Llywodraeth Cymru
Welsh Government

GUIDANCE

The Network and Information Systems Regulations 2018: guidance to the health sector in Wales

How health care providers in Wales should implement the NIS cyber security regulations.

First published: 15 March 2021

Last updated: 15 March 2021

Contents

Background

Application of NIS Regulations within Healthcare in Wales

Roles and Responsibilities

Managing Security Risks in Essential Services

Identification of Incidents by Operators of Essential Services (OES)

Responding to Incidents

Cyber Security Oversight

Enforcement

Appeal to the First-Tier Tribunal

Contacts

Annex 1: National Cyber Security Centre (NCSC) NIS Security Principles

Annex 2: Links to Further Guidance and Information

Background

The **EU Directive on Security of Network and Information Systems** (known as the **NIS Directive**), adopted by the European Parliament on 6 July 2016, provides legal measures to protect essential services and infrastructure by improving the security of their Network and Information Systems.

The aim of the NIS Directive is to instil a culture of security across sectors which are vital for our economy and society and moreover rely heavily on technology; such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Organisations in these sectors identified by the Member States as operators of essential services must take appropriate security measures, and notify serious incidents to the relevant national authority. Also key digital service providers (such as search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the NIS Directive.

The UK has implemented the requirements of the NIS Directive through the **Network and Information Systems Regulations 2018** (NIS Regulations); a UK-wide set of Regulations which came into effect on 10 May 2018. The NIS Regulations seek to ensure that 'essential services' have adequate data and cyber security measures in place.

The Regulations have played a key part in delivering the UK's **National Cyber Security Strategy 2016-2021** and putting in place an effective regulatory framework to protect the UK's Critical National Infrastructure.

The **Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019** amends the NIS Regulations in UK Law to take into account the UK exiting the EU, and the changing landscape of cyber security brought about by Brexit and amendments to the NIS Directive.

As Welsh Ministers were not designated under section 2(2) of the European Communities Act 1972 in relation to electronic communications, the NIS Regulations were made by the UK Government's Secretary of State and not Welsh Ministers.

Application of NIS Regulations within Healthcare in Wales

As Competent Authority for the health sector in Wales, Welsh Ministers will be responsible for overseeing the operation of the NIS Regulations within the sector. This includes taking enforcement action where necessary. The NHS Wales Cyber Resilience Unit, hosted within Digital Health and Care Wales (DHCW) will produce guidance for operators of essential services, and provide specialist support and guidance to Welsh Ministers in relation to the NIS Regulations. Links to this guidance can be found at **Annex 2.**

The National Cyber Security Centre (NCSC) are the UK technical authority under the NIS Regulations, and are therefore responsible for supporting operators of essential services and the competent authorities by publishing guidance and acting as a source of technical expertise.

This guidance applies to those who fall under the scope of NIS Regulations, however, the principles which it outlines can be applied by all healthcare settings in Wales as best practice.

Roles and Responsibilities

Competent Authorities

Welsh Ministers are Competent Authority on implementation of the **UK's NIS Regulations** in devolved health services in Wales (including hospitals, private clinics and online settings).

Competent Authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region;
- preparing and publishing guidance to assist Operators of Essential Services (OESs) or Relevant Digital Service Providers (RDSPs) in meeting the requirements of the NIS Regulations;
- establishing the identification thresholds for the OESs in their sector or region;
- keeping a list of all OESs who are designated, including an indication of the importance of each operator; keeping a list of all revocations;
- consulting and cooperating with each other, the Computer Security Incident Response Team (CSIRT), national Single Point of Contact (SPOC) and Information Commissioner's Office (ICO);
- assessing the compliance of operators to the requirements of the NIS Directive;
- determining the thresholds for reportable incidents in their sectors or region;
- cooperating with other Competent Authorities to provide consistent advice and oversight to OESs or RDSPs;
- receiving incident reports;
- making sure that there are processes in place for non-cyber incidents and issuing guidance to support companies dealing with non-cyber incidents;
- incident investigation; and
- enforcement, including issuing notices and penalties, of the requirements of

the NIS Regulations.

NHS Wales Cyber Resilience Unit

Welsh Ministers have asked the new Digital Special Health Authority Digital Health and Care Wales (DHCW), and in the interim the NHS Wales Informatics Service (NWIS), to support the implementation of the NIS Regulations on its behalf, utilising their cyber security expertise.

The NHS Wales Cyber Resilience Unit has been established to provide this challenge, support and assurance function, hosted within DHCW with separated governance and reporting.

The Unit will have delegated authority to operationalise the NIS Regulations on behalf of Welsh Ministers. It will have oversight of NIS assessments, and the associated action plans to remediate any gaps which those assessments identify. The Unit will also provide operational support and advice for those completing the NIS reporting framework set out by Welsh Ministers, and supporting operators of essential services in identifying and reporting a NIS incident. The Unit will also be responsible for reporting on the status of the NHS Wales cyber posture against the NIS Regulations to Welsh Ministers as Competent Authority.

Computer Security Incident Response Team (CSIRT)

The National Cyber Security Centre (NCSC) is the Computer Security Incident Response Team (CSIRT) under the NIS Regulations.

The CSIRT's role is to provide incident support and assistance to OESs and RDSPs on cyber matters, and their support is available 24/7. The CSIRT role is to:

- monitor security incidents at national level
- provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about threats, risks and security incidents
- respond to security incidents
- provide dynamic risk and incident analysis and situational awareness

In the event of an incident, an Operator of Essential Services (OES) or Digital Service Provider (RDSP) must continue with their function of incident management and NCSC will provide a level of assistance based on the impact and cause of the incident.

Welsh Ministers expect that in the event of an incident organisations also contact the NHS Wales Cyber Resilience Unit who can provide additional support and manage the escalation of reporting to Welsh Ministers.

Welsh Ministers will inform the CSIRT about any incident that may have a cross-border impact (that is, if the incident is likely to affect other countries). This will also include incidents which affect multiple organisations, sectors or geographic boundaries. Where an incident in Wales has cross border impact, Welsh Ministers and the NHS Wales Cyber Resilience Unit will coordinate with other Competent Authorities in that sector to agree common parameters.

Single Point of Contact (SPOC)

The National Cyber Security Centre (NCSC) will also act as the national single point of contact (SPOC) under the NIS Regulations. The SPOC's role is primarily a liaison role, facilitating cross-border cooperation and communication. The SPOC will submit annual reports to the Cooperation Group containing the number of incidents and the nature of these incidents. The SPOC will also submit biennial reports identifying the number of Operators of Essential Services (OESs) for each subsector.

Relevant Digital Service Providers (RDSP)

The Competent Authority for Relevant Digital Service Providers (RDSPs) is the Information Commissioner’s Office (ICO). RDSPs fall under the scope of the NIS Regulations if they fulfil one or more of the following criteria:

- provide one or more of these services to external bodies or customers:
    - **an online search engine** - a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found
    - **an online marketplace** - a digital service that allows consumers and/or traders […] to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace
    - **a cloud computing service** - A digital service that enables access to a scalable and elastic pool of shareable computing resources
- The organisation’s head office is within the UK, or it has nominated a representative in the UK.
- The organisation is neither a micro nor small enterprise as defined in **Commission Recommendation 2003/361/EC**.

It is possible for an organisation to be both an OES and a RDSP. In this scenario, that organisation will be required to follow both regimes under the NIS Directive.

Only those Relevant Digital Services Providers which provide services to Operators of Essential Services in Wales come under the scope of this guidance.

The NIS Regulations require organisations identified as Relevant Digital Service

Providers (RDSPs) to:

- ensure a level of security of network and information systems appropriate to the risk posed
- prevent and minimise the impact of incidents affecting their network and information systems with a view to ensuring the continuity of those services and
- take into account the following elements:
    - the security of systems and facilities
    - incident handling
    - business continuity management
    - monitoring auditing and testing; and
    - compliance with international standard

More information on RDSPs can be found on the **ICO's website**.

Operators of Essential Services (OES)

The health sector is one of six economic sectors considered “essential” under the NIS Regulations. However, only organisations that can significantly disrupt the delivery of essential services are considered ‘Operators of Essential Services’ under the NIS Regulations.

A Local Health Board or NHS Trust as defined in the National Health Service (Wales) Act 2006 is automatically considered an ‘Operator of Essential Services’ for the health sector in Wales for the purposes of the NIS Regulations. These organisations are:

- Aneurin Bevan University Health Board
- Swansea Bay University Health Board
- Cardiff and Vale University Health Board
- Hywel Dda University Health Board

- Cwm Taf Morgannwg University Health Board
- Betsi Cadwaladr University Health Board
- Powys Teaching Health Board
- Welsh Ambulance Services NHS Trust
- Velindre University NHS Trust (including NHS Wales Shared Service Partnership)
- Public Health Wales

In addition to the list above, the following organisations have been designated an OES by Welsh Ministers:

- Digital Health and Care Wales

Welsh Ministers may, by exception, designate an organisation as an OES even if that organisation does not meet the threshold for designation if it provides essential services which would have significant disruptive effects, in accordance with **NIS Regulation 8(1).** Welsh Ministers may also remove an organisation's designation as an OES should the organisation no longer meet the criteria defined in the NIS Regulations for this designation.

This list of OES will be reviewed periodically, including when significant changes occur.

The NIS Regulations require organisations identified as Operators of Essential Services to take appropriate and proportionate measures to:

- manage risks posed to the **security** of the network and information systems on which their essential services rely
- prevent and minimise the **impact** of incidents on the delivery of essential services and
- **report** serious network and information incidents that impact on provision of the essential service.

Managing Security Risks in Essential Services

The National Cyber Security Centre (NCSC) has defined a set of cyber security principles consisting of 14 top-level outcomes, with supporting narratives, which are grouped into four top-level objectives (see **Annex 1**).

These principles should be relevant to all network and information systems supporting the delivery of essential services, where is it assessed the compromise of such a system could result in an impact on the continuity of the essential service.

To support OES in meeting the security principles, the NCSC has also published a collection of guidance. Each of the principles is linked to specific guidance which highlights some of the factors that an organisation will usually need to take into account when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges. Links to this guidance can be found at **Annex 2**.

Welsh Ministers would encourage all health organisations, even if they do not fall under the scope of the NIS Regulations, to take on board the NCSC's principles as best practice.

Identification of Incidents by Operators of Essential Services (OES)

When identifying the specific network and information systems that NIS security requirements apply to, OES should have regard to the specific essential service they provide.

The security requirements only apply to the network and information systems being used in support of delivering an essential service, and where it is assessed that the compromise of such a system could result in an impact on the continuity of the essential service.

Thresholds for Incident Reporting for Operators of Essential Services (OES)

The descriptions below are taken from NHS Wales IT Service Management Service Level Target Policy.

An incident would be NIS reportable from ‘Catastrophic’ to ‘Moderate’ only if the resolution time could not be met, or the other impact descriptions were realised as a result of the event.

Impact	**Report Incident**	**CAF compliance required**	**Description**
Catastrophic	Yes	Yes	Incidents which cause extensive business and/or clinical risk and prevent the user from providing a normal service. These would typically be incidents which: • cause unavailability of the entire service to the end user for 4+ hours • cause incorrect processing of data or errors in a key system function • cause extensive business and/or high clinical risk
Significant	Yes	Yes	Incidents which cause significant business and/or

Impact	Report Incident	CAF compliance required	Description
			clinical risk and limit the ability of the user to provide a normal service. These would typically be incidents which: • cause unavailability of a key module or key system function for 4+ hours • cause incorrect processing of data or errors in a system function • cause a significant clinical risk
Moderate	Yes	Yes	Incidents which cause limited business and/or clinical risk and limit the ability of the user to provide a normal service. These would typically be incidents which: • cause unavailability of a non-key module or system function of a service for 8+ hours • cause a moderate clinical risk
Minor	No	No	Incidents which cause minor or negligible business and/or clinical risk and affect non-key system functions. These would typically be incidents which: • do not cause disruption of services; and • leave all system functions available but restrict performance, causing inconvenience but not disruption of service

Wider Resilience Risks and Identification

The NCSC's NIS principles and guidance are primarily focused on ensuring adequate cyber security risk management. However, OES will also need to take into account broader resilience risks when considering the security of their network and information systems. This includes ensuring they are resilient to wider risks such as loss of power supply, hardware or software failure, physical damage and environmental hazards.

As with cyber risks, it is the responsibility of OES to identify these broader resilience risks to their network and information systems and have appropriate organisational structures, policies and processes in place to understand, assess and systematically manage them. They should be included in any risk management plan which demonstrates those risks have been assessed and understood, and mitigation measures put in place where appropriate.

NIS requirements do not apply directly to the supply chains of OES. It is the OES responsibility to put in place appropriate and proportionate measures, and to ensure that their suppliers have in place appropriate measures, to manage risks of their services being disrupted via their supply chain.

Responding to Incidents

Definitions

The NIS Regulations defines an incident as **any event having an actual adverse effect on the security of network and information systems.** For the Health Sector in Wales, this applies to the provision of **essential services**.

A **network and information system** is:

1. an electronic communications network as defined in the **Communications Act 2003**;
2. 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
3. digital data stored, processed, retrieved or transmitted by elements covered under (a) or (b) above for the purposes of their operation, use, protection and maintenance.

An **essential service** is a service which is essential for the maintenance of critical societal or economic activities

A notifiable incident is **any incident which has an actual adverse effect on the security of network and information systems** and results in an impact on the continuity of the essential service that meets the thresholds set out in this guidance**.**

Security of network and information systems is defined in the NIS Regulations as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

Incident Reporting

Incident Notification

The NIS Regulations also make it mandatory for an OES to notify the Competent Authority of incidents affecting network and information systems that have a significant impact on the continuity of the essential service.

The way the UK Government has chosen to interpret this requirement within the NIS Regulations is to make a distinction between:

- **Reporting for incident management purposes** (which, while strongly recommended, will continue on a voluntary basis); and
- **Mandatory notifications under NIS Regulations** (which are only required when the level of disruption caused by an incident meets a specified threshold).

This distinction has been made by the UK Government so that OES do not wait until an incident reaches the 'significant impact' threshold that the NIS Regulations require before seeking support in containing and mitigating incidents that risk affecting essential services.

The purpose of notifications under the NIS Regulations is to enable Competent Authorities, including Welsh Government, to take any necessary regulatory follow-up actions and to meet other national obligations in the Directive, such as cross-border coordination.

Operators of Essential Services (OES)

Mandatory notifications under NIS Regulations

The NIS Regulations require OES to notify the Competent Authority of incidents without undue delay and **no later than 72 hours after the OES is aware that a notifiable incident has occurred**, and in line with the **National Cyber Security Centre’s Incident Management Guidance**.

Operators of Essential Services in the health sector in Wales are required to report incidents which meet the threshold of a NIS reportable incident to the NHS Wales Cyber Resilience Unit and Welsh Ministers.

The report should include:

- the operator’s name and the essential services it provides;
- the time the NIS incident occurred;
- the duration of the NIS incident;
- information concerning the nature and impact of the NIS incident;
- information concerning any, or any likely, cross-border impact of the NIS incident; and
- any other information that may be helpful to the competent authority;

Should a NIS incident occur that affects multiple OES, all impacted OES are required separately to notify the incident to the relevant Competent Authority. If an OES is in any doubt over whether it needs to notify the NHS Wales Cyber Resilience Unit of an incident, the OES is encouraged just to do so.

Voluntary reporting of incidents below the NIS threshold

Welsh Ministers expects all organisations, including OES, to voluntarily report any significant cyber incidents to the NCSC and the NHS Wales Cyber Resilience Unit so they can get support and assistance on managing the incident, and so that Welsh Ministers can also respond effectively when required.

Notifying the NHS Wales Cyber Resilience Unit, and through them Welsh Ministers, as soon as possible is strongly encouraged. Where an incident has not yet met the threshold but it is likely or expected that it might meet the threshold at a future point, it should be reported as soon as possible.

Recording of Incidents

Every reported incident (i.e. a voluntarily reported incident which is below the

NIS incident threshold and those incidents that meet the NIS reporting threshold) will be logged by the NHS Wales Cyber Resilience Unit. The Unit will also be responsible for analysing the data to identify if there are trends, similarities or differences between the reported incidents. This intelligence will assist the NHS Wales Cyber Resilience Unit and Welsh Ministers to identify as early as possible any potential harmful activity on the Health networks and critical systems.

Other incidents which are out of scope of the definition of NIS Incident, whether they be of an ICT nature or otherwise should be managed by the relevant incident management protocol in place, in accordance with the organisation's own procedures.

Digital Service Providers (RDSPs)

If a Digital Service Provider determines that the NIS incident relates to, or may result in a data breach then the incident must also be reported to the **Information Commissioner's Office (ICO)** as the Competent Authority for RDSPs, whilst also informing the NS Wales Cyber Resilience Unit.

Incident Reporting guidance for RDSPs can be found on the **ICO website**.

Investigating Incidents

All OES must notify Welsh Ministers and the NHS Wales Cyber Resilience Unit of incidents that meet the thresholds set out in this guidance. Following the notification, and allowing for a period of resolution and recovery, Welsh Ministers will decide whether or not the incident requires further follow-up investigation.

There is no requirement under the NIS Regulations for Welsh Ministers to investigate *every* reported incident. The decision to investigate will be made jointly between the NHS Wales Cyber Resilience Unit and Welsh Government.

The NHS Wales Cyber Resilience Unit will establish a triage system of determining the severity and impact of the reported incident, which will assist in the categorisation of the incident. This may include requesting further details of the incident. The NHS Wales Cyber Resilience Unit will support Welsh Ministers in this process. The purpose of these assessments could be to:

- establish the cause of the incident and assess whether the incident was a breach of the NIS regulations
- assess whether effective and reasonable risk management was in place
- assess whether the operator had appropriate security measures in place
- assess how the OES responded to and managed the incident.

It is expected that the OES will also conduct their own investigations and this will form the basis for the conversation between Welsh Government, the NHS Wales Cyber Resilience Unit and the OES.

Once the assessment has concluded, Welsh Ministers, supported by the NHS Wales Cyber Resilience Unit, will determine the next course of action. This could be:

- advice/guidance to the OES
- enforcement action
- penalties
- no action required

The OES will be notified by Welsh Ministers of the outcome of this investigation in writing. The NHS Wales Cyber Resilience Unit and Welsh Ministers will maintain a confidential register of reported incidents which will include whether or not an investigation took place, and the outcome of any investigation.

It is important to note that simply having an incident is not in itself an infringement of the NIS Regulations and therefore does not automatically mean enforcement action will be taken. The key factor for determining whether enforcement action should be taken when there has been an incident, is whether or not appropriate and proportionate security measures and procedures were in place and being followed. Not having notified Welsh Ministers and / or the NHS Wales Cyber Resilience Unit of an incident that meets the incident notification thresholds would be an infringement of the NIS Regulations.

Cyber Security Oversight

Monitoring

Competent Authorities are required to monitor the application of the NIS Regulations with operators of essential services, which includes monitoring whether OES are meeting their security duties. This will be done through assessing the level of compliance of OES against the security requirements set out in this document.

This role must be fulfilled through a proactive approach which specifically includes direct engagement with OES, publishing guidance (such as this document) and implementing an assessment framework to check compliance with the security requirements which includes an audit regime. The overarching principle of this process is one of collaboration between Welsh Ministers and OESs.

OES are advised to nominate a point of contact within the organisation with whom Welsh Ministers and the NHS Wales Cyber Resilience Unit can communicate information concerning the NIS Regulations.

Inspections

Under the NIS Regulations, Welsh Ministers have the power to inspect operators of essential services. However, Welsh Ministers intend to rely on information collected by the NHS Wales Cyber Resilience Unit to monitor compliance with the NIS Regulations, including information collected through reporting and assessments.

Therefore, it is Welsh Ministers policy to only use their power to inspect where the NHS Wales Cyber Resilience Unit is unable to obtain sufficient information from an operator of essential services, or in response to a specific concern.

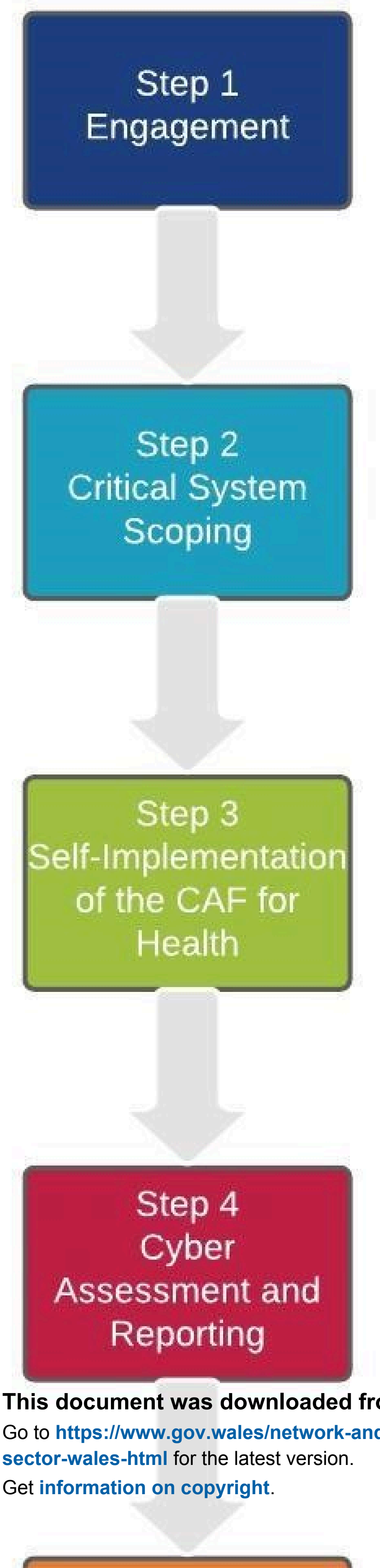
Cyber Assessment Framework (CAF) for Health in Wales

Competent Authorities are required to assess the compliance of OES with the requirements of the NIS Regulations. Compliance should be assessed against the fourteen NIS security principles at **Annex 1**.

To ensure an appropriate and proportionate approach each health organisation will be assessed independently against the **Cyber Assessment Framework (CAF) for Health in Wales** (link at **Annex 2).**

The applicability of each step will be discussed and agreed with a health organisation during the initial engagement step and determined based on several factors including the assessment of cyber security risk, health organisation complexity, and regulatory requirements.

The CAF for Health in Wales adheres to the principles of the **National Cyber Security Centre's Cyber Assessment Framework (CAF)** and consists of the following steps:



Step 1
Engagement

Step 2
Critical System Scoping

Step 3
Self-Implementation of the CAF for Health

Step 4
Cyber Assessment and Reporting

Step 1 – Engagement

Engagement will commence when Welsh Ministers notify the health organisation’s Accountable Manager that under applicable regulatory obligations their organisation is now deemed an OES under the NIS Regulations.

Step 2 – Critical System Scoping

Using the provided Critical System Scoping template and Guidance, each OES must determine and document all critical systems in scope of the relevant safety, security, or resilience regulation(s) for the health sector. This may include systems and services operated on behalf of the OES by third party suppliers.

Step 3 – Self Implementation of the Cyber Assessment Framework (CAF) for Health in Wales

Each OES must identify and determine any gaps that exist between their current Cyber security controls and the CAF for Health in Wales.

Step 4 – Cyber Assessment and Reporting

The NHS Wales Cyber Resilience Unit, and designated third parties, will conduct a Cyber assessment of all OES.

Step 5 – Remedial Action Implementation

Upon completion of the CAF for Health in Wales, each OES must complete the Improvement Action Plan section of the CAF for Health in Wales and begin to address any gaps.

Step 6 – Continual Improvement

Welsh Ministers and the Cyber Resilience Unit understand that this regulatory landscape is an emerging and fast-moving area, and recognise the challenging constraints that health organisations currently operate within. As such, a decision has been taken to operate a tiered approach to compliance that ensures fairness and promotes continual improvement towards conformance with the CAF for Health in Wales.

Assessment Process

All OES are expected to complete self-assessments using the CAF for Health in Wales. OES are expected to engage directly with the NHS Wales Cyber Resilience Unit during this process and to raise any queries they have on how to apply the assessment.

Assessments are to be carried out on an annual basis, although in the event of deficiencies more frequent assessments may be undertaken. The CAF for Health in Wales will also be reviewed on an annual basis, or in the event of a significant incident, by the NHS Wales Cyber Resilience Unit.

Upon completion of the self-assessment, the results will be discussed with the NHS Wales Cyber Resilience Unit and Welsh Ministers, who will work with OES to establish if and when improvements should be made. OES will need to propose measures they consider appropriate, and it will be for the NHS Wales Cyber Resilience Unit and Welsh Ministers to determine whether they are sufficient.

Beyond the first year, the NHS Wales Cyber Resilience Unit and Welsh Ministers will use the results of the self-assessment, along with threat and vulnerability information, to establish a risk-based programme of ongoing activity (including audits as described above) to monitor compliance.

Activity will be focussed on organisations where the most serious concerns have been identified and/or where potential incidents could have the greatest impacts on the sector. The exact nature of this activity may differ between OES, and timescales will be agreed with each OES individually.

Alongside this focussed activity all OES should strive to improve the security of their network and information systems, following the NIS Regulations, NCSC's NIS principles (Annex 1) and the Cyber Assessment Framework for Health in Wales.

Enforcement

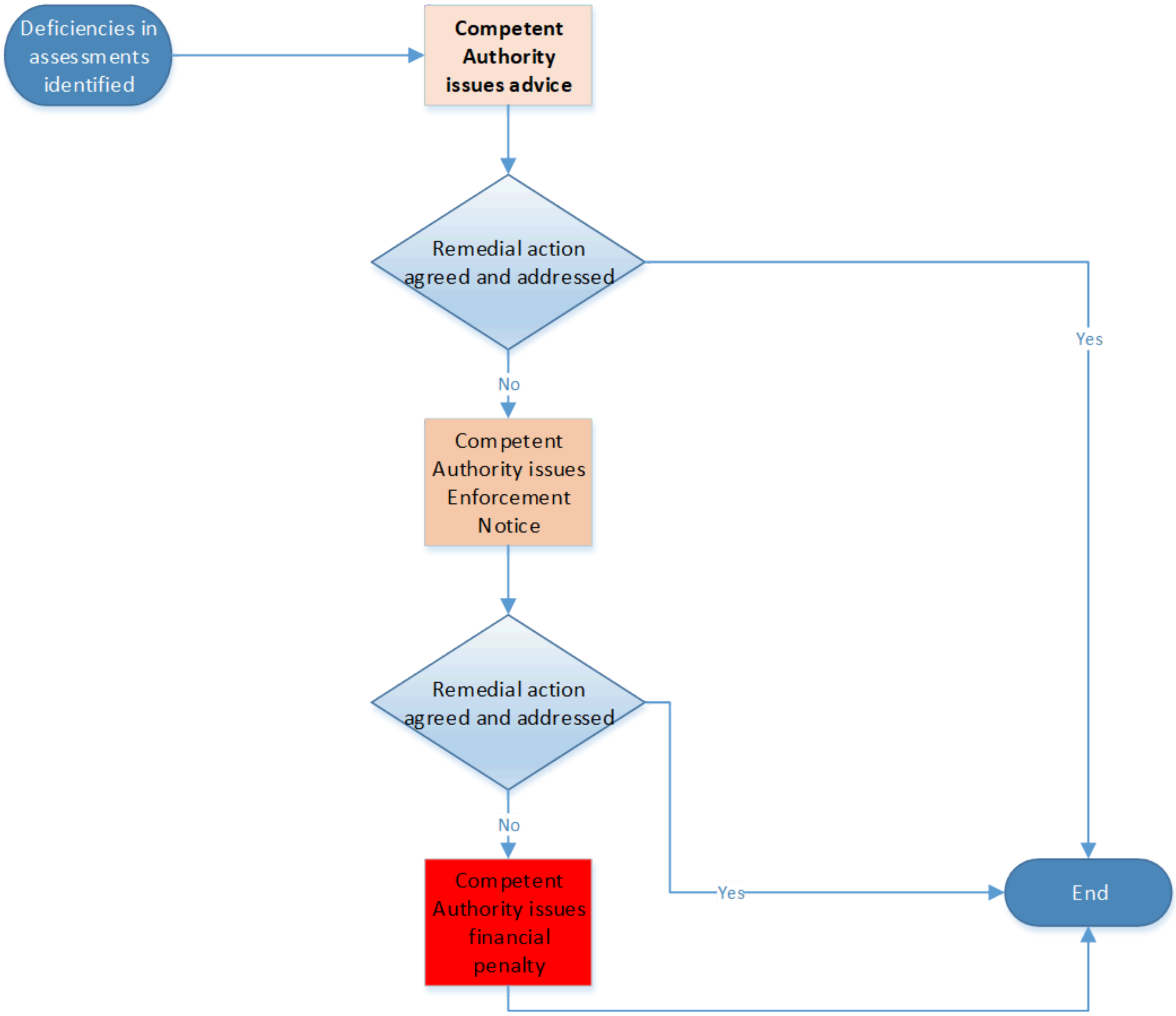
So that OESs and RDSPs are clear as to the approach being taken, Competent Authorities should implement a stepped process of enforcement in which OES and RDSPs are given advice and / or guidance, enforcement action, penalties or no action is taken.

Simply having a cybersecurity incident is not by itself an infringement of the NIS Regulations; the key factor for determining enforcement action is whether or not appropriate and proportionate security measures and procedures were in place and being followed. Steps organisations have taken to improve their cyber resilience will be a significant factor in determining the level of enforcement issued.

Welsh Ministers will use a stepped approach to enforcement when an OES is found to be failing to meet requirements. This relies heavily on a collaborative approach between Welsh Ministers, supported by the NHS Wales Cyber Resilience Unit, and OES. Any enforcement, particularly the issuing of penalties, will be a last resort and in all cases will be proportionate to the failing identified.

If an OES is not compliant with the NIS Regulations, Welsh Ministers as Competent Authority can take a number of actions to inform and enforce their decisions, through the use of Information Notices and Enforcement Notices.

The stepped approach that Welsh Ministers will take in the Health Sector in Wales is summarised below:


Deficiencies in assessments identified
Competent Authority issues advice
Remedial action agreed and addressed
Yes
No
Competent Authority issues Enforcement Notice
Remedial action agreed and addressed
No
Yes
Competent Authority issues financial penalty
End

Step 1: Advise

- Where deficiencies are identified in assessments, the initial approach taken will be to engage and discuss with the OES. This will include discussing what the failing or deficiency is and how and when it can be addressed.
- Welsh Ministers and the NHS Wales Cyber Resilience Unit will agree the remedial actions proposed by the OES and when these actions should be completed. This may then be followed up by further assessments or audits to ensure that these actions have been taken and any failings have been addressed appropriately and proportionately.
- A stronger line may be taken if these actions fail to be addressed in the agreed timeframe although this can still stop short of any formal enforcement action.
- Welsh Ministers may issue information notices requiring the OES to provide specified information to support compliance assessment.

Step 2: Enforcement Notice

- Where the initial collaborative approach has not worked, and it is clear that failings are not being addressed, a formal enforcement notice will be issued.
- This will set out the failings identified, the steps to be taken and the time period in which they need to be completed.

Step 3: Penalty Notice

- Where the OES has failed to take adequate steps to rectify a failure identified in an enforcement notice, a monetary penalty may be issued.
- Such a step is likely to be taken where the initial actions taken by the Welsh Government and the NHS Wales Cyber Resilience Unit have not been successful at instigating action by the OES.

Financial penalties which can be applied are:

- Up to £1 million for any contravention which the enforcement authority determines could not cause a NIS incident;
- Up to £8.5 million for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in a disruption of service provision by the OES for a significant period of time; and
- Up to £17 million for a material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy.

Whilst any enforcement action will be proportionate, Welsh Ministers will use their full range of enforcement powers where sufficient action is not being taken by operators.

NIS Enforcement and other Legislation

It is not possible to rule out the possibility that enforcement action could be taken under both the UK General Data Protection Regulation (GDPR) and NIS Regulations because these are separate legislative regimes with differing legal requirements. This will apply not just to GDPR but other sectoral and general legislation.

However, the NIS Regulations make provision for Competent Authorities to consider whether enforcement action is reasonable and proportionate on the facts and circumstances of the case, including consideration of whether a contravention is also liable to enforcement under another enactment.

Appeal to the First-Tier Tribunal

Operators of Essential Services have the right to appeal to a First-Tier Tribunal against one or more of the following decisions of Welsh Ministers:

- A decision to designate them as an operator
- A decision to revoke them as an operator
- A decision to serve a Penalty Notice or Enforcement Notice on them

The grounds of the appeal are:

- that the decision was based on a material error as to the facts
- that any of the legislative procedures 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 another material irrationality including unreasonableness or lack of proportionality which substantially prejudiced the interests of the OES

The first-tier tribunal must determine the appeal after considering its grounds and by applying the same principles as would be applied by a court on an application for judicial review.

Contacts

> **The contact email address for the Competent Authority in relation to cyber security incidents is**
>
> **Email: HSS.CyberReporting@gov.wales**
>
> Rydym yn croesawu gohebiaeth yn Gymraeg / We welcome correspondence in Welsh.

Annex 1: National Cyber Security Centre (NCSC) NIS Security Principles

The implementation of Article 14 of the NIS Directive is described via 4 top-level objectives. The objectives will be realised through implementation of 14 sector-agnostic security principles devised by the National Cyber Security Centre (NCSC). Each principle describes mandatory security outcomes to be achieved.

The full guidance collection on the NCSC's website (see **Annex 2**) goes into further detail on each principle with references to a range of existing guidance and standards.

Objective A: Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

A1. Governance

Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.

A2. Risk management

Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.

A3. Asset management

Determining and understanding all systems and/or services required to maintain or support essential services.

A4. Supply chain

Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect essential services and systems from cyber attack.

B1. Service protection policies and processes

Defining and communicating appropriate organisational policies and processes to secure systems and data that support the delivery of essential services.

B2. Identity and access control

Understanding, documenting and controlling access to essential services systems and functions.

B3. Data security

Protecting stored or electronically transmitted data from actions that may cause disruption to essential services.

B4. System security

Protecting critical network and information systems and technology from cyber attack.

B5. Resilient networks and systems

Building resilience against cyber attack.

B6. Staff awareness and training

Appropriately supporting staff to ensure they can support essential services' network and information system security.

Objective C: Detecting cyber security events

Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

C1. Security monitoring

Monitoring to detect potential security problems and track the effectiveness of existing security measures. C2. Proactive security event discovery

Detecting anomalous events in relevant network and information systems.

Objective D: Minimising the impact of cyber security incidents

Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

D1. Response and recovery planning

Putting suitable incident management and mitigation processes in place.

D2. Lessons learned

Learning from incidents and implementing these lessons to make a more resilient service.

Annex 2: Links to Further Guidance and Information

EU Directive 2016/1148 on the security of network and information systems (NIS Directive)

Full text of the NIS Directive (in PDF format)

Network and Information Systems Regulations 2018 with **further amendments to the legalisation**.

Consultation on the Security of Network and Information Systems Directive

Details of the public consultation run by DCMS and the UK Government response that determined how the UK would implement the Directive.

NCSC's NIS Guidance Collection

This is the central page linking to all of the NCSC's guidance on the NIS Directive

NCSC’s Incident Management Guidance

This is the **specific guidance from the NCSC** relating to how to develop and carry out an incident response plan.

Top-level NIS objectives and NCSC guidance

This page lists the four top-level security objectives that the UK is using to implement article 14 of the NIS Directive, linking through to the principles and guidance for each area.

CPNI website

A useful resource for all organisations is the CPNI website which contains advice and guidance on many aspects of physical and personnel security.

Technical guidelines for the implementation of minimum security measures for Digital Service Providers

This document was produced by the European Union Agency for Network and Information Security (ENISA) to define the common baseline security objectives for RDSPs under the NIS Directive. It describes different levels of sophistication in implementing those objectives and maps the objectives against other well-known industry standards, guidance and frameworks. Whilst this has been developed for RDSPs there are sections that are also relevant to OES.

ISO27001

This standard specifies the requirements for establishing, implementing and maintaining an information security management system.

NIST cyber security framework

This framework was developed by the US Government in collaboration with the private sector and contains a set of industry standards and best practice to support organisation in managing cyber risks. The Framework Core is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors.