NIS | Competent Authority

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

NIS Competent Authority Audit Guidance

Table of Contents

1 Introduction 3
2 Purpose 3
3 Use of NCSC Cyber Resilience Audit Scheme. 3
4 NCSC Cyber Resilience Audit Scheme 4
5 Audit Process 5
6 Audit Notification 6
7 Audit Scope 7
8 Security Clearance 7
9 Access to Information 7
10 Conflict of Interest 7
11 Procurement 8
12 Pre-audit Meetings 9
13 Audit Conditions 9
14 Audit Reporting 10
15 Audit Report Meeting 11
16 Post Audit Meeting 11
17 Next Steps 11
18 Follow Up Audit 11
19 Audit Quality 12
20 Complaints procedure 12

1 Introduction

This document is intended only for organisations that meet the thresholds to be deemed an OES and for which the Department of Finance (DoF) is the designated NIS Competent Authority under the NIS Regulations 2018. This includes sectors for Energy (Electricity, Gas & Oil), Health, Drinking water supply and distribution, Transport for rail and road in Northern Ireland.

This guidance has been issued by the Department of Finance (DoF) NIS Competent Authority Compliance & Enforcement Branch (NISCA C&E) pursuant to regulation 3 of the NIS Regulations 2018[1]

The NIS Competent Authority will use a third-party cyber security audit model where organisations are accredited via the NCSC Cyber Resilience Audit Scheme. These organisations can be contracted by the OES to perform NIS audits on behalf of the NIS Competent Authority pursuant to regulation 16.(1)(c) where 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 determine the scope, any additional selection criteria and scope of the audit that is to be carried out on its behalf.

In line with regulation 16(3)(a) all reasonable costs associated with the audit will be paid by the OES.

2 Purpose

The purpose of this document is to provide guidance to organisations designated as Operator of Essential Service (OES) under the NIS regulations 2018 or have been deemed an OES by the Competent Authority under regulation 8(3).

This guidance will inform an OES of the NIS Competent Authority audit process and how to appoint an audit organisation from the NCSC Cyber Resilience Audit Scheme, to act on behalf of the NIS Competent Authority.

3 Use of NCSC Cyber Resilience Audit Scheme.

The NIS Competent Authority will use the NCSC Cyber Resilience Audit (CRA) Scheme as a list of approved organisations to conduct a NIS compliance audit on its behalf as permitted in regulation 16(1)(c) and as part of its oversight process in determining the compliance with OES security duties as set out in regulation 10.

Before considering the procurement of a compliance audit, the Operator of Essential Service must ensure that the organisation conducting the audit is registered under the NCSC CRA

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

Scheme as an Assured Service Provider. Further information on the scheme can be obtained at the following webpage: Introduction to Cyber Resilience Audit - NCSC.GOV.UK

Operators of Essential Service must take note that where the NIS Competent Authority has placed additional requirements above that of the NCSC CRA Scheme, they must ensure that these requirements have been included in their procurement documentation.

These additional requirements will be set out in the audit notification from the NIS Competent Authority to the OES.

4 NCSC Cyber Resilience Audit Scheme

The Cyber Resilience Audit Scheme gives consumers of the scheme confidence in companies that have been assessed as meeting the NCSC standard for delivering independent CAF-based audits.

4.1 Who is it for?

The NCSC Cyber Resilience Audit Scheme is aimed primarily at Oversight Bodies (regulators or government policy organisations) with responsibility for understanding cyber resilience of organisations within the sector for which they are responsible.

NIS Competent Authority is a Scheme Partner within this scheme.

4.2 NCSC CRA Scheme Roles and Responsibilities.

The NCSC Cyber Resilience Audit Scheme has the following roles and responsibilities.

Role	Who?	Scheme Responsibilities for this role include:
Scheme Owner	NCSC	a. publishing and maintaining the Cyber Resilience Audit standard and associated documentation. b. assuring service providers are in line with the standard and associated documentation. c. training and pre-briefing for service providers on the CAF. d. publishing a list of Assured Service Providers. e. monitoring the operation of the scheme. f. complaints and disputes where they relate to the supplier's assured status. g. working with Scheme Partners to develop and improve the scheme. h. enabling co-ordination with Scheme Partners and Assured Service Providers.
Scheme Partner	A cyber oversight body that uses the	a. defining how the scheme is used and communicated in their sector. b. defining how Assured Service Providers should conduct and report on audits in their sector.

	scheme in their sector	c. (optionally) defining additional sector-specific requirements or additional assurance. d. (if c is implemented) sharing any additional requirements or assurance as part of the co-ordination of the scheme. e. requiring or recommending, as good practice, that Sector Organisations should have cyber resilience audits carried out by Assured Service Providers. f. responding to complaints and disputes where they relate to individual audits and how they are conducted against any sector specific direction. g. working with the Scheme Owner to develop and improve the scheme.
Assured Service Provider	Assured commercial suppliers of cyber audit services	a. meeting the CRA Scheme standard, associated documentation, and any membership obligations. b. (If required) meeting additional sector specific requirements to provide services in specific sectors. c. following any Scheme Partner direction describing how audits must be conducted or reported on.
Sector Organisations	Organisations which are regulated or overseen by Scheme Partners.	a. (if required) contracting with Assured Service Providers as and when directed by Scheme Partners. b. meeting any requirements set out in the scheme standard and associated documentation.

5 Audit Process

The NIS Competent Authority will use the following audit process as an integral part of its oversight process and as a means of assessing compliance with the NIS Regulation security duties of the OES outlined in regulation 10.

6 Audit Notification

The NIS Competent Authority will inform the OES that a NIS compliance audit is required the scope of which will include all the essential services provided by the OES. The NIS Competent Authority will provide the following information:-

- The scope of the audit[2]
- Any additional criteria to be included in selecting the CRA Assured Service Provider. For Example:-
    - ISA/IEC 62443 OT qualified/experience.
    - Requirement to undertake NIS CA specific induction training.
    - Requirement for NIS CA staff to be included in the audit team.
    - Reporting and access to audit information post audit.
    - De-briefing on completion of audit.
    - Other criteria as deemed appropriate.

  Where additional information is requested, the OES should validate that the Assured Service Provider has met the additional criteria as part of their procurement due diligence.
- The date for the Audit to be completed by.

It is intended that a reasonable notification timeframe will be given to procure and complete the audit.

[2] Note: - It is important that the contracted scope of work is clearly defined. If during the pre-audit meeting the scope varies significantly from that of the original contract, the operator and the Assured Service Provider may need to agree any commercial implications with the OES.

7 Audit Scope

The NIS Competent Authority expectation is that a full CAF assessment for the OES essential service to be completed in no more than two phases and no longer that over a two-year period as part of its oversight process. The scope for each engagement will be determined by the NIS Competent Authority and shared with the OES as part of the Audit Notification stage.

The OES is expected to be familiar with the scope of the essential services they provide and the critical network and information systems that the essential services rely on.

The OES must ensure that the Assured Service Provider is clearly informed of the scope of the OES's essential services. This should include as a minimum a definition of the essential services, critical functions and supporting critical systems, services and suppliers that underpin the essential service. The minimum security standard is defined by the relevant CAF specific sector profile being used for the NIS Compliance Audit.

In some cases, a specific audit may be required in response to a change or incident, and a more limited scope may be set by the Competent Authority. In these cases, the scope and timeframes will be agreed between the Competent Authority and the OES prior to the audit going to procurement.

8 Security Clearance

The NIS CA delegates the determination of whether security clearance is a requirement for Assured Service Providers to the OES. The OES must ensure that Assured Service Providers can only subcontract to other companies under the CRA Scheme operating at the security level determined necessary by the OES for the Audit.

9 Access to Information

The OES should ensure that provision is made to secure and retain all information collated by them and the Assured Service Provider as part of the audit, including Auditor notes, determinations and qualifications, and that it will be made available to the NIS Competent Authority if requested during the audit or up to **four** years after the audit has been completed.

10 Conflict of Interest

Conflicts of interest must be handled as follows:

The OES should seek to avoid using an Assured Service Provider that may give rise to a conflict of interest. Examples of potential conflicts of interest include but are not limited to:

i) An Assured Service Provider having interests in products or services covered under the scope of an Audit;
ii) An Assured Service Provider conducting an audit of an OES for whom they have implemented or consulted on any of the Cyber elements covered in the scope of the Audit, where it could be assessed or provided as evidence;

iii) Personal relationships between members of staff responsible for the management of or undertaking an Audit and staff within the OES organisation.

Where Assured Service Providers subcontract work relating to an audit, 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 on the Audit as a result.

The OES must notify the Competent Authority if they become aware of or suspect an actual or potential conflict of interest and any mitigations where possible . Failure to notify could invalidate the audit. The NIS CA can assess the conflict-of-interest case and provide direction.

11 Procurement

The OES will use NCSC Cyber Resilience Audit Scheme in procuring an Assured Service Provider to complete an on-site compliance audit of the essential service and supporting network and information systems. The audit outcome will inform the Competent Authority of the OES compliance with the security duties of operators of essential service outlined in the NIS Regulations This will be based on the NCSC Cyber Assessment Framework (CAF) as the standard for compliance against an agreed sector specific profile. The NCSC CAF version and sector profile to be used in the audit will have been agreed with the OES and outlined in the Audit Notification.

The procurement approach taken to procure from the CRA Scheme list of organisations will be entirely at the discretion of the Operator of Essential Service, (e.g. Direct award or competitive tender), provided the supplier selected is registered on the NCSC CRA Scheme and there is no conflict of interest. While the Scheme provides a level of assurance, it is expected that the OES will conduct their own commercial due diligence as part of their supplier assurance procurement activities.

Where the NIS CA has additional requirements, the OES will be informed of these as part of the Notification stage and must be included in the procurement criteria.

Where the OES has additional requirements not specified under the NCSC Cyber Resilience Audit scheme or in the NIS CA Notification (e.g. security clearance), these should be discussed directly with any prospective suppliers during the procurement process.

11.1 Award of contract notification.

The OES must inform the NIS Competent Authority once a contract with a CRA Assured Service Provider has been agreed. The following details must be forwarded:-

- the selected Assured Service Provider organisation details
- Audit Charter
- Date of commencement
- Date of completion
- Suggested date of pre-audit meeting (allow 4 weeks lead in time)
- Draft Audit Plan

These must be emailed to nis.ca@finance-ni.gov.uk. Failure to inform the Competent Authority before the audit is commenced may result in the audit being invalidated.

An NCSC CRA Assured Service Provider must conduct the compliance audit in line with the expectations and conditions set out in section 11 and the NCSC Cyber Resilience Audit scheme standard.

12 Pre-audit Meetings

Prior to a compliance audit commencing it is recommended that the Assured Service Provider receives an organisational brief from the OES in advance of the audit commencing to ensure correct preparation and planning for the audit.

The Competent Authority will meet with the Assured Service Provider before the audit commences. The Assured Service Provider must attend this pre-audit meeting failure to do so will invalidate the audit. The Competent Authority will emphasise that the Assured Service provider is acting on their behalf as part of the Audit and provide the OES current CAF self-assessment and NIS CA feedback for discussion. There will also be an opportunity for clarification of areas where the Assured Service Provider may require further direction. Previous CAF reports may be shared with the Assured Service Provider in advance of the audit commencing.

Should the contracted scope of work vary significantly from that of the original contract as a result of the pre-audit meeting, the operator and the Assured Service Provider may need to agree any commercial implications with the OES.

13 Audit Conditions

The audit is an independent physical validation of the Operator of Essential Service current security posture using the NCSC CAF version 3.2 in combination with the sector specific profile as the minimum standard to be met by the OES. The results of the compliance audit do not constitute any approval or decision by the Assured Service Provider as to the operator's compliance or overall adequacy with applicable regulatory requirements. Decisions relating to an entity's compliance with the regulatory requirements can only be made by the Competent Authority. The NIS Competent Authority may wish to attend all or part of the audit as necessary.

The compliance audit must:

- Be fact-based, impartial and conducted with the highest level of integrity;
- ensure consistency between the scope of the critical service and list of critical systems and the security boundary provided by the OES;
- be evidence-based by observing processes in practice, sampling, conducting interviews, and reviewing policies and other relevant documentation provided by the OES;

- report an expert opinion of 'achieved', 'partially achieved', 'not achieved' or 'not relevant' with associated commentary against each CAF Contributing Outcome and indicators of good and 'not good' practice;
- report where applicable, recommendations, mitigations, remediations or good practice; and follow the latest guidance produced by NCSC and NIS Competent Authority.

The Assured Service Provider audit team must not:

- Complete a compliance audit where there is a conflict of interest;
- seek to alter, by increasing or decreasing, the critical service scope as defined by the associated OES; but comment on the suitability of this scope should be made.
- perform any type of testing (e.g. penetration testing) during a compliance audit, unless otherwise explicitly agreed by the OES;
- amend in any way an OES's completed parts and NIS Competent Authority feedback of the CAF self-assessment; or
- provide confirmation or expectation on whether an OES is complying with the NIS Regulations 2018.

14 Audit Reporting

The Assured Service Provider will provide a report to communicate the results to the OES and NIS Competent Authority upon completion of the engagement.

The following report audit format should be used to provide this information:

- Report Title;
- Name of OES Assured Service Provider;
- Applicable report dates e.g. report approval date and, date and duration of the audit;
- name of all Assured Service Provider Audit Professionals conducting the audit, their role, and their signatures;
- Statement that this is an independent compliance audit carried out on behalf of the NIS Competent Authority;
- Executive Summary;
- Statement of standards and methodology used throughout the audit.
- Statements of audit procedures, sampling, audit risk;
- Any necessary disclaimers;
- Statement of any auditor concerns, reservations, or qualifications to the audit;
- summary table showing OES self-assessment and compliance audit assessment of Contributing Outcome achievement; audit observations, and highlighting any deviations from the latest OES CAF self-assessment;

- Detailed findings and opinion listed against NCSC CAF Contributing Outcomes and indicators of good and 'not good' practice;
- An assessment rating based on evidence against each Contributing Outcome;
- List of audit activities including evidence reviewed and interviews conducted;
- where applicable any findings and recommendations;
- Remediation suggestions that might support future remediation plans;
- Date of scheduled Post Audit meeting with the OES and Competent Authority;
- Provisional date of Follow Up Audit.

15 Audit Report Meeting

Upon completion of the Audit a report meeting will be held between the Assured Service Provider, the OES and the NIS Competent Authority. This meeting will review the report findings and recommendations, where applicable, the aim of which is to convey a comprehensive understanding of the OES security posture against the minimum-security standard and provide an opportunity to clarify any points in the report in preparation for the development of a remediation plan and agree the date of the Post Audit Meeting, where necessary.

16 Post Audit Meeting

The Post Audit meeting will be between the NIS CA and the OES to agree a corrective and remediation action plan with agreed timescales to meet or exceed the minimum-security standards set by the NIS Competent Authority.

17 Next Steps

The NIS Competent Authority will monitor the progress against any audit findings, recommendations remediation plan, where applicable, as part of its ongoing engagement with the OES. The NIS competent authority reserves the right to consider any enforcement action necessary to ensure that corrective action is taken in a reasonable and timely manner.

18 Follow Up Audit

The OES will make provision for the same Assured Service Provider to provide a Follow Up Audit against the Audit findings, recommendations and agreed remediation plan. It is the intention that the output of this report will be provided to the NIS Competent Authority as a measure of the OES posture with the minimum-security standards set by the NIS Competent Authority.

The NIS Competent Authority will set out timeframes for the Follow Up Audit will need to be completed.

19 Audit Quality

Assured Service Providers must have an audit methodology and quality control processes in place to ensure quality and consistency of audits. This must include ensuring that the sections in the compliance audit report are completed in line with NCSC Cyber Resilience Audit Scheme standard and industry or international recognised quality standards e.g. ISACA IT Audit Framework or ISO 27007.

The NIS Competent Authority will provide feedback to Cyber Resilience Audit Assured Service Providers and the NCSC on the compliance audit including report documentation, to ensure continuous improvement of the Cyber Resilience Audit Scheme.

Where the audit and documentation are not completed to a satisfactory standard the Competent Authority may take action including, but not limited to, the following:

- Requiring the Assured Audit Service Provider to complete the audit again at their cost.
- Requiring the Assured Audit Service Provider to complete documentation again at their cost.
- Recommending suspending the Assured Audit Service Provider to the NCSC.

20 Complaints procedure

Where there is a dispute the OES and the Assured Service Provider should first try to resolve the dispute directly. If no resolution can be reached the OES or the Assure Service provider should notify the NIS Competent Authority at NIS.CA@Finance-NI.Gov.uk.

All complaints will be investigated in a competent, diligent and impartial manner. The Competent Authority will contact the relevant parties and review the dispute, requesting further detail where necessary, and come to a decision. The Competent Authority will communicate the rationale and decision to the OES and the Assured Service Provider.