

Guidance

Ofgem Competent Authority Guidance for Downstream Gas and Electricity in Great Britain

Publication date: 30 November 2018

Contact: Cyber Security Team

Team: Network and Information Systems - Competent Authority

Email: cybersecurityteam@ofgem.gov.uk

Overview

The EU Directive on security of network and information systems (2016/1148) (NIS Directive) was transposed into UK law as The Network and Information Systems Regulations 2018 ("NIS Regulations") and came into force on 10 May 2018 for the water, health, transportation, digital and energy sectors. The NIS Regulations impose new duties on Operators of Essential Services ("OES") and give relevant Competent Authorities ("CAs") new powers and responsibilities to ensure OES are meeting those duties.

Ofgem have been designated in the NIS Regulations as a joint CA with the Department for Business, Energy and Industrial Strategy ("BEIS"), for the Downstream Gas and Electricity sectors in Great Britain.

OES are those gas and electricity operators which are determined by thresholds defined in the NIS Regulations and those determined by BEIS.

This guidance helps OES to understand their new duties and sets out Ofgem's initial approach to the implementation of the NIS Regulations. The guidance is the first in a developing strategy.

© Crown copyright 2018

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [Open Government Licence](#).

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

Contents

Introduction	4
1. Target Audience	4
2. Executive Summary	4
3. Background	5
4. Limitations.....	5
5. Status of this guidance.....	5
6. Ofgem Guidance Framework	6
Section A – Approach	7
1. Timeline	7
2. Overall Reporting.....	7
3. Scoping	9
4. Self-Assessment	12
5. Improvement Planning	13
6. Audit and Inspections.....	14
Section B – Cyber Incidents in DGE	16
1. NIS Incident Reporting	16
2. Incident Recovery	18
3. Post-Incident Investigation	18
Section C – Enforcement	20
Glossary of Terms	22
References	22
UK References	22
Related International References	23
Frequently Asked Questions	23
Appendices	24
Illustration of NIS and CAF Hierarchy and Structure.....	24
Purdue Enterprise Reference Architecture	25
Incident Contact Details	26

Introduction

1. Target Audience

This guidance is for **Operators of Essential Services (“OES”)**, as defined by the **Network and Information Systems Regulations 2018 (“NIS Regulations”)** (Reference 3) with undertakings in **Downstream Gas and Electricity (“DGE”)** in Great Britain. It may be used as a point of reference by Ofgem¹ in its role as a **Competent Authority (“CA”)** under the NIS Regulations (**“Ofgem”**). Ofgem may have regard to this guidance when interpreting the NIS Regulations to the extent it considers appropriate. This guidance fulfils the duties of the Gas and Electricity Markets Authority laid out at regulation 3(3)(b) of the NIS Regulations.

2. Executive Summary

This guidance has been issued to support OES with compliance with the NIS Regulations. Ofgem would like to acknowledge the contribution from the **Department for Business, Energy and Industrial Strategy (“BEIS”)**, industry and the **National Cyber Security Centre (“NCSC”)** in the development of this guidance.

The intent of the NIS Regulations is to increase the overall cyber-security and cyber resilience of OES, in relation to the network and information systems that support the delivery of essential services. OES **must** take appropriate and proportionate technical and organisational cyber-security countermeasures to manage risks posed to the security of the network and information, on which their essential service relies, and to prevent and minimise the impact of incidents on the essential service.

This will be achieved through partnership and collaboration between OES and Ofgem. This guidance supports OES in complying with the requirements of the NIS Regulations. It sets a process to help OES demonstrate they are managing cyber security risks in relation to essential services. This guidance should be used in accordance with the **National Cyber Security Centre (“NCSC”)** 14 NIS Principles and the **Cyber Assessment Framework (“CAF”)** (Reference 4).

In this guidance, we have set out a series of activities that OES are expected to complete. These include:

- Scoping of self-assessment,
- Self-assessment, and
- Identifying and implementing improvement plans.

OES will perform self-assessments against the CAF in the coming months. OES are expected to engage directly with Ofgem, and to raise any queries they have on how to apply the self-assessment at the earliest possible opportunity. Upon completion of the self-assessment, Ofgem may, where appropriate, review the self-assessment and work with OES to establish improvement plans. OES will propose what cyber-security countermeasures they consider appropriate to manage the risks and Ofgem may provide advice on whether further cyber-

¹ Ofgem is the Office of Gas and Electricity Markets. Ofgem is a non-ministerial government department governed by the Gas and Electricity Markets Authority. The terms “Ofgem” and the “Gas and Electricity Markets Authority” may be used inter-changeably in this guidance.

security countermeasures are required. Where appropriate, audits and inspections may also be scheduled by Ofgem to determine an OES's compliance with the requirements of the NIS Regulations and/or in respect of matters related to the self-assessment and improvement plans they submit.

OES also have a duty to report to Ofgem incidents that meet the defined NIS thresholds which have an adverse effect on security of network and information systems, used in the provision of the essential service. Ofgem may also liaise with the respective entities and conduct post-incident inspections (See Section B).

3. Background

Ofgem appreciates that cyber security is a developing area. OES should ensure that they keep up to date with industry good practice and accepted standards. Suggested industry standards include those listed as References 5, 7, 8 and 9.

As energy systems evolve to meet new requirements, it is important that cyber security enables and supports this transition. OES **must** manage their cyber security risks and actively monitor these to ensure a resilient energy system now and in the future.

4. Limitations

This guidance represents Ofgem's interpretation of current and developing standards for cyber-security predominantly on OT. It does not cover protection of personal data or intellectual property considerations for OES.

This guidance is the first iteration and may be updated and expanded in the future as required, based on the continued partnership and collaboration with the industry. This may include when the NCSC reviews the CAF in summer 2019.

This document does not provide guidance around the project engineering lifecycle, from design, development, factory or site acceptance testing, commissioning, decommissioning and disposal. Security requirements should be considered from the start of the design process. OES should also ensure that appropriate and proportionate cyber-security compliance requirements are used in the procurement process and for product specifications, with appropriate security standards. We recommend that OES engage with BEIS industry collaboration teams and the NCSC for continuing support and guidance in these areas.

For those OES who are considering strategic aspects of cyber-security and resilience as part of the '**Revenue Using Incentives to deliver Innovation and Outputs**' framework ("**RIIO-2**") for gas and electricity transmission and gas distribution licensees, Ofgem plans to consult on proposals for the RIIO-2 price control, which includes proposed approach to cyber resilience. Interested parties are invited to respond to that consultation.

5. Status of this guidance

Responsibility for compliance with the NIS Regulations lies with the boards of the OES. While this guidance may help OES in achieving and maintaining compliance, OES should not rely solely on Ofgem and/or this guidance for this purpose.

Ofgem relies on the information and data submitted by OES as being accurate and reliable. Any information or data provided to Ofgem (in whatever form) may be used for the purposes of enforcement action in accordance with Ofgem's statutory duties.

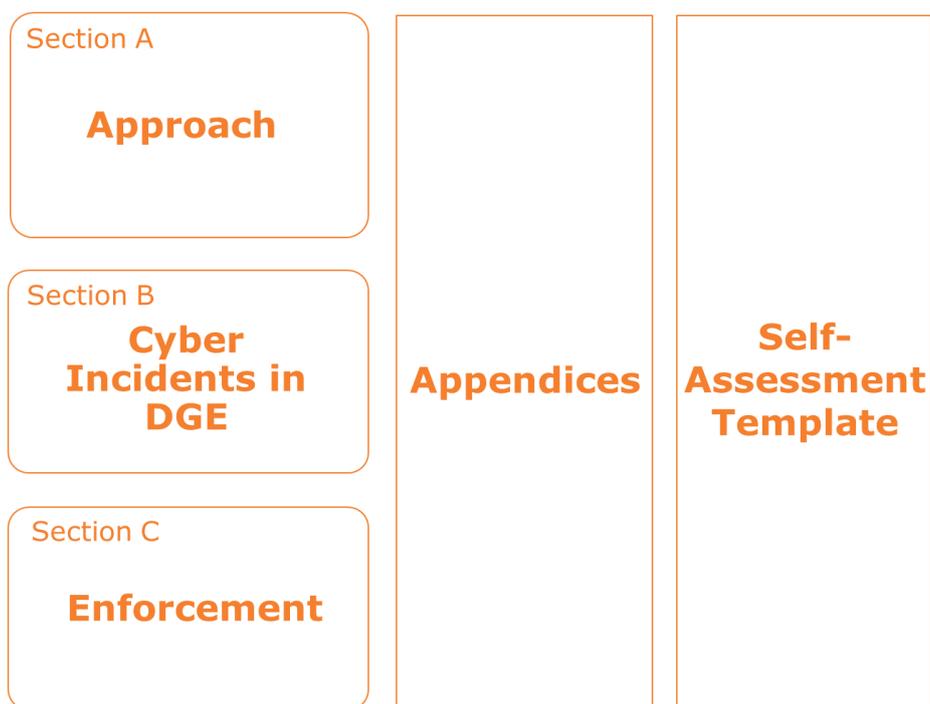
Ofgem’s receipt of any information or data from an OES or other party (howsoever provided and including, without limitation, in an OES self-assessment report, completed CAF spreadsheet, improvement plan, audit or inspection report) should not be taken as tacit approval or endorsement of any conduct described therein. In addition, any reviews or associated commentary Ofgem may provide in relation to the same are purely advisory and do not represent Ofgem’s approval or endorsement of an OES’s conduct, 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.

The guidance does not state the law and is not intended to provide a comprehensive guide to compliance with the NIS Regulations. The 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.

6. Ofgem Guidance Framework

Below is a summary of this guidance for DGE in Great Britain.

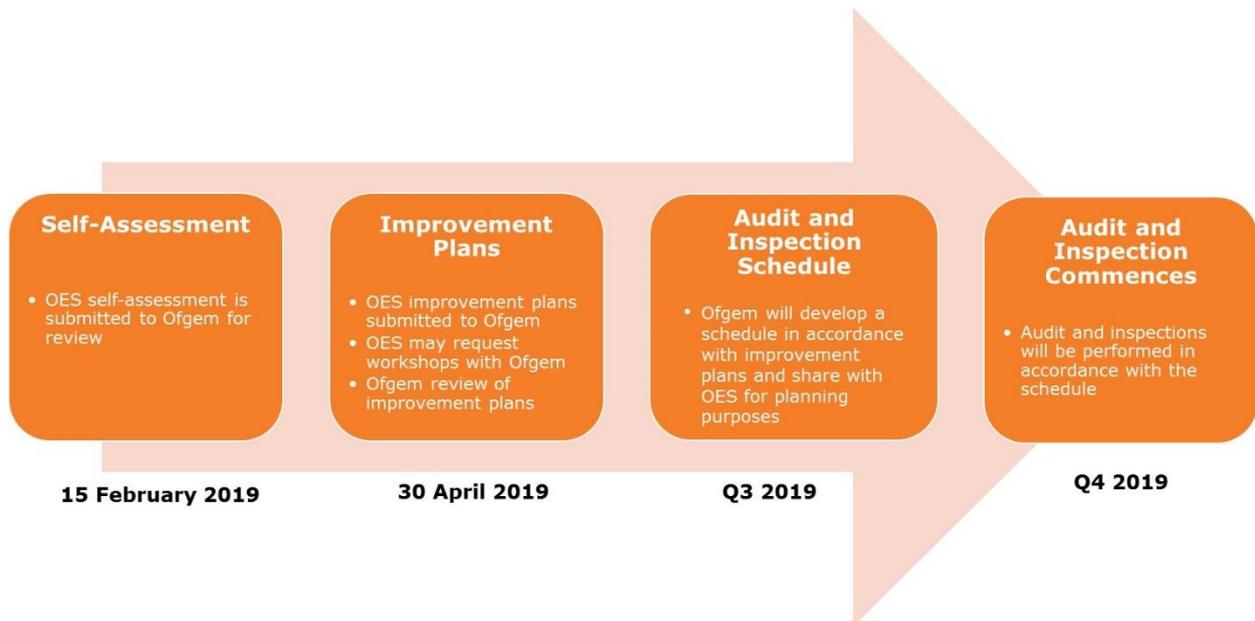
Ofgem Guidance Framework



Section A – Approach

1. Timeline

Below sets out the overall timescales until Q4 2019. It is expected that these timelines are adhered to by all OES. It is the responsibility of OES to inform Ofgem at the earliest possible opportunity, should there be any issues in being able to comply with the timescales.



1. Self-Assessment - OES are expected to submit self-assessments by 15 February 2019 for each of the essential services that they provide. Ofgem may, where appropriate, review the self-assessments and seek further information or clarification from the OES on their contents.
2. Improvement Plans - Once a self-assessment has been reviewed, OES may need to develop improvement plans to mitigate risks that require treatment. OES may request workshops with Ofgem in developing their improvement plans. OES should submit their improvement plan to Ofgem by 30 April. Ofgem may, where appropriate, review the improvement plan and seek further information or clarification from the OES on its contents.
3. Audit and Inspections Schedule - Ofgem may, where appropriate, develop an audit and inspection regime and share this with OES for planning purposes.
4. Audit and Inspection Commencement – Where appropriate, Ofgem may also commission audits and/or inspections of an OES.

2. Overall Reporting

OES are requested to submit the following reports to Ofgem using the methods set out in this section. The scoping performed and previously submitted to Ofgem in October 2018, should be appended to the self-assessment report to serve as context. The scoping document defines the parameters for an OES self-assessment.

2.1 Self-assessments

OES will submit their self-assessments to Ofgem and these comprise of:

- **Part 1: OES Self-Assessment Report**

This provides a high level overview of the complete self-assessment, any significant risks identified and any initial proposals for risk treatment. This should be submitted using the self-assessment reporting template which can be found on Ofgem’s website.

- **Part 2: The NCSC CAF spreadsheet (“CAF Spreadsheet”) with supporting evidence**

A completed CAF spreadsheet should be submitted to Ofgem, plus supporting evidence to validate the self-assessment. Evidence is required for areas identified as ‘Not Achieved’ or ‘Partially Achieved’. No supporting evidence is required to be submitted where CAF outcomes have been ‘Achieved’, although justification should be provided in the CAF assessment. Part 2 should be submitted to Ofgem at the same time as Part 1 (see FAQs on how to send submissions to Ofgem in a secure fashion).

OES should submit one self-assessment per business line, for example one generation, transmission, distribution, supply or gas storage. OES may choose to develop several CAFs, for each asset, site or system, for their own self-assessment purposes, however these should not be submitted to Ofgem.

It is appreciated that there may be instances where an OES may be mostly ‘Achieved’ and only parts of the OES are ‘Not Achieved’ or ‘Partially Achieved’. As there may have already been significant efforts or resources invested to address cyber security and resilience in these areas, the OES may discuss the CAF assessment to reflect this with review from Ofgem. Therefore, an OES could mark ‘Achieved’ with exceptions listed under the justification section. Any exceptions need to be made explicit and it should be indicated how the exceptions have been risk assessed and managed accordingly. Where these risks are above tolerance, they should be listed in Part 1 submission (see section A 2.2).

Once submitted, Ofgem will acknowledge receipt of the self-assessment and may then review OES submissions. Ofgem may, where appropriate, enter into a discussion with OES and request further information on the reported items to back up its assessments. This may be to seek further clarification on CAF outcomes deemed as ‘Not Achieved’ or ‘Partially Achieved’. Should language within the self-assessment be unclear or ambiguous, Ofgem will need to clarify this with the OES.

OES are requested to be as clear and open as possible in their self-assessments. OES are requested to contact Ofgem at the earliest possible opportunity if they are unsure of anything at any point. Once OES have completed their self-assessment, OES should consider areas for improvement (see Section A 2.2).

In the initial self-assessment, Ofgem recognises that OES may not have ‘Achieved’ in all categories. The key action is for OES to undertake an accurate self-assessment and develop an improvement plan, where improvements are required.

Where OES have provided justifications for items listed as ‘Achieved’, this will be accepted by Ofgem and evidence is not expected to be submitted. A high level justification should, however, be provided within the CAF self-assessment spreadsheet as to why an item is deemed to be ‘Achieved’. These areas may still form part of OES audits and inspections.

2.2 Improvement Planning

Following the process for submission of Part 1 and Part 2 submissions set out above, OES will develop their improvement plans. OES may request workshops with Ofgem as set out above. Improvement plans should build upon the OES's self-assessments, identifying risks in accordance with their own risk management and risk methodology. The improvement plan should set out the cyber-security countermeasures OES intend to take where the risk is above the OES own risk tolerance levels. Improvement plans may cover both short term measures ('quick-wins') or longer term strategic measures, for which budget needs to be sought through business planning. Ofgem may, where deemed to be required, review the improvement plans with the OES in order to assist them with prioritisation and risk mitigation planning.

Ofgem may also work with the industry to assist with the development of an appropriate Improvement Planning template. Ofgem aims to circulate the template for OES to submit by 30 April 2019.

2.3 Incident reporting

OES should use the reporting template provided in Annex G of reference 2. OES should continue to report all incidents to the NCSC and **BEIS Emergency Response: Capabilities and Operations team ("ERCO")** for response and recovery support (relevant contact details can be found in Appendix 3). Where an incident escalates into a NIS reportable incident, this **must** be reported to Ofgem in the manner defined in Section B. It is not the role of Ofgem to perform cyber incident response.

3. Scoping

The network and information systems which are within the scope of the NIS Regulations are only those that are relevant to the delivery of the essential services that the OES provides and where compromise of that system could impact the continuity of the essential service. The preliminary work for scoping has been conducted via Ofgem, and the **Energy Emergency Executive Committee, Cyber Security Task Group ("E3CC")**, established sub-groups and on a one-to-one basis with OES. Ofgem requested OES to submit final scoping by 15 October 2018.

The output of scoping is for OES to identify critical systems and networks, to develop an understanding for the self-assessment. The scoping document should set out clear lines of responsibility and accountability, statement of assumptions made, identification of reliance scope, list of systems and networks, grouping of assets, where applicable and listing of all relevant sites or aggregated numbers of related sites.

A useful point of reference for systems, networks and categorisation is the 'Energy Delivery Systems Cyber Security Procurement Guidance' (Reference 1).

3.1 Structure of scoping report

The format of the scoping report can be tailored for OES's needs. The typical format is one which has all of the following:

1. High level description of the critical systems and networks.
2. High level diagram of environment mapped to Purdue architecture model (See Appendix 2).
3. Indication of the major interactions between zones and conduits.
4. High level description of any major upgrades or replacements due in the next 24 months.

5. List of assumptions made and list of systems and networks that may be related and deemed explicitly as out of scope, including justification as to why they are deemed as out of scope. Boundary diagrams may be a useful aid to illustrate this for cases of interfaces or common interfaces.

3.2 Suggested principles

1. Only network and information systems that are deemed necessary to the delivery of essential services should be considered.
2. Therefore, essential services managed by manual processes, which OES are not dependent upon the information, being provided from information systems, will automatically be de-scoped.
3. Risk analysis will include internal and external influences, and by both intentional and unintentional means.
4. Appropriate segregation of 'other' information systems will be deemed adequate to de-scope, with explanation and evidence.
5. However, risks posed to the essential services which are reliant upon network and/or information services, which have persistent or intermittent interconnections or related devices shall be in scope.
6. Transferring responsibility of systems that are critical to the provision of the essential service, are typically performed if those systems are operated by an entity which is also regulated under the NIS regulations and has included such systems in their scope.
7. The OES will be required to validate that the information is accurate.
8. Network and Information systems deemed low risk may still be in scope due to the attack vectors posed, which may affect other systems or network architecture.
9. Network and Information systems will be in scope if OES are unable to operate under normal conditions beyond the acceptable outage period, with no alternative and sustainable means of operating.

3.3 Further suggestions

- All relevant systems, networks, assets and sites under the ownership of OES should be listed, even if they are managed and operated by another party.
- Where grouping of assets/sites are performed and not considered to be in scope for NIS, OES should provide appropriate justification(s).
- It may be that the OES has already identified much of the above, perhaps from a Business Continuity Management programme or discontinuity analysis, Cyber Risk Reviews or other risk management programme. For the purposes of the NIS regulations these need to be refreshed.

3.4 Further considerations for OES from the NCSC

1. Organisational – which organisations, sections and people have access to the networks and information systems that deliver the essential service.
2. Interfaces - What cyber-security countermeasures is there at the boundaries of the scope? Are there sufficient cyber-security countermeasures at the boundary of the scope to provide confidence OES are meeting the requirements of the NIS Regulations?
3. Dependencies – What internal (e.g. internet gateway) and external factors (e.g. telecoms networks) do the networks and information systems rely on to provide the essential service?
4. Supply Chain – Who manages and maintains your systems and how do they do that?

5. There are often several ways to map the functional and logical view in a scope. There isn't a 'right answer'. Use the approach that helps your organisation understand the components that support the essential service and how they interact.
6. The systems in scope of NIS Regulations may change over time, due to increased knowledge of how the essential service is provided or due to changes in the network and information systems used.
7. The OES should regularly review their systems in scope of the NIS Regulations (at least every twelve months) and as part of any significant change activity.

3.5 Steps for scoping

Below are some suggested steps to take for scoping:

Step 1: Identify critical business processes and their inter-dependencies classified with high impact.

Step 2: Identify and group assets/sites according to criticality to the overall essential service.

Step 3: Map (high-level not sub-level) critical business processes reliance upon the various grouping of assets/sites.

Step 4: Identify asset/site owners and determine who manages these and where there may be shared responsibilities.

Step 5: Determine impact of loss of group of assets, to business objectives and national requirements.

Step 6: Identify supporting systems and networks.

3.6 Examples of critical network and information systems

This is not an exhaustive list but indicates some of the systems an OES may deem critical for the provision of the essential service they provide.

- Distributed Control System
- Supervisory Control and Data Acquisition Systems
- Gas Turbine Control System
- Steam Turbine Control System
- Water Treatment Plant System
- Cooling Water Makeup System
- Common Services (Auxiliary) System
- Coal plant System
- Generator Protection Systems
- Fire Safety Systems
- Emergency Shutdown Systems
- Switching System
- Engineering Systems
- Communication Systems
- Plant Information Systems
- Remote Terminal Units
- Programmable Logic Controllers
- Plant based Heating Ventilation and Air Conditioning
- IT Systems deemed critical by the business for the delivery of essential services
- Trading systems

Where OES have acquired new sites or significant assets, and scoping has already been reviewed by Ofgem, then this will be out of scope for the current self-assessment. Where current sites, significant assets, critical systems or networks, or significant supporting

security systems are to be decommissioned 12 months from May 2019, this should be listed as excluded from the scoping for self-assessment in Year 1. Supporting plans which reflect this and that have been approved by OES senior management, should be submitted to Ofgem as part of the scoping document.

4. Self-Assessment

It is the government's view that the principles-based approach is a more effective way of driving improvements to cyber security in the context of NIS, than an approach based on prescriptive rules. This is due to complex and rapidly changing areas within cyber security. OES understand their own business better than any external entity and should be more capable of taking informed, balanced decisions about how they achieve the outcomes specified by the NIS principles.

The NCSC has developed a method of assessing the extent to which an organisation is managing the cyber security risks, surrounding the delivery of essential services. This assessment method is known as the CAF.

The CAF has been designed by NCSC to provide an outcome-focused assessment against the 14 NIS principles across four objectives (NIS and CAF hierarchy and structure is set out in Appendix 1). Each of the principles is linked to specific guidance which highlights some of the factors that OES will usually need to take into account when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges.

The principles are broken down into 39 contributing outcomes. Each outcome is associated with a set of **Indicators of Good Practice ("IGPs")** arranged in a table format. OES should assess whether they can be considered 'Achieved', 'Partially Achieved' or 'Not Achieved' against each outcome. The result of applying the CAF is 39 individual evaluations that reflect to what extent an OES meets the IGPs.

IGPs aren't intended to be prescriptive, there may be alternative sources of good practices, such as some international standards, frameworks or methodologies, which may be helpful to OES, in managing cyber security risks.

The principles carry no assumptions about how the specified outcomes should be achieved. NCSC has noted, assessment of contributing outcomes should involve the role of expert judgement and interpretation.

It is for OES to determine the most appropriate cyber-security countermeasures to deliver outcomes within their organisational context, to manage cyber security risks.

Ofgem may, in some cases, suggest additional guidance to OES, on how the outcomes can be achieved.

OES are expected to undertake a robust but realistic CAF self-assessment supported by evidence. The self-assessment is to be performed within the parameters set out in the scoping document. This may include both legacy and current networks and systems which are still in operation. It is *highly* recommended, that OES commence assessments with the most critical sites and assets first.

It would be advisable to obtain some or all of the following prior to commencing self-assessment:

- Organisational and Governance Structure
- Reporting relationships
- Existing Roles and Responsibilities
- Existing Security Metrics

- Cyber Security Strategy
- Most recent Cyber Security Risk Assessments
- Existing / Planned Security Initiatives and Roadmap
- Existing Cyber Security and related Policies / processes / procedures / guidelines / standards
- Asset Inventory across locations
- Network Architecture
- Network Zoning Details
- Gain an understanding as to how the site and system(s) fit in the overall 'value' or 'supply' chain, to gain insight into business and operational criticality of each site and system(s)
- Identify the single point of accountability for each site, system and asset
- For each site under assessment, identify key stakeholders to assist in obtaining the list of vendors and versions of Industrial Control Systems (as those listed in 3.6) which are used to support particular production processes in the location
- Identifying what assets and components are critical for the site.
- For each main OT, obtain the number of independent instances of the system used to support the processes.

Whilst performing self-assessments, OES should identify the following:

- For each instance of the main Industrial Control System obtain an estimate size of the instance through:
 - number of devices which are managed by the system
 - number of operator stations
 - number of controllers
 - number of servers
- Identify connections and data feeds to and from the control systems, including manual data feeds as well as intermittent and persistent physical or network connections
- Identify if there are any known issues with systems
- Identify major projects underway or scheduled
- Understand the dependencies relating to the site

Since the NIS Regulations do not apply directly to the supply chain of OES, it is the OES responsibility to put in place appropriate and proportionate cyber-security countermeasures with their suppliers. OES should ensure that suppliers have in place appropriate cyber-security countermeasures to manage risks of their services being disrupted through the supply chain.

5. Improvement Planning

Once OES self-assessment have been submitted to Ofgem, OES should begin to develop improvement plans. Where Ofgem carries out a review of the self-assessment, this may include assisting OES in identifying the risks that require treatment through cyber-security countermeasures. Ofgem expects OES to take a risk-based approach when considering where improvements are needed. The onus is therefore on OES to identify risks in accordance with their own established methodologies and processes.

Improvement plans should set out the cyber-security countermeasures OES intend to take where they deem the risk to be above their own risk tolerance levels. All high risks above OES risk tolerance levels should be identified with appropriate and reasonable cyber-security countermeasures to reduce the risk to acceptable levels. Improvement plans may cover, short term measures ('quick-wins'), medium term measures or longer term measures, for which budget needs to be sought through business planning.

It is *highly* recommended that all cyber-security countermeasures are considered in the order of people, process and technology. The rationale is that the underpinning process and

technology can essentially be undone by the people, and the culture of security needs to be well embedded.

OES will review their final improvement plan in conjunction with Ofgem. The aim of the improvement plan is to develop a short-to-medium approach to raise levels and manage cyber security risks. As previously mentioned, Ofgem may work with industry to develop a template improvement plan.

OES may need to undertake a significant amount of work to put in place both a **Cyber Security Management System ("CSMS")** and the necessary technical cyber-security countermeasures to manage risks appropriately. Ofgem estimates the preparation of the CSMS with associated design changes could take 6 to 12 months, subject to the circumstances of the OES and any required improvements. Implementation of the CSMS and implementation of quick wins could take 6 months.

Robust strategic improvement planning, recruitment and training could take 6 months. Timelines for initiatives and cyber-security countermeasures will form part of the improvement plan, this should also be reflected in OES own business planning.

The priority of cyber-security countermeasures to address high risks should be based in accordance with those which are deemed to be 'quick-wins' first. Quick-wins are those cyber-security countermeasures which have the least amount of dependency, complexity and overhead. This may include and is not limited to:

- Focussed awareness sessions or training for selected individuals or groups,
- Revision of contractual obligations for third parties,
- Disconnecting undocumented and/or rogue connections,
- Establishing practices for OT engineering laptops,
- Establishing practices for the usage of removable media,
- Removal of redundant accounts,
- Managing the change of default user accounts and passwords or
- Ensuring change management is strictly followed.

6. Audit and Inspections

Based on the improvement plans reviewed across the sector, Ofgem expects to develop an audit and inspection schedule in accordance with identified themes and risk across the sector. Audits and inspections are expected to be driven by this plus inclusion of specific items that will be raised on a case-by-case basis with OES.

Following the submission of the first self-assessment and improvement plan, any audit and inspections are expected to commence in Q4 2019. An OES can expect to be audited or inspected once in the first year and then as part of a rolling audit and inspection regime thereafter. Each audit or inspection can last from three to five days typically on site, which may scale upwards depending on the schedule and the coverage determined to be required.

Previously an option considered was for OES to cover the costs of audit and inspections directly from an accredited list of independent third parties (4.15 from reference 2). However, Ofgem intend to use the cost recovery powers under the NIS Regulations for the purposes of carrying out audit and inspections on OES. It is expected that Ofgem will commission any audit and inspections with a limited number of third parties to act in the interests of Ofgem and to provide an opportunity to:

- Perform normalisation and benchmarking
- Provide insight on interpretation of compliance and risk profiles
- Ensure sufficient oversight

OES should put in place all necessary internal business arrangements, irrespective if Ofgem shall be recovering the costs from OES or OES shall be making payment directly to accredited independent third parties.

Section B – Cyber Incidents in DGE

OES should respond to incidents as per their current procedures, including contacting government departments as per existing arrangements (see contact details in Appendix 3). OES should not wait until an incident reaches the NIS incident reporting threshold before seeking support from the NCSC and other parts of government in containing and mitigating incidents that risk affecting essential services.

Reporting the incident to Ofgem will have no impact on how the response process is handled by either government or the OES involved.

Ofgem does not have a role in providing support during incident response. NCSC as the NIS **Computer Security Incident Response Team (“CSIRT”)** provide support during incident response.

1. NIS Incident Reporting

Incident reporting is invaluable to:

- build an understanding of the threats affecting the sector and provide early warning
- enable timely advice across the sector and cross-sector where appropriate
- support specific law enforcement response where required
- provide historical context when performing likelihood assessments in future

OES **must** notify Ofgem about any incident which has a significant impact on the continuity of the essential service which that OES provides (**“a network and information systems”** or **“NIS”** incident) (Regulation 11). A NIS incident is an incident, which has an actual adverse effect on the security of network or information systems, used in the provision of essential services, with reference to the NIS incident reporting thresholds (see below).

When an OES becomes aware that an incident has reached the threshold for reporting under NIS, they **must** report it to within 72 hours.

At this point Ofgem will be aware of the incident but does not have a role in providing support for incident response. Reporting the incident to Ofgem will have no impact on how the response process is handled by either government or the OES involved.

It is requested that the OES report the NIS incident using the template provided in Annex G in reference 2, however the template is not a requirement.

The contact information in the event of a NIS or non-NIS reportable incident can be found in Appendix 3.

The NIS Incident Reporting Thresholds for Electricity and Downstream Gas, from Annex F of reference 2, are found below to serve as a reminder for OES:

Sector	Incident Threshold	Aligns with
Gas Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to offtakes and affects customers.	Current Ofgem reporting requirement
Electricity Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to grid supply points and affects customers for more than 3 minutes.	Current Ofgem reporting requirement
Gas Distribution	Unplanned single incident loss of supply to 5,000 customers.	Current Ofgem reporting requirement
Electricity Distribution	Unplanned single incident loss of supply to 50,000 customers for more than 3 minutes.	Current Ofgem reporting requirement
Gas Interconnectors	Unplanned loss of ≥ 10 MCM over a 24-hour period.	Upstream Gas Production, Processing and LNG/Gas Storage thresholds, which are aligned to existing Oil and Gas Authority reporting thresholds.
Electricity Interconnectors	The net unauthorised or unplanned loss or gain of ≥ 560 MW of interconnector flow in a given direction.	Incidents that have the potential to impact the delivery of electricity to end customers
Electricity Generation	The unauthorised or unplanned loss of ≥ 1500 MW of electricity generation, when cumulated with all generators operated by affiliated undertakings. This includes generation scheduled to dispatch within the next 4 hours.	Incidents that have the potential to impact the delivery of electricity to end customers
Energy Suppliers	Unplanned shut off or single incident loss of supply to 50,000 customers for more than 3 minutes.	Electricity distribution operator threshold.

The thresholds established are for the purposes of clarifying what the incidents are which have a significant impact on the continuity of the essential service that the OES provides. For the avoidance of doubt, this has no effect on the determination of whether or not an OES has satisfied its security duties in terms of Regulation 10 of the NIS Regulations.

A cyber-attack may not be immediately identifiable as such, and so OES may want to look for one or more of the following:

- related security breaches, including physical
- data copied to OT environment or connection of unauthorised removable media
- suspicious requests and/or instructions
- known activation of software or script
- unauthorised access and/or configuration changes to security software

The failure to notify Ofgem of a NIS incident is a contravention of the NIS Regulations under regulation 11. However, an incident is not necessarily a contravention of the NIS Regulations and therefore may not lead to enforcement action being taken.

After receipt of the notification, Ofgem may, if appropriate, liaise with NCSC and BEIS to ensure that communications are aligned with the OES and, if necessary, the general public are informed about the incident and any actions to take.

2. Incident Recovery

Ofgem will generally seek to ensure that any necessary regulatory intervention during an incident is kept to a minimum to ensure OES have the necessary time to respond and recover.

When systems and equipment have been made safe by the OES, there are further priorities. These may be in order of importance listed below:

1. Starting limited, degraded operation(s) where the risk to safety is acceptable, in accordance with accepted practice.
2. Returning the overall network system to 'normal state' of functioning.
3. Taking any and all remedial action where the point of breach has been identified.
4. Identifying, isolating and preserving evidence for forensic analysis.
5. Internal investigation into how systems were breached (this should not interfere with any official investigation).
6. Remedial action(s) to prevent further breaches.

Affected systems and equipment should be put into a safe state to prevent harm or damage occurring after the initial incident has taken place.

3. Post-Incident Investigation

The picture below is a high-level process flow in relation to reporting and investigation by Ofgem.



Within 30 days of a NIS incident being reported by an OES, the OES is expected to submit an interim report to Ofgem.

Within 60 days of a NIS incident being reported by an OES, the OES is expected to submit a post-incident investigation report with lessons learned, to Ofgem. Although high unlikely, it is noted that there may be circumstances that the incident is still ongoing at the 60-day mark. Should an OES believe it will not be able to meet this deadline, the OES should inform Ofgem at the earliest opportunity.

Following the receipt of the post-incident investigation report, Ofgem may decide whether or not the incident requires further investigation. The purpose of the investigation may be to:

- establish the cause of the incident and assess whether the incident was preventable;
- assess whether effective and reasonable risk management was in place;
- assess whether the OES had appropriate security measures in place; and/or
- assess how the OES responded to and managed the incident.

Should an investigation be appropriate, Ofgem may use the OES developed post-incident investigation report as a basis for review. Once the investigation has concluded, Ofgem may decide on any appropriate next steps. These may be no action, advice or formal enforcement action.

Where a cyber-attack has taken place, OES should consider the risk from further cyber-attacks and take advice from NCSC on the likelihood of this occurring. OES should capture lessons learned through formal reporting for continual improvement to manage times of crisis and disaster recovery. These lessons may be used to update OES's emergency response and contingency plans.

Section C – Enforcement

Ofgem is in the process of developing its approach for any future enforcement action it takes when an OES fails or is failing to meet the duties set out in NIS Regulations. It is expected that until Q3 2019, given the initial collaborative and partnering approach between Ofgem and the OES, that enforcement action in respect of a breach of the OES' security duties under regulation 10 will not be a priority matter for enforcement, unless it is necessary in the circumstances of a particular case.

Any enforcement action will be dealt with on a proportionate basis, which takes account of the seriousness of any contravention(s) of an OES' duties under the NIS Regulations.

When developing its enforcement approach to and conducting enforcement under the NIS Regulations, Ofgem will have regard to the enforcement objectives and principles set out in its Enforcement Guidelines at paragraphs 1.7-1.12 (reference 6).

An OES duties under the NIS Regulations are set out at regulations 10 and 11 and include:

The security duties of operators of essential services

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.

(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.

The duty to notify incidents

11.—(1) An OES must notify the designated competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident")...

The occurrence of a "NIS incident" itself does not necessarily mean that there has been an failure by an OES to comply with its security duties or notification duties. The key factors for determining enforcement will be:

- whether or not appropriate and proportionate security measures were in place and were being followed for OES' security duties in terms of regulation 10; and/or
- whether NIS incidents are notified to Ofgem in terms of regulation 11.

Ofgem's approach to enforcement is in development. Its anticipated approach to enforcement is as follows:

Step 1: Advise and persuade

When any non-compliance is identified, the initial approach taken by Ofgem will be to engage and discuss these with the OES. This will include discussing what the failing or deficiency is, how and when it should be addressed and in what timescale. Ofgem may review any remedial actions proposed by the OES (including when these actions should be completed). Should this be appropriate, Ofgem may follow up with further audit and/or inspections to ensure these actions have been addressed appropriately.

Ofgem may issue information notices under regulation 15 of the NIS Regulations requiring the OES to provide specified information to support any assessment of compliance.

Step 2: Enforcement notice

Where the initial collaborative approach has not worked or is not appropriate and/or it is clear that failings are not being addressed, a formal Enforcement Notice may be issued (regulation 17). The Enforcement Notice will include the failings identified, the steps (if any) to be taken to rectify the failures, the time period in which they **must** be completed and how and when representations on the Enforcement Notice may be made.

Step 3: Penalty notice

Where the OES has failed to take adequate steps to rectify a failure identified in an Enforcement Notice or Ofgem is not satisfied with the representations made by an OES in response to such an Enforcement Notice Ofgem may impose a financial penalty (regulation 18).

In determining the value of the financial penalty, Ofgem will consider the appropriate and proportionate level within the prescribed limit of £17m by reference to the tiered limitations set out at regulation 18 (6).

If an infringement occurs which breaches the NIS Regulations and another regulatory requirement or legislation, Ofgem will have regard to this and where appropriate discuss the best approach with any other relevant regulators, for example with Information Commissioner's Office on **General Data Protection Regulation ("GDPR")** breaches.

Step 4: Reviews

It should be noted that regulation 19 of the NIS Regulations sets out that an OES may request an independent review of penalty decisions taken by Ofgem in order to challenge the following matters:

- a) the grounds for imposing a penalty notice, or,
- b) the sum that is imposed, and or,
- c) the time period within which the penalty notice **must** be paid.

Any request to conduct a review **must** be made in writing and copied to Ofgem setting out the reasons for requesting a review and any relevant evidence, within 30 days of receipt of the penalty decision.

Glossary of Terms

Abbreviations	Explanation
BEIS	Department for Business, Energy and Industrial Strategy
CA	Competent Authority
CAF	NCSC Cyber Assessment Framework
CSIRT	Computer Security Incident Response Team
CSMS	Cyber Security Management System
DGE	Downstream Gas and Electricity Sectors
DMZ	Demilitarised Zone
E3CC	Energy Emergency Executive Committee, Cyber Security Task Group
ERCO	BEIS Emergency Response: Capability and Operations
GDPR	General Data Protection Regulation
IGP	NCSC Indicators of Good Practice
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
OES	Operator of Essential Services
OT	Operational Technology
RIIO	Revenue Using Incentives deliver Innovation and Outputs

References

UK References

1. Energy Delivery Systems Cyber Security Procurement Guidance 2018, <http://www.energynetworks.org/electricity/engineering/cyber-security-procurement-language-guidance.html>
2. BEIS Security of Network and Information Systems Regulation 2018 Implementation in the Energy Sector for GB, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf
3. NIS Regulations 2018, <https://www.legislation.gov.uk/uksi/2018/506/made>
4. NCSC NIS Guidance Collection (including Cyber Assessment Framework) 2018, <https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework>
5. Introducing component-driven and system-driven risk assessments, 2017, <https://www.ncsc.gov.uk/guidance/introducing-component-driven-and-system-driven-risk-assessments>
6. Ofgem Enforcement Guidelines, 2017, <https://www.Ofgem.gov.uk/publications-and-updates/enforcement-guidelines>

Related International References

7. [IEC 62443 Series: Security for Industrial Automation and Control Systems](https://www.isa.org/isa99/), <https://www.isa.org/isa99/>
8. ICS Security Related Working Groups, Standards and Initiatives, <https://www.enisa.europa.eu/events/good-practices-for-an-eu-ics-testing-coordination-capability/ics-security-related-working-groups-standards-and-initiatives>
9. NIST Publication 800-82 – Guide to Industrial Control Systems (ICS) Security, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

Frequently Asked Questions

How much detail and supporting documentation is expected for the initial scoping submission?

Answer: Ofgem is not expecting mass supporting documentation for scoping. What is expected as reasonable and sufficient is typically 2 -5 pages.

What supporting evidence should be submitted with the self-assessment?

Answer: Evidence provided should be current and accurate and reflect a realistic picture of all OES critical systems in scope. Evidence is required for aspects which are 'partially-achieved' or 'not achieved'.

The quality of information provided is paramount, and where it does not exist, efforts should be made to develop these within reasonable timescales. These include and are not limited to:

- Provide a list of existing improvement plans
- Provide organograms and role descriptions
- Identify corporate risks appetite and risks tolerance levels
- Provide references to key policies, processes and procedures, adhered to in completing this process
- OES should provide important context in the evidence where it will illustrate
- Foreseen changes such as disinvestment or upgrade projects
- Risk(s) identified which are above tolerance, where risk treatment chosen by OES is to accept the risk(s)

How should I be sharing information with Ofgem?

Answer: Ofgem currently use Huddle workspace for OES to share sensitive information such as individual scoping and reporting. Huddle adheres to the 14 CESG and Cabinet Office Cloud Security Principles, which detail how cloud providers manage the services provided to G-Cloud. Several UK Public Sector Senior Information Risk Owners, have assessed and entrusted the use of Huddle for Official (OFFICIAL-SENSITIVE) content.

Switch Egress, is currently certified under the NCSC Commercial Product Assurance scheme and is also deemed appropriate for use. Ofgem are expected to be storing high-volume using approved mechanisms and further information may be made available to OES for their own assurance.

Appendices

Appendix 1

Illustration of NIS and CAF Hierarchy and Structure

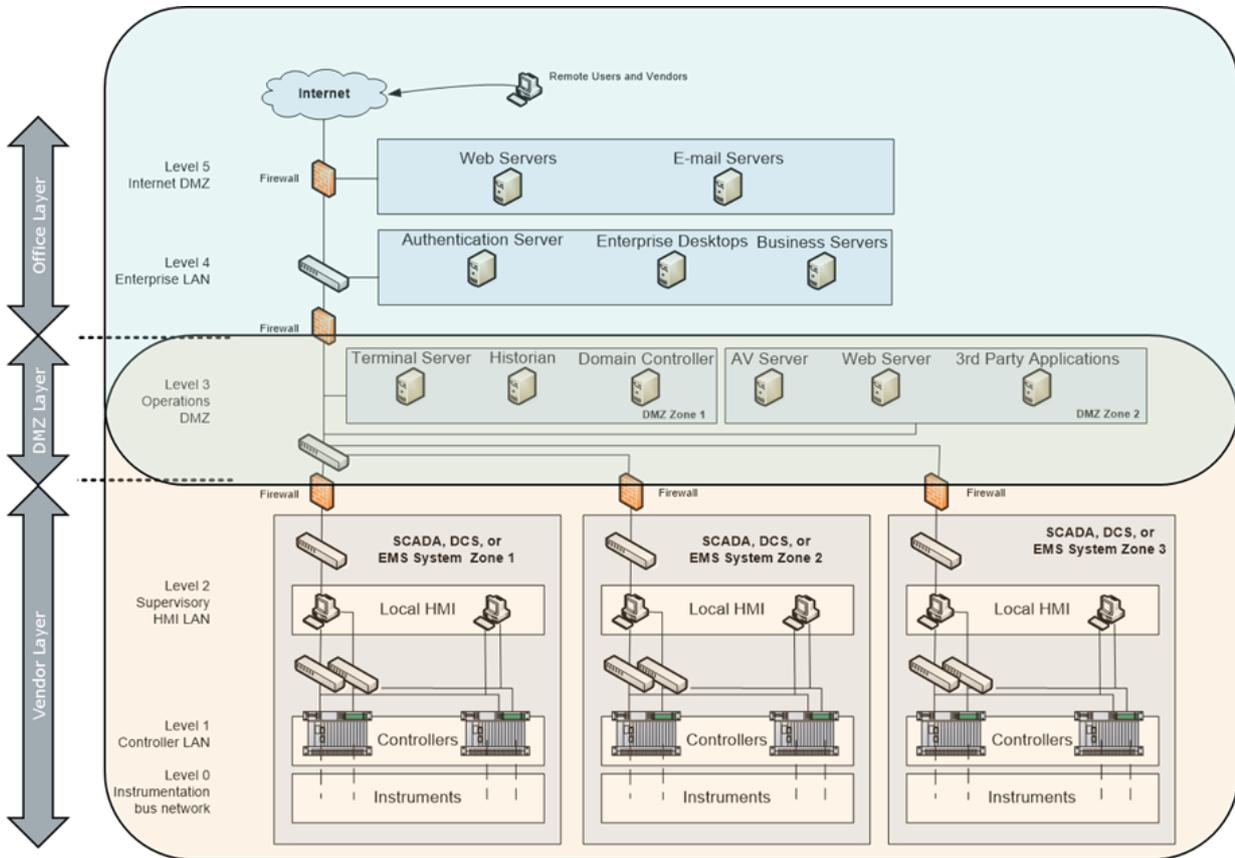
Objectives x 4	A Managing Security Risk	B Protecting Against Cyber Attack	C Detecting Cyber Security Events	D Minimising the Impact of Cyber Security Incidents
Principles x 14	A1-A4	B1-B6	C1-C2	D1-D2
Contributing Outcomes x 39	A1.a-c A2.a-b A3.a A4.a	B1.a-b B2.a-d B3.a-e B4.a-d B5.a-c B6.a-b	C1.a-e C2.a-b	D1.a-c D2.a-b
Indicators of Good Practice Multiple indicators per Contributing Outcome				

A: Managing Security Risk		B: Protecting Against Cyber Attack		C: Detecting Cyber Security Events		D: Minimising the Impact of Cyber Security Incidents	
A1: Governance	A2: Risk Management	B1: Service Protection Policies and Processes	B2: Identity and Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response and Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks and Systems	B6: Staff Awareness and Training				

This table is provided for illustration purposes only.

Appendix 2

Purdue Enterprise Reference Architecture



Appendix 3

Incident Contact Details

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

OES should contact NCSC using the following details;

Email - incidents@ncsc.gov.uk, Telephone (24/7) – 0300 020 0973

Ofgem

OES should contact Ofgem using the following details:

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