NIS | Competent Authority

Department of Finance
An Roinn Airgeadais
www.finance-ni.gov.uk

NETWORK INFORMATION SYSTEMS REGULATIONS 2018

Guidance for Operators of Essential Services

October 2022

NIS Competent Authority for Northern Ireland

1 Contents

2 About this Guidance

This guidance is developed by the Department of Finance pursuant to, and in satisfaction of, Regulation 3(3)(b) and the competent authority obligation to prepare and publish guidance.

The Department of Finance is the designated Network and Information Systems (NIS) competent authority within Northern Ireland for Operators of Essential Services (OES) in the health, drinking water supply and distribution, road and rail transport and energy sectors, and referred to in this guidance as the NIS competent authority

This guidance will help an organisation identify if they are an Operator of Essential Service (OES) as defined by the NIS Regulation.

The guidance will help organisations understand what the NIS Regulation is and how it applies to them as an OES. It will help an OES understand the role and responsibilities of the Northern Ireland NIS Competent Authority as the body responsible for oversight and enforcement of the NIS Regulations and how these duties will be carried out.

The Guidance also provides an outline of the Department of Finance process for administering the NIS legislation and conveys the role and responsibilities on operators of essential services (OES) as part of that process.

The guidance underpins the collaborative engagement approach sought between the NIS competent authority and OES community to ensure compliance with the NIS Regulations and ultimately better overall protection of essential services within the health, drinking water, road and rail transport and energy sectors in Northern Ireland.

The guidance will be kept under review and will be updated to reflect views of the industry and to reflect learning gained from implementing the legislation. This will help ensure that the guidance is accurate, up-to-date and relevant.

An OES should ensure they have obtained any legal or professional advice necessary to ensure compliance with their duties under the NIS Regulations. This guidance:

- does not create any rights enforceable at law in any legal proceedings;
- is not a substitute for legal advice;
- is not a set of binding instructions, although it includes references to provisions in the NIS Regulations which are statutory requirements; and
- does not limit the ability of relevant Competent Authorities to make their own judgement or establish their own processes in accordance with the NIS Regulations. Competent Authorities are not bound to follow this guidance and may depart from it in appropriate circumstances.

This guidance replaces the previous guidance published by the NIS competent authority in July 2018. It reflects the current NIS Regulations including new or amended statutory provisions in relation to:

- enforcement;
- penalties;
- appeals; and
- inspections.

3 What is the NIS Directive?

The NIS Regulations are not a cyber regulation as often mis-construed by its title. It provides 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.

The Network Information Services (NIS) Directive was developed by the EU to boost the overall level of security for network and information systems that support the delivery of essential services. It applies to those sectors which are vital for our economy and society, providing services such as the supply of electricity and water and the provision of healthcare and transport and digital services.

This NIS Directive was adopted by the European Parliament in July 2016 and came into force in August 2016. EU Member States had until 9 May 2018 to transpose the Directive into domestic legislation. The UK implemented the requirements of the NIS Directive through a UK-wide set of Regulations - the Network and Information Systems Regulations 2018 (NIS Regulations), which came into effect on 10 May 2018[1]. Amendments to these regulations were made on exit of the EU under the Network Information Systems (Amendment and Transitional Provision etc.) Regulations 2020[2] coming into force in December 2020 and these regulations continue to evolve. Operators of Essential are advised to ensure the are referencing the most recent version of the regulations.

The NIS Regulations establish a legal framework to ensure that essential services and selected digital service providers within the UK put in place adequate measures to improve the security of their network and information systems, with a particular focus on those services which if disrupted, could potentially cause significant damage to the UK's economy, society and individuals' welfare; and to ensure serious incidents are promptly reported to the competent authorities.

The measures help improve the security of network and information systems that underpin essential service delivery across the UK by:

- Ensuring the UK has in place a national framework to support and promote the security of network and information systems, consisting of a National Cyber Security Strategy. A new UK cyber strategy was published December 2021[3]
- a Computer Security Incident Response Team (CSIRT), a national Single Point of Contact (SPOC) and a NIS Competent Authority (or Authorities); In the UK the CSIRT and SPOC are provided by NCSC as part of GCHQ.
- Set up a CSIRT to promote swift and effective operational cooperation on incidents and sharing of information about risks;
- Ensuring that organisations within those vital sectors of our economy are

---

[1] The Network and Information Systems Regulations 2018 (legislation.gov.uk)

[2] The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (legislation.gov.uk)

[3] National Cyber Strategy (publishing.service.gov.uk)

effectively managing the security of their network and information systems.

Organisations within those sectors that are identified by the UK as "Operators of Essential Services (OES)" will have to:

- take appropriate and proportionate technical and organisational measures to manage the security of their network and information systems. This includes managing cyber security risks and broader security and resilience risks to network and information systems supporting essential services;

- take appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems; and

- notify the relevant authority of any incidents affecting network and information systems which have a significant impact on the continuity of the essential service they provide.

In Northern Ireland the NIS Regulations are administered by a number of competent authorities with responsibilities at a sectoral or regional level.

4 Who are the Competent Authorities?

Oversight and enforcement of the NIS Regulations is the responsibility of the designated competent authority. These can be found in schedule 1 of the NIS Regulations.

The UK Government decided that a multiple competent authority approach was appropriate, with each competent authority having a detailed understanding of the individual sector/region and the associated challenges. Competent authorities have therefore been designated for each sector or region covered by the NIS Regulations. The following competent authorities have been designated for services that operate in Northern Ireland or at a UK level encompassing responsibilities for Northern Ireland.

- **Department of Finance – CA for Operators of Essential Services (OES)**

  The Department of Finance is designated for Operators of Essential Services (OESs) at a regional level in health, drinking water supply and distribution, road and rail transport and energy sectors in Northern Ireland.

- **Information Commissioner – CA for Relevant Digital Service Providers (RDSP)**

  The Information Commissioner is designated at a UK level for organisations defined as relevant digital service providers (RDSPs). A RDSP would provide services such as online marketplaces, online search engines and cloud computing services.

- **Office of Communications – CA for Digital Infrastructure Services**

  Office of Communications (Ofcom) are designated at a UK level as the competent authority for Digital Infrastructure which are specific kinds of services such as top-level domain registration services, Domain Name System (DNS) services and Internet Exchange point (IXP) services.

- **Civil Aviation Authority (CAA) – UK Level CA for Air transport**

  The Secretary of State for Transport and Civil Aviation Authority (act jointly) for air

transport sector across the UK. This subsector includes passenger airports, en-route air traffic control services, provision of services by air carriers that meet the thresholds defined in schedule 1 The air transport subsector of the NIS Regulations.

- **Secretary of State for Transport – UK Level CA for Water Transport**

  The Secretary of State for Transport is responsible for the water transport sector across the UK. This subsector includes shipping in the UK for freight and passenger services subject to meeting the thresholds outlined in Schedule 1 The water transport subsector of the NIS regulations.

This guidance has been developed by the Department of Finance acting as the competent authority for Operators of Essential Services in the health, drinking water supply and distribution, road and rail transport and energy (Electricity, Gas and Oil) sectors but may be useful for other organisations in the wider NIS context.

5 Responsibilities of the Competent Authority

Competent authorities have the sole authority and responsibility for all regulatory decisions in relation to the NIS Regulations.

As per regulation 3 competent authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region;
- establishing the identification thresholds for the OES in their sector or region;
- preparing and publishing guidance to assist OES or Digital Service Providers in meeting the requirements of the NIS Regulations (including this guidance document);
- keeping a list of all OES who are designated and all revocations;
- assessing compliance of OES against the requirements of the NIS Regulations, including audits;
- determining the thresholds for notifiable incidents in their sectors or regions;
- receiving incident notifications;
- cooperating with other competent authorities to provide consistent advice and oversight to OES or Digital Service Providers;
- consulting and cooperating with the CSIRT, SPOC and Information Commissioner's Office (ICO);
- making sure that there are processes in place for responding to physical security incidents, system failures or natural hazards affecting network and information systems - and issuing guidance to support companies dealing with those types of incidents;
- investigating incidents;
- enforcement, including issuing notices and penalties, of the requirements of the NIS Regulations.

OES should refer to the current regulations and engage with the relevant competent authority when interpreting this guidance to seek clarifications and support where needed.

6 Are you an OES (Operator of Essential Service)?

To establish if your organisation is an Operator of Essential Service to which this guidance will apply consider the following terms as defined in the Regulations.

1. the service satisfies a threshold requirement for that essential service within a sector and sub sector as defined in schedule 2 paragraphs 1-9 of the regulations and set out in and reflected in Appendix 1 of this guidance, and

2. You deliver an essential service under the Regulations. an "Essential Service" means a service which is essential for the maintenance of critical societal or economic activities; and

3. the service relies on network and information systems or

4. You have been specifically designated by the competent authority under regulation 8.(3)

If you meet these checks then by default you are an OES - Operator of Essential Service under these Regulations to which this guidance applies, and you have legal responsibilities.

The Regulations 8.(3) allows a competent authority to designate a person an Operator of Essential Service even if a person does not meet the threshold requirements as an OES for the subsector. This would be a formal notification from the NIS CA where it concludes that an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the service provision on society or the economy or other essential services then that person or organisation could be formally designated by the NIS competent authority as an OES.

If you do not meet or exceed the thresholds or requirements set out in the latest regulations, then you would not be deemed an OES insofar as this guidance relates unless the NIS competent authority specifically designates you as such.

Where an organisation is in doubt whether they are an OES or not it would be prudent to seek independent legal advice and engage with the competent authority on the advice received.

7 Operator of Essential Service Responsibilities

7.1 Compliance with the NIS Regulations

An OES should familiarise themselves with the relevant duties and consider the various steps required to achieve and maintain compliance with the latest revision of the NIS Regulations. It is important to seek their own legal advice and guidance on their obligations. A number are highlighted here:

- Notification as an OES under regulation 8 and where applicable 8A
- Manage risk and impact to essential service as per regulation 10
- Notify competent authority of incidents as per regulation 11
- Cooperate with Enforcement powers as per

- regulation 15 information notices,
- regulation 16 power of inspection,
- regulation 17 enforcement notices; and
- regulation 18 penalty notices;

Regulation 8 and 8A places obligations on an organisation to assess if they are an OES and if so to notify the competent authority.

Where an organisation is registered outside the UK but operates in Northern Ireland there is an obligation for an OES to provide a UK contact and person to act on behalf of the OES with the competent authority pursuant to regulation 8A.

7.2 Security duties to protect continual delivery of essential services

Regulation 10 set out the obligations on an OES to manage risk and impact to the continual delivery of the essential service. As a general rule this is identifying, by using a risk-based methodology, the essential services you provide, the scope of the service and understanding of the dependencies of this service on network and information systems.

The regulations define network and information systems as:-

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

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; 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;

and where these systems are key to the delivery of an essential service.

As a general rule if a device or system needs connected to a network, Wi-Fi, internet, mobile etc or has a digital, electronic or physical interface for the transfer of information or configuration e.g. an API, usb, dongle, laptop or tablet connection then this is something to consider in terms of scope and management of risk and implementation of risk controls. An OES should then query is this essential for the continued delivery of the essential service? if so then the organisation should consider it in scope and effectively manage the risks to it.

This can be achieved with the implementation of a management system for security and resilience which:

1. Employs appropriate risk-based processes for identifying and managing the scope of the essential service and 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 A 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 or service 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.

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 to 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)

OES are encouraged to look at current advice and guidance from suppliers, industry, CPNI and NCSC and other relevant sources on secure practices relevant to their sector and systems.

7.3 OES duties concerning security incident

The NIS Regulations state that an incident is “any event having an actual adverse effect on the security of network and information systems”

Under Regulation 11 (1) – (4) of the NIS Regulations an OES must notify the NIS competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides.

This must be done without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred providing key details of the incident to DoF as the NIS competent authority at NIS.incident@finance-ni.gov.uk using the incident form on the website Northern Ireland NIS Competent Authority.

Information is limited to information which may reasonably be expected to be within the knowledge of that OES. It is possible that complete information will not be available at the time of the report. In such cases, additional information should be provided as it becomes available, but meanwhile the OES in question should not withhold reporting until more complete information is available. More detail on the incident reporting process will be published on the website incident reporting section.

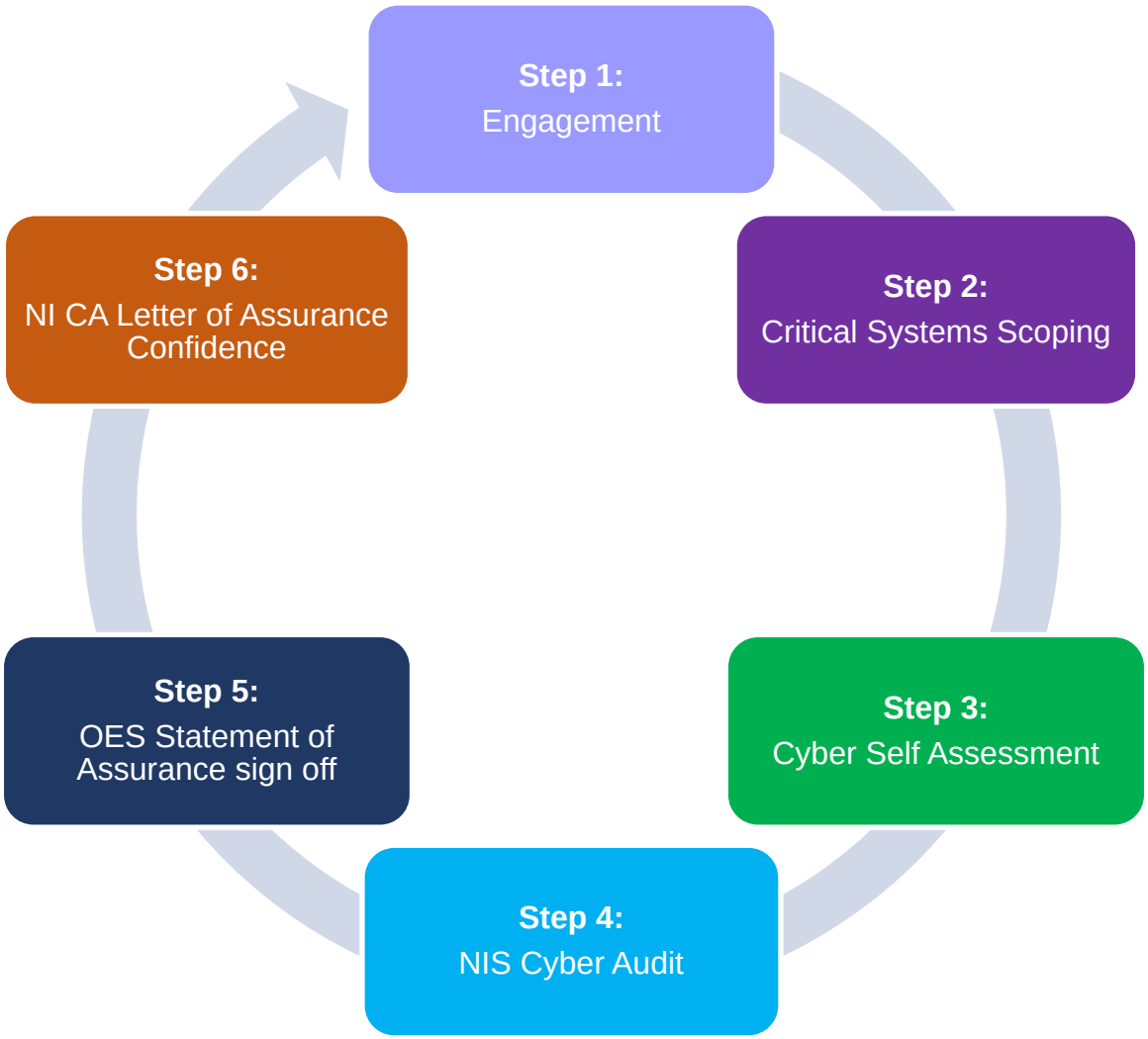
OES should note that the NIS competent authority's role does not include incident response nor does NIS incident reporting to the NIS competent authoritysubstitute responsibilities for reporting to other agencies.

8 DoF NIS Oversight Process

DoF as the NIS competent authority will use the following NIS oversight process to obtain assurances and confidence from an OES on compliance with the NIS Regulations within the sectors and OESs for which they are responsible.

8.1 NIS Oversight Process

The NIS competent authority's six-step oversight process will be applied across all sectors and provides opportunities for OESs to demonstrate compliance with the NIS regulations and also to benchmark the maturity of their network and information systems security management system using the NCSC Cyber Assessment Framework (CAF). The oversight process is a continuous improvement assurance cycle looking to impart a level of confidence with the competent authority on compliance to the NIS regulations and improve security to the provision of essential services to Northern Ireland society and economy and contributes towards compliance to the NIS Regulations.



This process will be more fully documented in the NIS competent authority NIS Oversight guidance.

Step 1 – Engagement
It is the responsibility of an organisation under 8.(2) of the NIS regulations to notify the competent authority that they are an OES.

The NIS competent authority will contact OES to initiate engagement with them. It is our approach to ensure that engagement is a continuous part of this oversight process reinforcing a "prevention rather than cure" and a collaborative approach to regulation compliance within the sectors and with the OES.

Step 2 – Critical Systems Scoping

An OES is ultimately responsible for their own risks and the identification and validation of their essential service and critical systems scope.

DoF would encourage an organisational level risk-based approach to identifying the essential services and scoping of the essential services to ensure that comprehensive full scope boundary for the essential service and supporting network information systems, suppliers, assets, interfaces etc are captured.

An OES should consider a clear and demonstrable methodology to achieve this and ensure all stakeholders deemed relevant by the organisation have been included in defining this (e.g. workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc).

An OES must consider the definition and scope of essential services in the context of the NIS Regulations:-

- where an essential service is defined as "a service which is essential for the maintenance of critical societal or economic activities"; and
- in the context of the thresholds stated in schedule 2 paragraphs 1-9 which are relevant for their sector and sub-sector in which they operate; and
- where the delivery of these essential services relies on network and information systems as defined by
    a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003;
    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; 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; or
- where the competent authority has designated and organisation as an OES under 8(3) of the regulations.

Step 3 – Cyber Assessment Framework Self-Assessment

The NCSC have developed the Cyber Assessment Framework guidance collection[4] which is composed of 14 security and resilience principles, associated guidance, and the cyber 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).

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, industry, and supplier good practices to inform good security and resilience of their services and systems and inform strategic and tactical development plans to remediate risk and vulnerable areas or deal with possible future risks materialising.

Some OES may have adopted security control frameworks (i.e. ISO27001 or NIST 800-53). We acknowledge that there is overlap with this work and the tenants of the CAF. This work is not nugatory work, nor do we want added effort or expense to OES in developing the CAF returns as long as a clear mapping of the outputs of one framework can be clearly demonstrated in the CAF assessment return on how this meets the indicators of good practice. Some work has been completed by NCSC on mapping common frameworks to the CAF.

Step 4 – NIS Cyber Audit – Assure Scheme

This stage will look to provide confidence and assurance to the NIS competent authority on NIS compliance part of which will include the CAF return, scope of the essential service boundary through an audit of the OES.

Under NIS Regulations 16.(1)(c) a competent authority may "direct the OES to appoint a person who is approved by that authority to conduct an inspection on its behalf".

The NIS competent authority will adopt a third-party cyber security audit model where accredited "Qualified Entities" are contracted with by OES via a certified authorisation scheme to perform NIS Audits on behalf of the NIS competent authority who will also determine the scope and terms of the audit NIS competent authority.

"Qualified Entities" mean an accredited supplier certified by the NIS competent authority via an authorisation scheme to carry out NIS audits on an OES. All costs associated with the audit will be paid by the OES.

Step 5 – OES Statement of Assurance

A signed Statement of Assurance will be submitted by the OES which constitutes a commitment from an OES that information provided is complying with the NIS competent authority Oversight Process and that this is an accurate and current representation of their essential service and technical and organisational measures taken to manage risk and minimise impact to that essential service.

---

[4] NCSC CAF guidance - NCSC.GOV.UK

Step 6 – CA Assurance confidence

The letter of assurance confidence will be signed by the NIS competent authority as confirmation that an OES has met the agreed requirements of the NIS competent authority oversight process. It is important to note that this is not a confirmation of compliance with all applicable regulatory requirements; this remains solely the OES organisations responsibility.

9 NI Competent Authority's approach to enforcement.

The NIS competent authority's preferred approach to NIS regulation and administration is "Prevention rather than cure." We would prefer to work collaboratively with OES to ensure compliance and an appropriate and proportionate application of the NIS Regulation rather than taking an enforcement route. However, it is a legal responsibility on an OES to comply with the regulations and where this is deemed not to be the case and appropriate action not taken then as the NIS competent authority, we will look at enforcement approach . Any action will be in line with the regulations and pursuant to Regulation 23 and the general considerations will be taken into account.

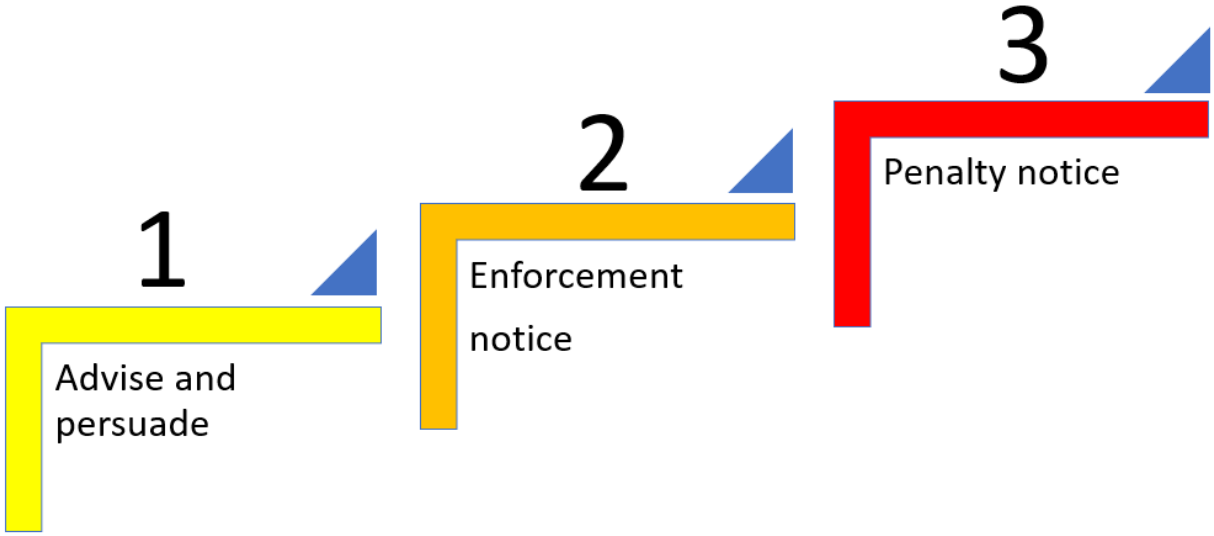
There are a number of enforcement instruments available to the NIS competent authority.

- Information Notices
- Power of Inspection
- Enforcement Notices
- Penalties

The NIS competent authority, depending on severity of a breach, can instigate and enforcement instrument as deemed appropriate. However a stepped approach to enforcement is preferred and, in most cases, will be adopted.

In extreme cases fines of up to £17M can be levied if deemed appropriate.

The process is a 3 stepped approach to enforcement.



The stepped approach that will be taken in the Northern Ireland sectors may be

summarised as follows:

9.1 Step 1: Advise and persuade

When any deficiencies are identified, the initial approach taken by the NIS competent authority will be to engage and discuss this with the OES. This will include discussing what the failing or deficiency is and how and when it can be addressed.

Where more information is needed to conduct a thorough assessment the NIS competent authority may issue information notices requiring the OES to provide specified information to support the assessment.

The NIS competent authority will provide where there is a failure and any remedial actions proposed by the OES and when these actions should be completed. The NIS competent authority may wish to follow-up with further assessments or audits to ensure that these actions have been taken and any failings have been addressed appropriately and proportionately and where appropriate can insist on a partial or full audit under the power of inspection regulation 16.(1).

A stronger line will be taken if these actions fail to be addressed in the agreed timeframe the NIS competent authority may provide a notice of its intention to serve an enforcement notice to avoid where possible the need to progress to any formal enforcement action.

9.2 Step 2: Enforcement notice

Where the initial collaborative approach has not worked and the NIS competent authority has reasonable grounds to believe that the OES is not meeting its obligations the NIS competent authority can levy an enforcement notice. This will set out the failings identified, the steps to be taken and the time period in which they need to be completed.

9.3 Step 3: Penalty notice

Where the OES has failed to take adequate steps to rectify a failure identified in an enforcement notice a notice of intention to serve or to serve a monetary penalty to the OES will be taken. In determining the value of the monetary penalty, the NIS competent authority will consult with a wider stakeholder group and the NIS Oversight and Enforcement panel considering if there was a “material contravention” of the regulations on a case by case basis to inform the enforcement decision and consider the appropriate and proportionate level within the prescribed limit of £17m.

10 Appeals process

An OES can appeal a designation or penalty decisions taken by the NIS competent authority and may appeal to the General Regulatory Chamber (GRC) as the First Tier Tribunal on the grounds set out in regulation 19A(1) around designation or revocation of an OES or the serving of an enforcement or penalty notice.

Appeals can only be made on the grounds set out in regulation 19A(3) where:-

- the decision was based on a material error as to the facts;
- any of the procedural requirements under these Regulations in relation to the

decision have not been complied with and the interests of the OES have been substantially prejudiced by the non-compliance;

- the decision was wrong in law;
- there was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES.

An OES may submit a notice of appeal within 28 days of the date on which the relevant decision or enforcement notice was received. If an OES misses the 28-day deadline, they may submit reasoning for missing the deadline to the GRC. The GRC will make the final decision to hear such an appeal after considering the information provided by the OES.

The GRC will determine the appeal in accordance with regulations after considering the grounds of appeal against 19A(3) and by applying the same principles as would be applied by a court on an application for judicial review.

The First-tier Tribunal may, until it has determined the appeal, and unless the appeal is withdrawn, suspend the effects of the whole or part of any of the decision which the OES is appealing.

If an Enforcement Notice is not suspended in whole or part by the GRC, then it (or relevant parts of it) remain in force and can be enforced.

After considering the OES's appeal, the GRC may confirm any decision to which the appeal relates or quash the whole or part of a decision to which the appeal relates. Where the Tribunal quashes the whole or part of a decision, it will remit the matter back to the Competent Authority with a direction to reconsider the matter and make a new decision having regard to the ruling of the GRC.

The Competent Authority will reconsider the matter having regard to the direction of the GRC. If the Competent Authority makes a new decision, this will be considered final.

The appeal process is governed by the General Regulatory Chamber tribunal procedure rules ("the GRC rules")

The GRC rules set out the procedural rules for proceedings before the General Regulatory Council as the First-tier Tribunal for the NIS Regulations 2018, including by when and how an OES should appeal and how hearings are conducted.

11 Incident reporting and investigation

All OES must notify the NIS competent authority in writing of incidents that has a significant impact on the continuity of the essential services. Following the notification, and allowing for a period of resolution and recovery, the NIS competent authority will decide whether or not the incident requires further follow-up investigation. This may include requesting further details of the incident.

The purpose of these investigations will be to:

i. establish the cause of the incident and assess whether the incident was preventable;
ii. assess whether effective and reasonable risk management was in place;
iii. assess whether the operator had appropriate security measures in place; and
iv. assess how the OES responded to and managed the incident.

Once the investigation has concluded, the NIS competent authority will decide on any appropriate next steps, which could be no action, advice or formal enforcement action.

It is expected that OES will also conduct their own investigation which can form the basis for the conversation between the NIS competent authority and the OES. Additional information may be required by the NIS competent authority and in some cases may instruct the OES to appoint a third-party investigator and/or auditor from an approved list. Where this type of action is required, the intention is that it will be the responsibility of the OES to contract the third party and pay the costs.

The results of such investigations/audits will be shared with the NIS competent authority to determine if further action is required.

It should be noted that simply having an incident is not usually itself an infringement of the NIS Regulations and therefore, does not automatically mean enforcement action will be taken.

A key factor for determining whether enforcement action is required will be whether proportionate security measures and procedures were in place and being followed and whether the OES has responded to any earlier recommendations made by the NIS competent authority, the maturity of their network and information systems security management system, where the NIS competent authority has conducted a post-incident investigation or not having notified the NIS competent authority of an incident that had a significant impact would be an infringement of the NIS Regulations.

Further incident guidance is available on the DoF NIS competent Authority website Northern Ireland NIS Competent Authority.

Appendix 1 – Schedule 2 of the NIS regulations extract.

This is a summarised extract of the NIS Regulation Schedule 2. Although every effort has been made in this guidance to accurately reflect the Regulations it is incumbent on an organisation to refer to the latest Regulation and conduct their own review.

Relevant Sectors	Sub-Sectors	Threshold
Energy	Electricity supply	the holder of a supply licence under Article 10(1)(c) of the Electricity (Northern Ireland) Order 1992(23) who supplies electricity to more than 8,000 consumers; and the holder of a generation licence under Article 10(1)(a) of the Electricity (Northern Ireland) Order 1992 with a generating capacity equal to or greater than 350 megawatts
	Single Electricity Market Operator	the holder of a Single Electricity Market operator licence under Article 10(1)(d) of the Electricity (Northern Ireland) Order 1992
	Electricity Transmission	the holder of a transmission licence under Article 10(1)(b) of the Electricity (Northern Ireland) Order 1992
	Electricity distribution	the holder of a distribution licence under Article 10(1)(bb) of the Electricity (Northern Ireland) Order 1992
	Gas supply	the holder of a supply licence under Article 8(1)(c) of the Gas(Northern Ireland) Order 1996 who supplies gas to more than 2,000 customers.
	Gas transmission	the holder of a gas conveyance licence under Article 8(1)(a) of the Gas (Northern Ireland) Order 1996
	Gas distribution	the holder of a licence under Article 8(1)(a) of the Gas (Northern Ireland) Order 1996.
	Gas storage	the holder of a licence under Article 8(1)(b) of the Gas (Northern Ireland) Order 1996.
	Operation of liquid natural gas (LNG)	the holder of a licence under Article 8(1)(d) of

	facilities	the Gas (Northern Ireland) Order 1996.
	Gas processing	an operator of a relevant gas processing facility or facility with a throughput of more than 3,000,000 tonnes of oil equivalent per year; or a relevant upstream pipeline and associated infrastructure connected to and operated from a relevant gas processing facility with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
	Gas petroleum production	a relevant offshore installation which is part of a petroleum production project (other than a project primarily for the storage of gas) with a throughput of more than 3,000,000 tonnes of oil equivalent per year. or a relevant upstream petroleum pipeline connected to and operated from such an installation with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
	Oil conveyance by pipeline	For the conveyance of oil any operator of a relevant upstream petroleum pipeline which has a throughput of more than 3,000,000 tonnes of oil equivalent per year excluding natural gas. or
	Crude oil based Fuel transmission by pipeline	operators of any pipeline with throughput of more than 50,000 tonnes of crude oil based fuel per year
	Oil processing	an operator of a facility or pipeline [relevant oil processing facility or relevant upstream pipeline connected to and operated from a relevant oil processing facility] with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
	Crude oil based fuel production, refining, storage and transmission	For crude oil based fuel [production, refining, onshore storage and transmission] – the operator of a facility which has a storage capacity of greater than 50,000 tonnes of crude oil based fuel
	Petroleum production	For petroleum production projects (other than those used primarily for storage of gas) a

		relevant offshore installation or relevant upstream petroleum pipeline connected to and operated from such an installation with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
Transport	Rail transport operator	any railway undertaking in Northern Ireland.
	High-speed rail	an operator of a railway asset for high-speed rail services.
	Light rail	[Trams, metros, tube] operator with more than 50 million annual passenger journeys
	International rail	a rail service where all carriages on the train cross a border of the United Kingdom and that of a Member State, and where the principal purpose of the service is to carry passengers or goods between stations located in the United Kingdom and a station in at least one EU Member State
	Road transport services	road authority responsible for roads in the United Kingdom that have vehicles travelling more than 50 billion miles in total on them per year
	Road transport intelligent transport systems	road authority that provides Intelligent Transport Systems services which covers roads in the United Kingdom that have vehicles travelling more than 50 billion miles in total on them per year
Health	Healthcare	the Health and Social Care Trusts within the meaning of “HSC Trust” in section 31 of the Health and Social Care (Reform) Act (Northern Ireland) 2009.
Water	Drinking water supply and distribution	supply of potable water in the United Kingdom is the supply of water to 200,000 or more people.

Table 1. extract of OES thresholds from NIS Regulations Schedule 2