NIS | Competent Authority

Department of Finance

An Roinn Airgeadais

www.finance-ni.gov.uk

NETWORK INFORMATION SYSTEMS REGULATIONS 2018

NIS Competent Authority Oversight Process

October 2022

NIS Competent Authority for Northern Ireland

Contents

1 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. Referred to in this guidance as the NIS competent authority.

This guidance will help an organisation understand the NIS competent authority's approach to administration and oversight of the NIS regulations in relation to these regulated sectors.

The guidance underpins the collaborative engagement approach sought between the Department of Finance and OES community to ensure compliance with the NIS Regulations and ultimately better overall protection of essential services within the health, drinking water supply and distribution, 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 DoF 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.

2 NI Competent Authority Oversight Process

Oversight of the NIS Regulations is the responsibility of the designated Competent Authority to ensure that the operators of essential services within the health, drinking water supply and distribution, road and rail transport and energy sectors are compliant with the NIS regulations.

The Department of Finance as the designated NIS competent authority for these sectors has a 6-step regulatory oversight process that will be applied across all sectors.

The NIS competent authority's six-step oversight process will be applied across all sectors and provides opportunities for OESs to demonstrate confidence of 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.

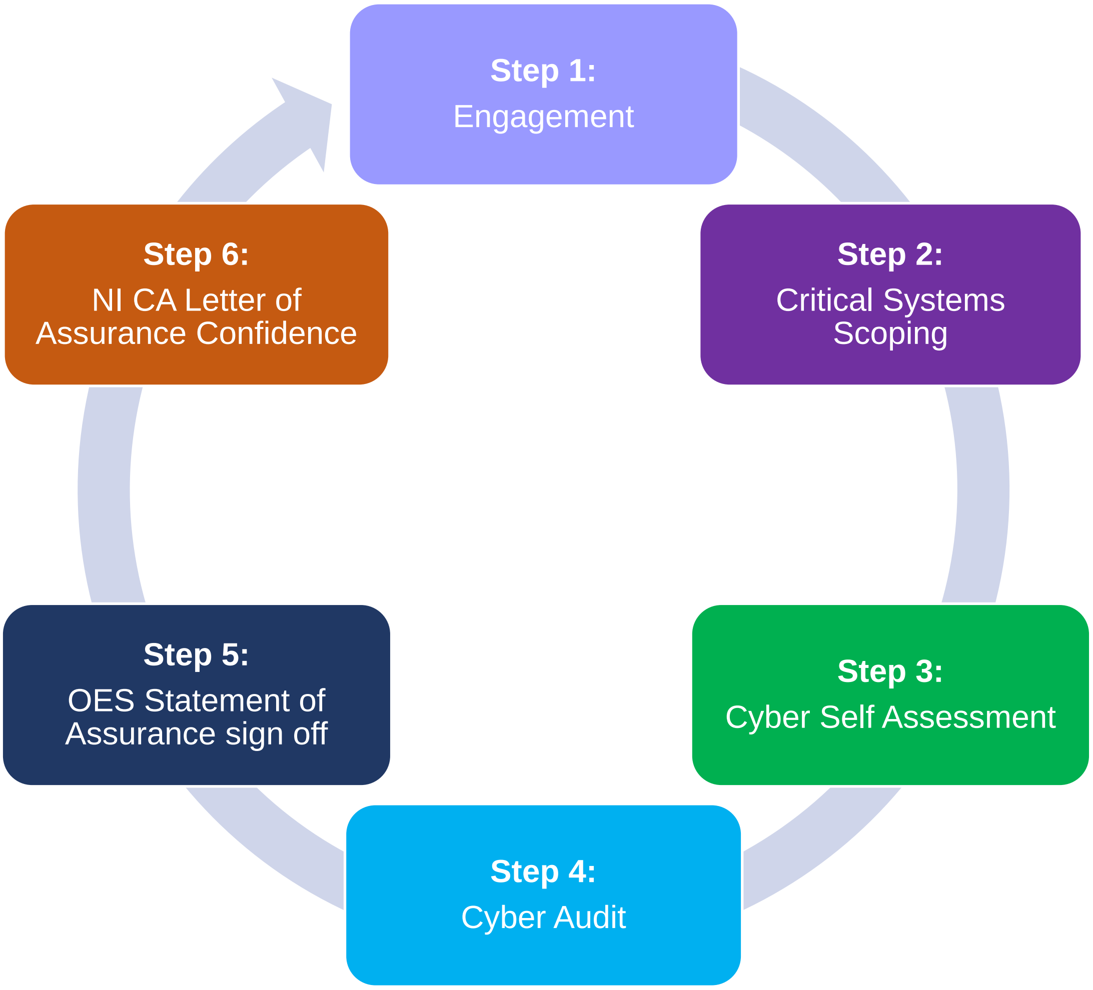

Figure 1. Oversight process

Through this process as the NIS competent authority we want to adopt a "prevention rather than cure" approach to regulation and through good application of the regulations prevent breaches or impact to services within the sectors we are responsible for. There is no one step more important that the others as combined they provide a constructive approach to application and monitoring of the NIS regulation compliance.

2.1 Step 1 – Engagement

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

As the NIS competent authority we will also do some due diligence with government, other regulators and key industry bodies to identify and consult with organisations that fall within the scope of the Regulation. There may also be occasions due to the risk of an organisation service they deliver, within the regulated sectors, may be such that the NIS competent authority will designate them an operator of essential services and as such they will have responsibilities under the NIS Regulation.

As the NIS competent authority initiation of the engagement step will be in a formal contact with the organisation to commence the oversight process with the intention to reinforce a collaborative approach to regulation compliance and engagement within the sectors.

The regulator will engage with the OES outlining the following key guidance complementing the NIS Oversight and assurance lifecycle:

- Cyber Security Responsible Manager Nomination Form;
- DoF NIS CA OES NIS Guidance;
- DoF NIS CA Oversight process guidance;
- Considerations on Essential Service Management of Risk;
- Cyber Assessment Framework (CAF) Guidance v3.1;
- Cyber Assessment Framework template

As part of the collaborative approach the NIS competent authority will engage at a sectoral and OES level to work with organisations towards better compliance outcomes based on the "prevention rather than cure" approach.

2.2 Step 2 – Critical Systems Scoping and risk assessment

An OES is ultimately responsible for delivering its essential services and in so doing protecting society and the economies of Northern Ireland. They are solely responsible for management and identification of their essential service, the scope of the essential service and the risks and risk levels that may impact this service and the identification and validation and critical systems scope.

An OES must consider the 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:-
  - an electronic communications network within the meaning of section 32(1) of the Communications Act 2003;
  - 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
  - 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.

2.2.1 Essential service scope

An OES must be able to demonstrate with evidence that a sound and robust methodology was followed, included all stakeholders deemed relevant by the organisation for the essential services (e.g. workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc) to define the essential service delivered by the business. From the business definition a full scope of the critical information systems, networks, assets, suppliers etc necessary in supporting this service.

2.2.2 Essential service risk management

Regulation 10 set out the obligations on an OES to manage risk and impact to the continual delivery of the essential service. The NIS competent authority does not mandate the use of any specific methodology for risk management. However, OES must use a consistent risk management methodology that covers the entirety of their NIS scope. An OES must explain their risk management methodology and should align to industry good practice and risk management standards where practicable. Example risk management standards include but are not limited to the ISA 62443-3-2 Security Risk Assessment and System Design standard, National Institute of Standards and Technology's (NIST) Risk Management Framework, ISO27005 and Information Security Forum's IRAM2 methodology. In addition to the standards detailed above, OES are encouraged to consider the risk management guidance published by the NCSC and CPNI as well as any OSINT information and how this, if used, contributes towards management of risk to the network information systems essential to the essential service delivery to an acceptable level determined by the OES.

An OES must take appropriate and proportionate technical and organisational measures to manage risks and limit impact posed to the security of the network and information systems on which their essential service relies. This includes taking 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 and must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

OESs must have regard to any relevant guidance issued by the relevant competent authority.

2.2.3 Critical Systems Identification

From the essential service scope, which could include 3rd parties operating on behalf of the OES, the OES must identify and document all critical network and information systems (including relevant people, processes, technology and data) that the essential services rely on. This should include the relevance of that service network information systems and assets and dependency in delivery of that essential service in terms of confidentiality, integrity and availability of the service so that these can be mitigated or managed in a timely manner with business scope and risk appetite. Some examples of systems that could be in scope are listed in Annex A.

2.3 Step 3 – Cyber Self-Assessment

The NCSC have developed the Cyber Assessment Framework guidance collection[1] 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 to inform which security and resilience changes to make, and how to make them.

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

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

OES that have adopted security control frameworks (i.e. output-based frameworks such as ISO27001 or NIST 800-53) may wish to present the mapping of security controls to CAF outcomes as part of their rationale.

2.4 Step 4 – Cyber Audit

This stage will look to provide confidence and assurance to the NIS competent authority on NIS

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

compliance part of which will include the CAF return, scope of the essential service boundary through an audit of the OES.

As part of 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.

Each certified NIS Supplier must nominate appropriate professionals who are then accredited to conduct a NIS audit on behalf of the OES as directed by the NIS competent authority.

The NIS competent authority will establish an ASSURE scheme which provides a mechanism for the NIS competent authority (in partnership with associated accreditation bodies) to ensure that ASSURE NIS suppliers and ASSURE cyber professionals are accredited to a high standard, are qualified and competent to conduct NIS audits in a consistent professional manner in accordance NIS competent authority's requirements agreed under the Assure scheme.

Each OES, when required to by the NIS competent authority, must procure NIS audit services from an accredited ASSURE NIS Supplier via an approved ASSURE Scheme. OES are to ensure that the organisation used has no direct or perceived conflicts of interest in fulfilling its assurance role with the OES.

During the NIS audit the appointed cyber professional(s) will conduct a NIS compliance audit for your organisation and issue an NIS Audit Report to the NIS CA and OES detailing:

- A validated opinion of NIS compliance based on confidence level scored from Green - 'achieved', Amber - 'partially achieved' to Red - 'not achieved'
- A review of all or relevant parts of CAF submitted by the OES with associated commentary and justification against each CAF outcome, based on the evidence provided by the OES and the audit findings against the indicators of good practice. Using the same confidence level scoring of Green - 'achieved', Amber - 'partially achieved' or Red - 'not achieved'
- Recommendations for the OES to input to and develop a corrective action plan to improve confidence levels where compliance is either Red - "not achieved" or Amber - "partially achieved".

Once the final NIS Audit Report has been submitted to the OES, the ASSURE cyber professional(s) are required to have a "wash-up" call with the NIS competent authority to discuss the ASSURE Cyber Audit.

All costs associated of the Audit will be paid by the OES.

2.5 Step 5 – OES Statement of Assurance sign off

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.

An OES is required to send, a provisional Statement of Assurance to the regulator by the agreed deadline, which must include the following:

- Description and scope of Essential Services;
- CAF assessment
- Independent NIS Audit report conducted on behalf of the NIS competent authority;
- Improvement plan with supporting documents and key milestones; and
- NIS security organisation structure with roles and responsibilities.

The NIS competent authority Compliance and Enforcement team will conduct an analysis of the information provided and request additional supplementary information if clarification is required.

As part of ongoing cyber security oversight process the NIS competent authority Compliance and Enforcement team will engage with the NIS competent authority Compliance and Enforcement panel providing a view of the OES;

- Essential Service
- Importance to Northern Ireland Society and Economy
- Current cyber risks to this service
- How OES manage and address security risk; and
- translate residual gaps into safety, security and/or resilience implications.

Engagement with NIS competent authority Compliance and Enforcement Panel will include briefing the relevant teams and working with the appropriate stakeholders to agree if there is a safety, security, or resilience impact that needs to be addressed.

The NIS competent authority will engage in discussions with the OES to review the Statement of Assurance including any amendments to corrective action plans. Following engagement, an OES will be required to finalise their Statement of Assurance ensuring it is signed by the OES Accountable Manager and returned to the NIS competent authority.

2.6 Step 6 – letter of 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.

Annex A – Scoping examples

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

- Operations management systems;
- Supervisory control and data acquisition systems (SCADA);
- Distributed control system (DCS);
- Local controllers (e.g. programmable and electronic controllers);
- Safety instrumented systems (SIS) and safety-related systems;
- Protection systems;
- Intelligent electronic devices;
- Remote terminal units (RTUs);
- Physical plant and sensing equipment;
- Data centre and cloud systems (e.g. cloud SCADA);
- Demand management and balancing systems;
- Real Time Operation Systems;
- Critical communications including wireless networks; and
- IT Systems deemed critical by the business for the delivery of essential services.
- Examples of ancillary systems that may be in scope include:
- Utility systems (e.g. Heating, Ventilation, and Air Conditioning (HVAC); Power supply; chilled water, Instrumentation air, etc.);
- Trading systems and interfaces;
- Backup control centres;
- Backup systems;
- Remote access solutions;
- OT configuration management;
- Change management systems;
- OT asset management systems;

- Cloud/on premise-based monitoring or management systems;
- Building management systems; and
- Physical and cyber security systems.

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

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

Scope boundaries and interfaces

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

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

These network and information systems should be included within scope descriptions or diagrams with necessary use of boundaries, interfaces, and system groupings to illustrate these cases.