, D2.a, and D2.b

- Not yet assessed.

5.4. OES must be able to provide rationale and evidence for the assessed status of each CAF contributing outcome. For CAF outcomes assessed as either 'Achieved', 'Partially Achieved', or 'Not Achieved', an OES must provide rationale as to how their existing security and resilience capability is deemed to meet any of those statuses. For CAF outcomes assessed as 'Not required' or 'Not yet assessed', an OES must provide rationale as to why these are exceptions and/or when they are due for assessment.

5.5. Regarding the assessment of a CAF outcome's status, the CAF's IGPs can be used to support this, but these cannot replace the use of expert judgement when making such assessments. Therefore, OES must use expert judgement to assess the status of any given CAF outcome. Expert judgement should be made by suitably qualified and experienced personnel within the security discipline and subsector domains. Expert judgement should also be informed by relevant guidance, standards, frameworks and/or methodologies.

5.6. OES that have adopted comparable outcome-based frameworks such as the NIST Cyber Security Framework may also present these views or map these to the CAF. However, it does not remove the requirement to assess the CAF outcomes and assign a status.

5.7. OES that have adopted security control frameworks (i.e. output-based frameworks such as ISO27001 [12] or NIST 800-53 [13]) may wish to present the mapping of security controls to CAF outcomes as part of their rationale. The use of security controls with mapping to the CAF can often provide better linkages between the CAF and risk mitigation which supports an OES's demonstration of compliance under regulation 10(1).

5.8. OES must develop and maintain a comprehensive CAF assessment covering the overall delivery of the essential service. Thereafter, OES may choose to develop any number of supporting CAF assessments for different types of asset or site for their own assessment and management purposes. OES should communicate with Ofgem any methodologies used for aggregating supporting CAF assessments into their overarching OES-level CAF assessment.

5.9. NCSC, BEIS or Ofgem may seek to introduce new security principles, from time to time, that may sit within the CAF itself or separately, depending on whether the related measures pertain to cyber or non-cyber.

6. Part D: Improvement Plan

6.1. Part D of the NIS Reporting Requirements covers any planned changes an OES expects to make in response to their risks in the form of security and resilience changes. An OES must consider both risk management decisions and CAF target profile deficiencies in order to identify any security or resilience outcomes that are required to be met. Security and resilience outcomes may then be broken down into outputs and/or requirements that are met through a programme of work and ongoing security operations.

6.2. OES must develop and maintain improvement plans ensuring that activity is prioritised based on minimising risks above tolerance levels or rectifying CAF target profile deficiencies.

6.3. Improvement plans should include:

- Project and initiative delivery details such as project/initiative name, project objectives, delivery approach, timelines and any other relevant information;
- Relevant linkages to risks and CAF outcomes;
- Articulation of specific outputs or controls that are being sought for implementation;
- Assurance criteria and approach to ensure desired changes have been attained through delivery and;
- Depending on delivery approach (e.g. waterfall, agile), summary of key project delivery information.

6.4. OES must regularly track progress and maintain, as a minimum, the following within their Improvement Plan:

- Progress against previously stated milestones, objectives, and delivery timelines;
- A view of newly implemented security and resilience controls;
- Assurance outputs, in particular related to attainment of CAF outcomes and overall risk reduction in line with OES risk tolerances.

6.5. To minimise reporting overheads, Ofgem may grant an OES an exception from reporting information associated with Part D: NIS Improvement Plan. An exception may be granted when an OES is also subject to RIIO Price Control Deliverable (PCD) reporting requirements and relevant details that would be included within Part D reporting is already presented, or expected to be presented, within a referencable PCD report or similar RIIO report.

7. Compliance Reporting

7.1. This section introduces the approach towards reporting compliance with the NIS Regulations. Table 3 introduces the various types of report, content descriptions for those reports and the triggers for submission to Ofgem. The subsequent sub-sections provide an illustrative reporting schedule and also details the expected structure and content of such reports.

Table 3: Compliance report types

Report name	Description	Template reference	Submission timings/triggers
NIS Self-Assessment and Improvement Report	The NIS Self-Assessment and Improvement Report contains details of the OES's organisation, scope, risks, current security and resilience, and the programme of work to maintain, operate, and/or enhance security and resilience. This report will be based on the NIS Reporting Requirements covering: Overview and Scope, Risk Management, NCSC CAF Assessment, and Improvement Plan.	Self-Assessment and Improvement Report Template	Once, when an OES is designated or at specific points in time as a result of major change (e.g. significant scope change, new risk approach adopted), or as directed by Ofgem.
NIS Annual Report	The NIS Annual Report is a report summarising the previous year's changes, current CAF and risk status. This report will also be based on the four-part NIS Reporting Requirements.	NIS Annual Report Template	Annually, by the end of July covering the reporting period of the previous financial year (i.e. for a report due in year 't', the reporting period will be April in year 't-1' to March in year 't').
NIS Check-in Report	The NIS Check-in Report will cover updates, changes, and key issues regarding an OES's NIS activity, in particular regarding administrative, scope, CAF, and improvement plan delivery. This report will cover the first 6 months of the financial year.	NIS Check-in Report Template	Annually, by the end of January covering the reporting period of the previous April to September
NIS Incident Notification Report	The NIS Incident Notification Report details the nature of an incident and is used by OES to comply with their duty to notify NIS Incidents (Reg. 11).	Found within Annex E of BEIS's Policy Guidance [14]	To be provided without due delay and in any event no later than 72 hours after the OES is aware that a NIS incident has occurred

Report name	Description	Template reference	Submission timings/triggers
NIS Incident Handling Report	The NIS Incident Handling Report details an OES's handling of a NIS Incident.	None	A report within 30 calendar days of the initial NIS Incident notification, and subsequently every 30 calendar days thereafter until Ofgem deems further reports are not required
OES Revocation Report	A report detailing any relevant details (e.g. the transition of a site to another OES, or decommissioning of a site) on the incumbent OES's scope.	None	Once, when an OES designation is revoked.

7.2. In terms of reporting scope, OES should report on each essential service they deliver. For example, an OES which delivers two essential service types (e.g. electricity transmission and distribution) must report separately for those services. This also extends to situations where the essential service lines may be the same, but the service is delivered by significantly different means (e.g. Renewable generation and Thermal generation under the electricity supply essential service line).

7.3. All OES-produced reports will be used to facilitate collaborative engagement between Ofgem and OES for the purposes of advisory and compliance support, in addition to feeding into inspections, and enforcement activities if required.

7.4. It is the responsibility of the OES to inform Ofgem at the earliest possible opportunity, should any issues arise in being able to comply with the expected schedules or structures for reporting.

Compliance reporting timelines

7.5. Annual reports and Quarterly Check-in Reports form the core of regular reporting for OES. Figure presents the reporting periods and submission deadlines for each.

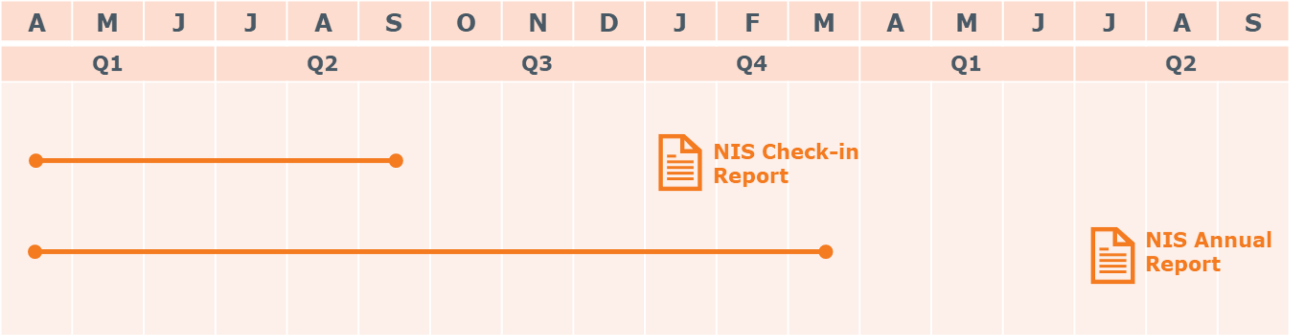


Figure 4: Illustration of reporting periods and submission deadlines for the NIS Annual Report and NIS Check-in Report

NIS Self-Assessment and Improvement Report

7.6. The NIS Self-Assessment and Improvement Report contains details of the OES organisation; the essential service scope; the risk position and risk response decisions; current and target state for security and resilience; and the programme of work to maintain, operate, and enhance security and resilience. This report is primarily based on the NIS Reporting Requirements comprised of the following four parts:

- **Part A: Overview & Scope (Section 3)** - This provides a high-level overview of the essential service and the key functions, sites and network and information systems that provision an essential service;
- **Part B: Risk Management (Section 4)** - This describes the security risk management approach, risk information and decisions, including prioritised risks, risk response decisions and associated risk mitigation plans;
- **Part C: NCSC CAF (Section 5)** - The CAF Self-Assessment demonstrates the current and target states of CAF outcomes with supporting evidence that has been assessed using expert judgement;
- **Part D: Improvement Plan (Section 6)** – Improvement planning articulates identified risk mitigations and CAF deficiencies as security and resilience requirements, which are in turn aligned to projects and/or initiatives. These plans can be used to measure progress made by an OES, as well as to set future programmes of work.

7.7. In addition to parts A-D, OES must also provide a summary of NIS Incidents that have occurred since the previous self-assessment or annual report or, if newly designated, any incidents occurring since designation. NIS Incidents are discussed further in Section 8.

7.8. An OES should perform a new set of assessments under the NIS Reporting Requirements under the following circumstances:

- a newly designated OES must comply with the NIS Reporting Requirements by submitting a NIS Self-Assessment and Improvement Report within 6 months of falling within the requirements set out in Regulation 8(1) or designation by BEIS under Regulation 8(5).
- a significant change occurs that affects the accuracy of an assessment under the existing NIS Reporting Requirements (for example, but not limited to; (e.g. significant scope change, new risk approach adopted etc.);
- at the request of Ofgem.

7.9. OES are encouraged to engage with Ofgem when developing a NIS Self-Assessment and Improvement plan Report.

7.10. Established OES (i.e. those OES that have previously carried out an assessment against the NIS Reporting Requirements or previous self-assessments), must indicate progress made against previous submissions.

7.11. The NIS Self-Assessment and Improvement Report must be signed off by the NRO.

NIS Annual Report

7.12. The Annual Report summarises the previous year's progress and compliance with the NIS Regulations. The Annual Report covers the same topics as the NIS Self-Assessment and Improvement Report and as such will be based on the NIS Reporting Requirements parts A-D.

7.13. Within the Annual Report, OES must maintain and attest the accuracy of their NIS Reporting Requirements parts A-D by providing updates on changes that have occurred in the previous year. It is intended that all required information to complete an Annual Report will be readily available to OES through their risk management, programme delivery and assurance processes. A full re-assessment is not expected to be required.

7.14. The Annual Report must also contain details of in-year NIS Incidents.

7.15. The Annual Report must be signed off by the NRO.

NIS Check-in Report

7.16. The NIS Check-in Report summarises changes and key issues regarding OES NIS compliance activity, in particular regarding administrative changes, scope changes, and improvement plan delivery. The NIS Check-in Report should include:

- **Administrative changes** - OES should declare any changes to administrative responsibilities (e.g. designated sign-off staff, security team structure).
- **Scope changes** - OES should declare and confirm any and all changes to the NIS scope. If there is a reduction or de-scoping, justifications are to be detailed. Decommissioning of an asset which is in-scope must still be reported upon with details of the decommissioning and risk exposure changes to the essential service documented.
- **Improvement plan progress** - OES must identify and report on NIS Improvement Plan progress against identified milestones and security and resilience requirements. Plan changes (e.g. delays, delivery changes) must articulate the potential impact on the delivery of improvements and how this may affect the risk status and/or CAF status. OES should include relevant rationale for improvement plan timelines such as scheduled outages related to the scope.
- **Indicative risk reduction, and CAF changes** – As an OES delivers their improvement plans, it may be that, through cyber risk management, programme delivery or assurance processes, an indicative risk reduction or CAF change has occurred. In these instances, OES should report on the indicative risk reduction or security and resilience changes that have occurred.
- **Incidents:** – OES should provide an update on any NIS Incidents.

7.17. NIS Check-in Reports must be signed off by the NRO.

NIS Incident Notification and Handling Reports

7.18. OES have a duty to notify NIS Incidents to comply with duties set out under NIS Regulation 11. Section 7 provides further details on the NIS Incident reporting process and references to relevant templates used in these instances.

7.19. In addition to NIS Incident reporting, OES should produce a NIS Incident Handling Report within 30 calendar days of the initial NIS Incident notification, and subsequently every 30 calendar days thereafter until Ofgem deems further reports are not required. Section 7 also provides further details on NIS Incident Handling Reports.

OES Revocation Reports

7.20. If an OES designation is planned to be revoked, the incumbent OES must produce a report detailing their essential service scope, what is occurring to their assets post revocation (e.g. decommissioning, transfer to another organisation etc.) including any relevant processes and/or parties involved, and any wider considerations on security risk (e.g. decommissioned site that maintains wider connectivity to other operators) that Ofgem should reasonably be made aware of.

8. NIS Incident Reporting

8.1. A NIS Incident is any incident which has a significant impact on the continuity of the essential service which that OES provides, where an "incident" means any event having an actual adverse effect on the security of network and information systems [1]. NIS Incident guidance is set out in BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [14]. The thresholds presented within BEIS's guidance are not intended to override the regulatory provisions and an OES must make use of its judgement to determine whether a NIS Incident should be reported in line with the NIS Regulations.

8.2. Effective incident reporting is not only an important compliance requirement, but it is also invaluable to:

- Build an understanding of the threats and hazards affecting the sector and provide early warning;
- Enable timely cross-sector advice where appropriate;
- Support specific law enforcement responses where required, and;
- Provide historical context when performing risk assessments in future.

8.3. OES should respond to NIS Incidents as per their incident response and business continuity policies and procedures. In addition to the mandatory reporting required by the NIS Regulations, OES responses may also include the reporting of NIS Incidents to relevant Government authorities and agencies on a voluntary basis as set out within BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [14].

8.4. Reporting an ongoing NIS Incident to Ofgem will have no impact on how the response process is managed within Government. OES are encouraged to seek support from the NCSC as the NIS Computer Security Incident Response Team (CSIRT) as soon as practicably possible after a NIS Incident is detected and report to BEIS through voluntary reporting channels.

8.5. OES should contact all relevant Government departments during or upon the discovery of a NIS Incident. Appendix A provides key contact details for BEIS, Ofgem and NCSC.

8.6. Notification of a NIS Incident to Ofgem does not relieve an OES from any other obligations or responsibilities it may have to notify incidents to Ofgem or to any other parties (e.g. notifying the duty officer of an outage).

NIS Incident Reporting to Ofgem

8.7. This section sets out the NIS Incident Reporting and Investigation Process (see Figure 3) of which step 1 (i.e. NIS Incident Notification Report) is used to satisfy the mandatory NIS Incident notification requirements detailed within BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [14] and Regulation 11 of the NIS Regulations [1].

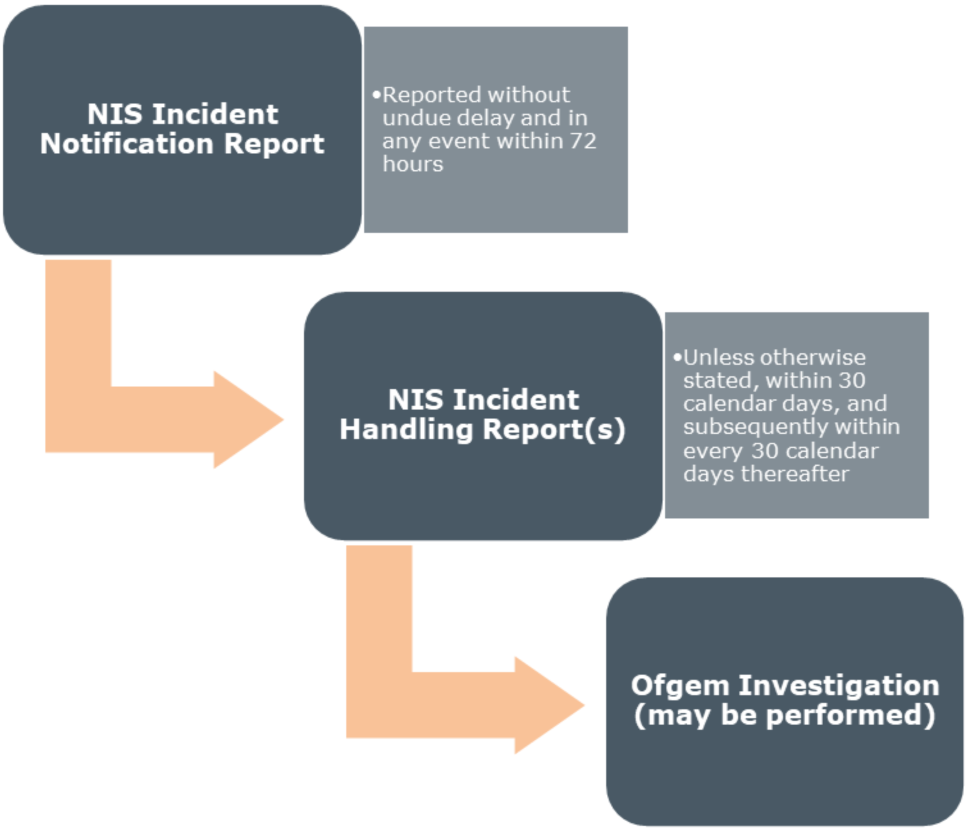

NIS Incident Notification Report
•Reported without undue delay and in any event within 72 hours
NIS Incident Handling Report(s)
•Unless otherwise stated, within 30 calendar days, and subsequently within every 30 calendar days thereafter
Ofgem Investigation (may be performed)

Figure 3: NIS Incident Reporting and Investigation Process

8.8. OES must notify Ofgem about any NIS Incident which has a significant impact on the continuity of essential service which that OES provides. Any notification made by an OES must make use of the approved template detailed within Annex E of BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations [14].

8.9. An OES must notify Ofgem without undue delay and in any event no later than 72 hours after the OES becomes aware that a NIS Incident has occurred.

8.10. After receipt of a notification Ofgem will notify BEIS in its capacity as the joint-CA, and NCSC in its capacity as the CSIRT. Ofgem's sharing of a reported NIS Incident should not preclude an OES from engaging with BEIS and/or NCSC on a voluntary basis, if the OES deems it prudent to do so, as voluntary support needs to be sought by the OES directly with those organisations.

8.11. The failure to notify Ofgem of a NIS Incident under Regulation 11(1) and comply with the notification requirements stipulated in Regulation 11(3) are contraventions of the NIS Regulations, which may lead to enforcement action against the OES.

NIS Incident Handling and Ofgem Investigation

8.12. Ofgem may seek to investigate further any reported NIS Incidents as set out in BEIS's Policy Guidance for the Implementation of the Network and Information Systems Regulations.

8.13. Steps 2 & 3 of the NIS Incident Reporting and Investigation Process within Figure 3 will be used, at least initially, to conduct further investigation into the NIS Incident.

8.14. Unless alternative timing is requested by Ofgem, the OES must submit NIS Incident Handling Reports to Ofgem within 30 calendar days of the initial NIS Incident Notification Report, and subsequently every 30 calendar days thereafter until Ofgem deems further reports are not required.

8.15. A NIS Incident Handling Report should cover:

- Summary of the NIS Incident
- Current status of the NIS Incident
- Summary of NIS Incident handling activity (e.g. operational response and recovery, and cyber incident detection, analysis, containment, and eradication)

8.16. In the event that the incident is still ongoing during the reporting timeline, then the OES should inform Ofgem on any potential delay at the earliest opportunity.

8.17. Following the receipt of the NIS Incident Handling Report, Ofgem may decide to conduct further investigation of the incident.

Abbreviations

Abbreviations	Explanation
BEIS	Department for Business, Energy and Industrial Strategy
CA	Competent Authority
CAF	Cyber Assessment Framework
CSIRT	Computer Security Incident Response Team
DCS	Distributed Control System
DGE	Downstream Gas and Electricity
DNRO	Deputy NIS Responsible Officer
GEMA	Gas and Electric Market Authority
HVAC	Heating, Ventilation, and Air Conditioning
IGP	Indicators of Good Practice
IRAM2	Information Risk Assessment Methodology 2
ISA	International Society of Automation
ISO	International Standards Organisation
KPI	Key Performance Indicator
NAO	NIS Accountable Officer
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
NIST	US National Institute of Standards and Technology
NRO	NIS Responsible Officer
OES	Operator of Essential Service
Ofgem	Office of Gas and Electricity Markets
OT	Operational Technology
RIIO-2	Revenue Using Incentives to deliver Innovation and Outputs
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SI	Statutory Instrument
SIS	Safety Instrumented System

References

[1] NIS Regulations 2018, https://www.legislation.gov.uk/uksi/2018/506/made, https://www.legislation.gov.uk/uksi/2020/1245/contents/made

[2] DCMS NIS Regulation 2018 Collection, https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[3] NCSC CAF Guidance, https://www.ncsc.gov.uk/collection/caf

[4] IEC 62443 Series: Security for Industrial Automation and Control Systems, https://webstore.iec.ch/searchform&q=62443

[5] NIST Risk Management Framework, https://csrc.nist.gov/Projects/risk-management

[6] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, https://www.iso.org/standard/75281.html

[7] Information Security Forum Information Risk Assessment Methodology 2 (IRAM2), https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/

[8] NCSC Risk Management Guidance, https://www.ncsc.gov.uk/collection/risk-management-collection

[9] ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, https://www.iso.org/standard/68091.html

[10] SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[11] Common Cyber Attacks: Reducing the Impact guidance, https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact#downloads

[12] ISO/IEC 27001 Information Security Management, https://www.iso.org/isoiec-27001-information-security.html

[13] SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[14] BEIS 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. Contact Details

General policy contacts

Ofgem

Email – cybersecurityteam@ofgem.gov.uk (not monitored 24/7)

BEIS

Email – nis.energy@beis.gov.uk (not monitored 24/7)

DCMS

Email – nis@dcms.gov.uk (not monitored 24/7)

NIS Incident reporting contacts

Mandatory

Ofgem

Email - cyberincident@ofgem.gov.uk (not monitored 24/7)

Voluntary

BEIS

Companies should contact their key policy contacts, and in the event of an incident out of hours - BEIS Emergency Response: Capability and Operations (ERCO) team using the following details:

Email - beis.erco@beis.gov.uk, Telephone (24/7) - 0300 068 6900

NCSC

Web-form (preferred) - https://report.ncsc.gov.uk/, Email - incidents@ncsc.gov.uk, Telephone (24/7) – 0300 020 0973