Guidance

NIS Security Assurance Guidance (Concept) for Downstream Gas & Electricity

Publication date:	30 April 2025
Version:	1.0
Contact:	Cyber Security Team
Team:	Ofgem Cyber Regulatory Directorate (NIS Competent Authority)
Email:	cybersecurityteam@ofgem.gov.uk

Ofgem, in its capacity as joint Competent Authority with the Department of Energy security and Net Zero (DESNZ), has issued this guidance to support a programme of wider assurance activity under Regulation 16 of the Network and Information Systems Regulations 2018 (NIS Regulations). This guidance is intended for Operators of Essential Services (OES) and select cyber security consultancies that are approved to conduct assurance activities such as Audit, Operational Exercising and Technical Testing. This document provides an overview of regulatory assurance approach and details the expected outcomes.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU.

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

Audience

This guidance is for OES and select cyber security consultancies in the downstream gas and electricity sector (DGE) Sector in Great Britain. It is intended to be used as a point of reference by Ofgem for providing assurance of the DGE Sector under the NIS Regulations.

This guidance cannot and does not anticipate every possible scenario. Where a scenario arises which is not addressed in this guidance, we aim to review and adopt an approach consistent with the specific context at issue and with the NIS Regulations.

This guidance is intended as practical advice and is not intended to augment the NIS Regulations. It provides further additional guidance to OES on conducting assurance activities under the NIS Regulations. This guidance, the process, timescales and criteria associated with it, and all other associated aspects are indicative and non-binding on Ofgem and may be changed at Ofgem's discretion.

1. Introduction

Purpose of this Document

1.1 This document outlines Ofgem's changes to our security assurance approach under the NIS Regulations for OES within the DGE Sector. It provides an updated view of how Ofgem will engage with OES to assess security maturity and their progress towards achieving the target CAF Profile[1].

1.2 This document is intended to be read alongside:

- NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain[2]
- NIS Supplementary Guidance and CAF Overlay for DGE Sector[3]
- NIS Inspection Framework for Downstream Gas and Electricity[4]
- Network and Information Systems Enforcement Guidelines and Penalty Policy[5]

These documents, alongside the associated templates, will be updated, where applicable, to align with the changes in our assurance approach.

Background

1.3 The NIS Regulations provide legal measures to maintain and improve the level of security (both cyber and physical resilience) 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.
- Regulation 10(2) - An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the

[1] We may periodically review and update the expected cyber resilience attainment levels for the DGE subsector. The current expectations are documented in DESNZ's 'Initial Target Attainment Levels of Expected Cyber Resilience by the DGE Subsectors'.
[2] https://www.ofgem.gov.uk/publications/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services
[3] NIS Supplementary Guidance and CAF Overlay for DGE Sector
[4] Available on demand
[5] https://www.ofgem.gov.uk/publications/network-and-information-systems-enforcement-guidelines-and-penalty-policy

network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

- 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.

- 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).

1.4 Following the consultation[6] held from 6 May 2024 to 22 July 2024 on the approach to supporting a programme of wider assurance activity under Section 16 of the NIS Regulations, we are publishing this assurance guidance to enhance regulatory oversight and integrate resilience practices into OES business-as-usual (BAU) activities.

1.5 This guidance introduces a requirement for the OES to engage and report their assurance activities to Ofgem as part of the annual compliance reporting process[7]. This guidance is issued to support OES with ongoing 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.

[6] Ofgem Security Assurance Framework published on 6th May 2024 for the consultation

[7] The full implementation of assurance related reporting requirements is planned for July 2026 regulatory submissions

Overview of Security Assurance Approach

1.8 Ofgem is committed to advancing regulatory effectiveness by adopting a risk-based, engagement-led approach. This ensures our resources are directed towards where it is most required, e.g. potential resilience gaps.

1.9 This approach builds on self-assessments, annual reporting, and previous engagements to ensure security controls are effective and resilience claims are reliable. Ofgem will increase and prioritise engagements, where required, and provide feedback on assurance activities, such as audits, operational exercises, technical testing, or sector-wide exercises.

1.10 OES should define and conduct their assurance activities based on their risk profile, aligned with the target CAF profile. These activities, including Audits, Operational Exercises, and Technical Testing, should be justified to Ofgem through their Compliance report that includes Annual Report, Assurance Programme Plan[8] etc. We have introduced a requirement to submit an Assurance Programme Plan[9] alongside the Annual Return to facilitate the receipt of this additional information.

1.11 Ofgem recommends OES select suppliers from accredited NCSC schemes, which provide recognised benchmarks for capability. Existing arrangements with key service providers are accepted if they meet the desired outcomes of equivalent accreditation standards and there are no conflicts of interest. Please refer to section 3 for further information.

1.12 Ofgem will engage with OES on selected assurance activities and will require visibility of their outputs. The outputs should be submitted as a regulatory submission and will be used by Ofgem to form a view of confidence and assess whether to utilise our powers of inspection under Section 16 of the NIS Regulations.

Regulatory Submissions Confidence Level

1.13 The Regulatory Submissions Confidence Level indicates Ofgem’s confidence in an OES's NIS programme, aligned to the relevant CAF profile. This confidence is derived from, but not limited to, the OES's regulatory submissions.

[8] Ofgem will provide a template and guidance for the Assurance Programme Plan.

[9] The full implementation of assurance related reporting requirements is planned for July 2026 regulatory submissions

1.14 To determine a level of confidence, Ofgem will assess, at a minimum, the following criteria:

- whether Assurance Programme Plans are appropriate and proportionate;
- the depth and breadth of the assurance activities covered;
- accuracy and veracity of the information provided;
- the effectiveness of controls under realistic threat scenarios;
- appropriateness and progress of remediation activities;
- progress against identified security improvement plans ensuring transparency in reporting; and,
- past inspection outcomes.

1.15 There may be instances where Ofgem will evaluate and consider the OES risk profile when determining the engagement approach.

1.16 This approach balances fairness and flexibility, providing support to the OES where it is most needed. It also ensures that Ofgem remains within its regulatory remit while adapting oversight to evolving threats and organisational contexts.

2. Assurance Activities

2.1 OES are required to conduct assurance activities based on their risk profiles and aligned with the target CAF profile. This is to demonstrate effective security risk management, as required by their obligations under the NIS Regulations. We have outlined the requirements related to the assurance process in the below sections. Ofgem will update the NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain (Ofgem NIS Guidance)[10] and associated templates to reflect this approach.

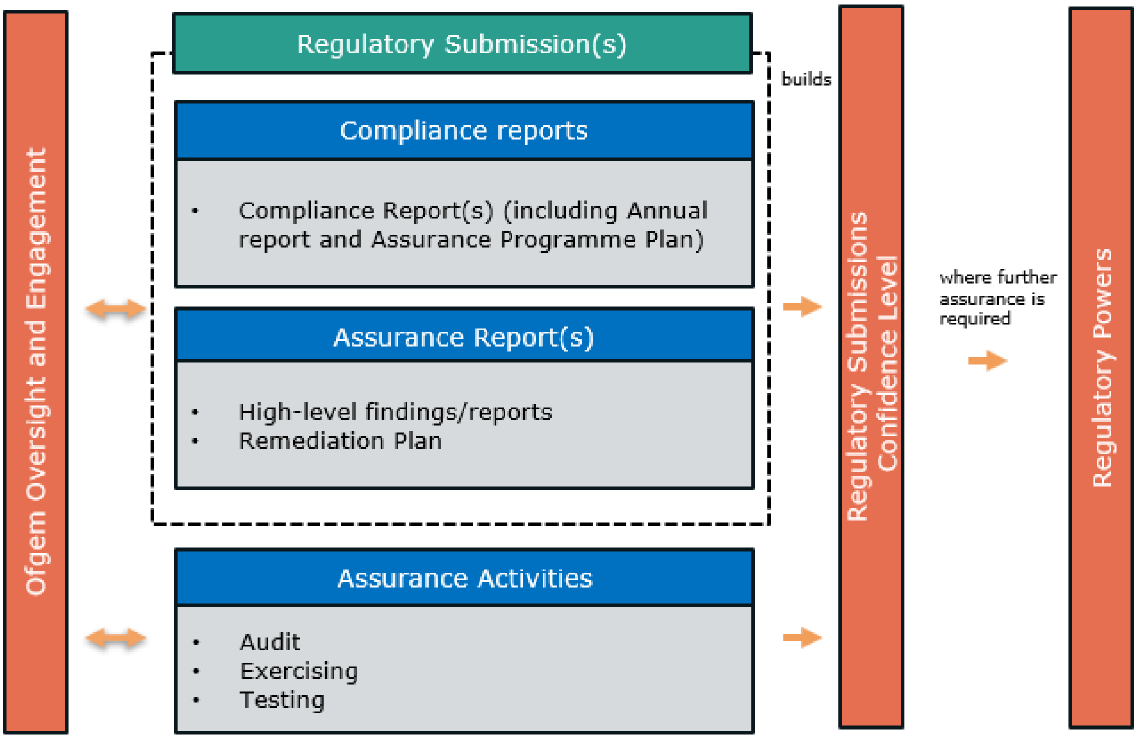
Ofgem Oversight and Engagement
Regulatory Submission(s)
Compliance reports
Compliance Report(s) (including Annual report and Assurance Programme Plan)
Assurance Report(s)
High-level findings/reports
Remediation Plan
Assurance Activities
Audit
Exercising
Testing
builds
Regulatory Submissions Confidence Level
where further assurance is required
Regulatory Powers

Figure 1 Components of Assurance Process

Regulatory Submission(s)

2.2 OES are required to submit their NIS Compliance Report(s), based on the NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain[11].

2.3 Alongside the NIS Annual Report, the OES are required to submit their Assurance Programme Plan. It should include as a minimum:

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

[11] Ofgem will be updating the NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain along with the supporting templates, to support the OES assurance activities and reporting.

- type of assurance activities planned;
- schedule of assurance activities;
- schedule for sharing assurance reports and remediation plans with Ofgem;
- assurance activity goals;
- assurance activity scope; and,
- updated remediation plans from previous assurance activities.

2.4 Ofgem may request additional information to perform 'deep dives' into areas requiring further investigation and/or assurance.

2.5 When considering assurance activities, OES should assess their risks and determine an appropriate and proportionate assurance programme (e.g. frequency, type, scope and schedule), aligned to the target CAF Profile. This approach should be justified to Ofgem through their NIS Compliance Report(s) and Assurance Programme Plan submission.

2.6 OES are recommended to submit a view of their assurance programme extending beyond 12 months, to support building Regulatory Submissions Confidence Level. Therefore, it is not expected that assurance activities take place at the end of the reporting period.

2.7 The confidence level is likely to be higher where an OES carries out a broader and deeper set of assurance activities, supported by accredited certification that is relevant to the NIS Scope[12]. Activities conducted as part of BAU processes may be used to build Regulatory Submissions Confidence Level, depending on the level of cyber security and resilience maturity.

2.8 As best practice, Ofgem recommends that OES select suppliers from accredited NCSC schemes[13] for assurance activities. These provide recognised benchmarks for capability. Existing arrangements with key service providers will be accepted if they meet the desired outcomes, such as equivalent accreditation standards and no conflict of interest.

2.9 Ofgem reserves the right to request additional details regarding assurance activities, confirm their suitability, and require visibility of the outputs to build confidence. This engagement will support Ofgem in effectively targeting its powers of inspection, exercising, and testing where needed.

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

[13] Note: Not all scheme members are skilled in OT/ICS networks; additional clarification to meet an OES's actual needs may be required

2.10 Ofgem may request to attend select assurance activities (e.g. planning meetings, workshops, the assurance activity, and close out meetings). Ofgem may on an ad-hoc basis, invite DESNZ and/or NCSC as observers to an assurance activity.

2.11 OES with interdependent systems with other OES may conduct joint assurance activities. The outcome of these activities will need to be incorporated into the individual OES assurance output.

2.12 Under Section 16 of the NIS Regulations, Ofgem reserve the right to use its own inspectors, direct an Ofgem approved organisation to conduct activities on our behalf and / or have an OES procure an Ofgem approved organisation to conduct assurance activities.

Assurance Activities

2.13 Ofgem intends to publish further guidance on assurance. High-level examples of assurance activities include (but are not limited to):

Audit

2.14 The Audit is intended to review and produce report findings based on the following (non-exhaustive) areas of focus:

- assessing the comprehensiveness, accuracy and veracity of the OES' NIS scope;
- assessing the comprehensiveness, accuracy and veracity of the OES' supporting evidence;
- reviewing improvement plans demonstrating consideration of Ofgem target CAF profile(s), as well as the milestones previously set by the OES;
- reviewing the progress made in risk reduction, as well as the effectiveness of the OES's risk management and risk mitigation activities;
- reviewing organisation controls and processes against OES' own policies, methodologies and standards;
- an audit of several or all CAF areas (including Ofgem CAF overlay objectives) to support building Confidence; and,
- where certifications have been used for all or part of the NIS scope, confirm their applicability and effectiveness to the scope they have been applied to.

2.15 An OES may procure NCSC accredited consultancy (or equivalent) to conduct an audit of several or all CAF areas (including Ofgem CAF overlay objectives) to support building Regulatory Submissions Confidence Level.

Equivalence

2.16 Ofgem expects OES to adopt recognised good practice frameworks and standards when designing and implementing their security programs to achieve compliance with the NIS Regulations. In this context, OES should consider leveraging existing—or obtaining new—valid independent certifications from accredited bodies to demonstrate alignment with specific areas of the target CAF profile.

2.17 Where these certifications align with defined NIS scope, they can provide Ofgem with additional assurance. Examples of such certifications include, but not limited to, Cyber Essentials Plus, ISO27001, NIST CSF, ISO 27019 and IEC62443. The OES may submit any accredited certificate (including the scope of applicability) to demonstrate alignment with the relevant contributing outcome, such as an ISO27001 certificate for demonstrating ISMS processes or an IEC 62443 conformance certificate for demonstrating relevant risk assessment processes or hardware/software security levels. The OES should justify that the standard adopted provides an appropriate level of equivalence based on the specific operational context of their business.

Operational Exercising

2.18 Operational exercises simulate real-world attack scenarios, technical failures, or other disruptions to assess how well security teams, processes and technologies perform under stress. These activities would need to use a recognised Operational/Information Technology scenario[14] involving resources, process and procedures directly related to the essential service(s).

2.19 Operational Exercising aims to evaluate and generate findings based on the following areas of focus (non-exhaustive):

- assessing the effectiveness and adequacy of security and resilience management process including response, recovery, reporting, continual improvement and analysis;
- evaluating critical factors such as incident response time, communication protocols, and implementation of recovery measures;
- validating the adequacy of the procedures, including incident response plans, business continuity plans and disaster recovery plans, in addressing potential

[14] https://www.ncsc.gov.uk/schemes/cyber-incident-exercising/introduction

incidents including cyber-attacks, technology failures, human errors and natural disasters; and,

- assessing the resilience of critical NIS assets by simulating various scenarios and evaluating the ability of the procedures to facilitate timely recovery and restoration of essential service, with a focus on regular drills and preparedness activities.

Technical Testing

2.20 Technical Testing aims to evaluate and generate findings based on the following key areas of focus (non-exhaustive):

- validating the effectiveness of security controls and measures implemented to protect NIS assets either by directly interacting with systems or simulating real operational conditions in a controlled environment; and,
- validate OES security posture and potentially identify vulnerabilities that could be exploited.

2.21 All Technical Testing are expected to follow recognised industry best practices and standards[15].

2.22 If an OES identifies a new or potentially impactful vulnerability or threat within the DGE Sector, they are expected to promptly engage and share this information with the NCSC[16], Ofgem, and relevant suppliers or partners. This collaborative approach ensures a coordinated response to mitigate risks and enhance sector-wide resilience.

Assurance Reporting

2.23 OES and third-party vendors may apply recognised standard practice to rate findings; however, we recommend that OES adopt the NCSC CAF as a basis for categorising their assurance activities and reporting. All high-level findings shared with Ofgem should be aligned with the CAF and Ofgem's Supplementary Guidance.

2.24 The OES is expected to provide Ofgem with the high-level findings/final report within 8 weeks following the assurance activities. If the OES cannot meet this deadline, they must engage with Ofgem to inform us of the changes, the reasons for the change and a new date for providing the relevant information.

[15] https://www.ncsc.gov.uk/schemes/check/introduction

[16] https://www.ncsc.gov.uk/information/vulnerability-reporting

2.25 Ofgem will consider what further regulatory action, if any, is required, e.g. additional engagement, additional assurance activity, enforcement action or penalty.

Regulatory Oversight and Engagement

2.26 When the regulatory reporting, assurance activities or engagement do not build sufficient confidence (as set out in Section 2 above), Ofgem will engage with the OES further or utilise its regulatory powers. This includes:

- seeking further information via an information Request[17];
- directing an NCSC accredited organisation (or equivalent) to conduct Audit, Operational Exercise or Technical Test on its behalf[18];
- directing the OES to procure an NCSC accredited organisation (or equivalent) to Audit, Operational Exercise or Technical Test on its behalf [19];
- conducting its own inspection[20] using the current Inspection Framework or Technical Test[21]; and/or,
- Issuing an enforcement notice[22] or penalty notice[23]. When considering an enforcement Notice or penalty notice, the Network and Information Systems enforcement Guidelines and penalty Policy[24] will apply.

2.27 Once the Regulatory Submissions Confidence Level is deemed sufficient, Ofgem will continue with the engagement-led approach.

[17] Section 15 (2) of the NIS Regulations
[18] Section 16 (b) of the NIS Regulations
[19] Section 16 (c) of the NIS Regulations
[20] Section 16 (1) (a) of the NIS Regulations
[21] Section 16 (5) (f) of the NIS Regulations
[22] Section 17 (1) of the NIS Regulations
[23] Section 20 of the NIS Regulations
[24] https://www.ofgem.gov.uk/publications/network-and-information-systems-enforcement-guidelines-and-penalty-policy

3. NCSC-Accredited Organisations

3.1 An OES may procure an NCSC-accredited consultancy (or equivalent) to conduct assurance activities.

3.2 All organisations conducting an independent assurance activity should be accredited by a relevant NCSC Scheme or equivalent standard.

3.3 Where possible, to ensure quality and consistency of assurance activity, equivalent standards will align with relevant industry accreditation schemes, for example, the NCSC Assured Security Consultancy Scheme ("ASCS"), Cyber Resilience Audit Scheme (CRA), Cyber Incident Exercise Scheme, CREST or other such schemes.

3.4 Independent assurance organisations may only require industry scheme membership relevant to the assurance activity they are required to conduct. In specific areas not suitably covered by industry schemes, Ofgem will require organisations to demonstrate additional certification and/or experience, for example, in Operational Technology.

Conflict of Interest

3.5 NCSC-accredited organisations shall seek to avoid any situation that may give rise to a conflict of interest between them, the OES and Ofgem. Examples of potential conflicts of interest include but are not limited to:

- an approved organisation having interests in products or services covered under the scope of the assurance activities;
- an accredited organisation conducting an assurance activity for an OES whom they have implemented or consulted on any of the elements covered in the scope of the assurance activity, or involved in the delivery of projects to an OES via the RIIO framework, where it could be assessed or provided as evidence; or,
- personal relationships between members of staff responsible for the management of or undertaking assurance activities and staff within the OES.

3.6 The accredited organisations shall notify Ofgem if they become aware of or suspect an actual or potential conflict of interest.

3.7 The accredited organisations shall only subcontract to other approved suppliers.

3.8 Where an accredited organisation subcontracts work relating to the assurance activity, they must ensure that there are sufficient measures in place to mitigate a conflict of interest by either party and that there is no impact on the outcome of the assurance activity.

3.9 When an OES utilises its internal team for assurance activities, it must demonstrate the team's independence from its operational and security functions. Furthermore, the OES should be able to demonstrate adherence to accreditation standards.

3.10 The OES should avoid linking staff remuneration to the outcomes of assurance activities, as this practice may inadvertently incentivise staff to misrepresent data.

4. Disclaimer

4.1 We would remind OES that responsibility for compliance with the NIS Regulations lies with their management teams and Board. While we hope that guidance and support from Ofgem, including interaction during the assurance processes, may help OES in achieving and maintaining compliance, OES should not rely solely on Ofgem for this purpose. OES should seek such legal or other professional advice as they consider appropriate to ensure compliance with their obligations under the NIS Regulations.

4.2 Assurance reports will be used by Ofgem in carrying out its functions under the NIS Regulations. Ofgem may, on an ad-hoc basis, invite DESNZ and/or the NCSC as observers to selected assurance activities. If an OES has any reservations with regard to proposed observers at the time, they are expected to raise this with Ofgem during the planning stage.

4.3 Ofgem and any appointed organisations rely on the information and data submitted by OES in connection with an assurance activity as being accurate and reliable. Ofgem's receipt of any information or data from an OES should not be taken as express or tacit approval or endorsement of any conduct described therein.

4.4 In addition, any assessments or commentary provided by Ofgem do not represent any form of approval or endorsement of an OES's conduct, unless expressly stated in writing.

5. References

[1] The Network and Information Systems Regulations 2018, May 2018:

https://www.legislation.gov.uk/uksi/2018/506/made

[2] DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain:

DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations

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

NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB v2.0.pdf

[4] NIS Supplementary Guidance and CAF Overlay for DGE Sector:

NIS Supplementary Guidance and CAF Overlay for DGE Sector

[5] Network and Information Systems Enforcement Guidelines and Penalty Policy:

Network and Information Systems - Enforcement Guidelines

6. Glossary of terms

Abbreviations	**Explanation**
Audit	an audit refers to a systematic and independent examination of an OES's cyber security measures and practices, adhering to the NCSC CAF's principles and objectives
DESNZ	Department for Energy Security and Net Zero
CA	Competent Authority
CAF	NCSC Cyber Assessment Framework
Compliance Report	a set of documents that OES submit to Ofgem to demonstrate adherence to regulatory requirements under the NIS Regulations.
DGE	Downstream Gas and Electricity
Enhanced CAF profile	The Enhanced Profile for DGE is a tailored profile that represents a more demanding target level compared to the Basic Profile, corresponding to a level of cyber resilience matched to a moderate cyber-attack capability.
IGP	NCSC CAF Indicators of Good Practice
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
OES	Operator of Essential Services
Operational Exercising	Operational exercising refers to the practice of conducting simulated security incidents to test and improve an OES's response capabilities.
Ofgem	Office of Gas and Electricity Markets
Technical Testing	Technical testing refers to the process of evaluating the security of an OES's systems, networks, and applications through various methods. These methods could include vulnerability assessments, penetration testing, and security configuration reviews