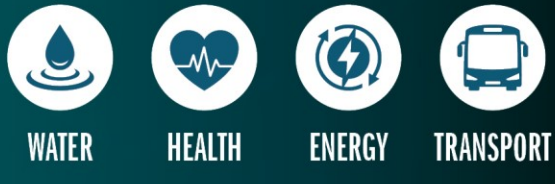
NIS | Competent Authority

Department of Finance | An Roinn Airgeadais

www.finance-ni.gov.uk

NIS Incident Reporting Guidance



NIS Competent Authority

WATER HEALTH ENERGY TRANSPORT

Contents

1. Introduction 3

1.1 Definition of an Incident 3

2. Incident Reporting 4

1.2 Mandatory Reporting 4

1.3 Voluntary Reporting 5

1.4 Specific reporting of Ransomware 6

1.5 Reporting of RDSP Incidents 5

2 Incident Reporting Process 6

2.1 The Initial Report 6

2.2 Interim reporting 8

2.3 Final reporting 9

3 Post Incident Review 10

4 Information Sharing 10

5 Incident Review 11

6 NIS Competent Authority Feedback and closure 12

Annex A – Incident Thresholds for Northern Ireland Sectors 13

Annex B – Flow chart for NIS incident reporting 15

1. Introduction

This document is only intended for organisations that meet the thresholds to be deemed an OES and for which the DoF is the designated competent authority. Under the NIS Regulations 2018 this includes Energy (Electricity, Gas & Oil), Health, Drinking Water supply and distribution, Transport for Rail and Road in Northern Ireland.

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 designated as an OES by the Competent Authority under regulation 8(3) and have a responsibility under regulation 11 to report all significant NIS incidents that affect the essential service for which they are responsible no later than 72 hours after they are aware that a NIS incident has occurred.

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]

Following a NIS incident notification, the NISCA C&E will monitor the incident and assess what further action, if any, is required in respect of that incident.

The NIS incident information will also be shared with National Cyber Security Centre (NCSC) as the Computer Security Incident Response Team (CSIRT), as soon as reasonably practicable.

1.1 Definition of an Incident

The definition of a NIS incident is:

> any incident which has a significant impact on the continuity of the essential service which that OES provides.

For clarity, a NIS incident can be a anything that has a negative impact on network and information systems including accidental or malicious events.

A significant NIS Incident is any event having an adverse effect to the continuity of the essential service for which that OES provides network and information systems. Guidance to assist an OES in determining a level of significance can be found in regulation 11(2) and Annex A.

While this guidance determines a framework to establish a level of significance it remains the responsibility of the OES to determine when an incident is significant and there may be circumstances where an incident could be deemed significant outside of the threshold definitions in Annex A but having an adverse effect on the provision of the essential service.

Under the NIS Regulations, network and information systems are defined as including:

- an electronic communications network as defined in the Communications Act 2003[2];
- any device or group of interconnected or related devices which perform automatic processing of digital data; or
- digital data stored processed, retrieved, or transmitted by an electronic network or device.

[1] The Network and Information Systems Regulations 2018 (legislation.gov.uk)
[2] https://www.legislation.gov.uk/ukpga/2003/21/section/32

The system of devices can be sometimes referred to as Operational Technology (OT) systems, Engineering Technology (ET), Information Technology (IT) systems and Internet of Things (IoT).

2. Incident Reporting

The NISCA C&E is not responsible for incident response or management and an OES should have their own incident response plans and support identified and in place.

When an incident affects the essential service, the OES may have various responsibilities to report this to regulatory, statutory, and voluntary authorities. It is essential that the OES understands their responsibilities in this regard as reporting to the NISCA C&E will not fulfil other regulatory, statutory, or voluntary duties.

An OES needs to ensure that any proportionate and appropriate measures necessary for incident mitigation to the supply of essential services are understood as part of their security duties under regulation 10(2). The OES is strongly encouraged to report any NIS incidents in writing as soon as they are aware and is encouraged to report material incidents even where an incident has not yet met the thresholds for mandatory reporting under NIS.

When an OES has an incident affecting the essential service it provides and this is a result of a network and information systems failure or degradation that has resulted from an accidental, malicious, or other cause then an OES is encouraged to report this to the Competent Authority.

NIS Incidents should be reported via email to: nis.incident@finance-ni.gov.uk

As part of the incident report an OES should provide a summary of the incident including;

- Incident type;
- How the incident was discovered;
- Time of discovery and current duration;
- Location of the incident(s);
- Services/systems affected;
- Impact on those services/systems;
- Impact on safety to staff or public;
- Whether there is any known or likely cross-border impact; and
- Any other relevant information.

It is important that NISCA C&E are kept informed of the incident as it progresses from initial report through to closure.

1.2 Mandatory Reporting

All incidents that affect the provision of an OES essential service resulting from a network and information systems failure or degradation and are determined to be significant by the OES with consideration given to regulation 11(2) or the guidance thresholds set out in Annex A is considered a reportable incident under Regulation 11 and must be reported.

There is a regulatory duty on an OES to notify the NISCA C&E of all NIS reportable incidents without undue delay **in writing[3] no later than 72 hours** after they are aware that a notifiable incident has occurred.

An OES should have their own incident management processes in place as part of their security obligations under regulation 10(2). Additional guidance on this can be found at the National Cyber Security Centre's (NCSC) Incident Management Guidance.

1.3 Reporting of RDSP Incidents

a "relevant digital service provider" ("RDSP") is a reference to a person who provides a digital service in the United Kingdom and satisfies the following conditions :-

(i) the head office for that provider is in the United Kingdom or that provider has nominated a representative who is established in the United Kingdom;

(ii) the provider is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC

and where a "digital service" means a service within the meaning of point (b) of Article 1(1) of Directive 2015/1535 which is of any the following :-

(a) online marketplace;

(b) online search engine;

(c) cloud computing service;

and where a "cloud computing service" means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

An OES may have a reliance on a RDSP to provide its essential service. Where and RDSP has an incident that causes a significant impact to the essential service the OES provides, the operator must notify NIS Competent Authority, in relation to it, about any significant impact on the continuity of the service it provides caused by an incident affecting the RDSP within 72 hours after they are aware that the incident has occured.

NIS Competent Authority strongly recommends that any incidents in relation to RDSP incidents that an OES is aware of that could be "likely to be significant" or "a near miss", or had an impact that has affected their essential service, but fell below the thresholds should still submit a voluntary report as outlined in section 1.4.

1.4 Voluntary Reporting

Where an incident affects the provision of an OES essential service resulting from a failure or degradation of network and information systems and in the OES consideration of regualtion11(2) and **does not** meet the guidance thresholds for significance set out in Annex A but is, or has a possibility to be, significant, this can be reported to the NISCA C&E.

While there is no legal requirement to report these "likely to be significant" or "near miss" incidents the competent authority would encourage an OES to report these in the same manner as a mandatory report.

[3] Email is an accepted and preferred form of written communication.

1.5 Specific reporting of Ransomware

Ransomware is the most significant national security cyber threat currently facing UK organisations. As ransomware attacks continue to become more sophisticated and damaging, we are taking steps to improve information gathering on related incidents.

Where an incident affecting Network and information systems has taken place whether the impact is significant i.e. must be reported, or not OESs are encouraged to report all ransomware related incidents, and the incident type on the form indicated as "Malicious".

3. INCIDENT INFORMATION:			
Incident Title			
Date/Time Incident Reported:		**Date/Time Incident Reported:**	
Internal Incident ID:		**Type of Incident:**	**Malicious** ☒ **Non- Cyber** ☐
Incident status	**Suspected** ☐ **Verified** ☐ **Closed** ☐	**Incident Stage:**	**Ongoing** ☐ **Closed but managed** ☐ **Closed** ☐

Additional details to be included in the body of the form would include the information above under section 2 and the following details:

- Notification that a ransomware incident has taken place;
- The category/categories of information and the systems that were, or are suspected to have been, subject to unauthorised access;
- Notification of whether a payment has been made and the amount paid;
- Contact information for the victim or an authorised representative responsible for technical management of the incident.

Organisations are encouraged to inform Action Fraud separately of the incident. Reporting the incident separately to Action Fraud will allow the incident to be reported as a crime and allow law enforcement or the NCSC to seek additional information about the incident. This will include information that is not relevant to a competent authority but is useful to law enforcement authorities, such as the nature of the ransomware demand, the amount, who it was paid to and how.

2 Incident Reporting Process

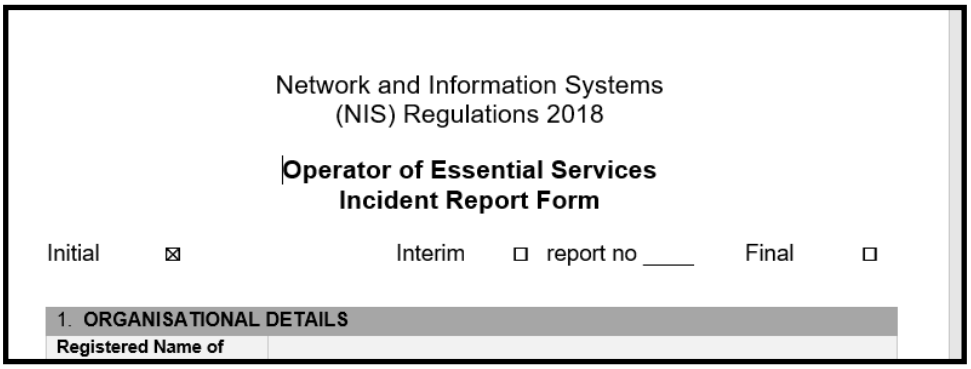
2.1 The Initial Report

Once a NIS Incident is discovered the following NIS Incident reporting form should be used by the OES to inform NISCA C&E.

This form has been developed to ensure that information detailed in the NIS regulations 11(3)(a) for reporting incidents is included in any submission.

Type of Report

On the first report of an incident the OES should ensure to tick the "Initial check box" to indicate this is an initial report.



Network and Information Systems
(NIS) Regulations 2018

Operator of Essential Services
Incident Report Form

Initial ☒ Interim ☐ report no ____ Final ☐

1. ORGANISATIONAL DETAILS	
Registered Name of	

In the early stages of an incident full details about the incident may not yet be known. An OES **should not wait** until all details are known before reporting but complete the initial incident report with as much detail as possible and available at the time. Follow up interim reports can be submitted as more information about the incident becomes available.

Organisational and reporting person details.

These areas are self-explanatory. Good practice would be to download the NIS incident report and have these fields pre-populated and included as part of your organisation's incident response plan.

Incident Information

This section of the report should include general details of the incident. An incident title and the operational ID reference used by your organisation to identify this incident. This is essential for ongoing correspondence and communication purposes as there may be occasions where more than one incident is ongoing at a time.

Type of incident

The report should indicate if the incident is malicious in nature e.g., from cyber bad actor or insider threat with motivation to destroy or disrupt the organisation's ability to deliver its normal operations. If the incident is not known then leave both boxes blank and update to either "Malicious" or "Non-Cyber" in subsequent reports when this then becomes apparent.

Incident Status

Incident status can be used to determine the nature of an incident.

Suspected: If an OES is still at an investigative stage or if an OES is not sure if the incident is a NIS type incident an OES may wish to report to the NISCA C&E for consideration then the "suspected" box should be ticked.

Verified: Use once an incident is known to be a NIS type incident. The incident will remain verified until the incident is closed.

Incident Stage

The incident stage allows NISCA C&E to understand how the incident is progressing.

Ongoing: An incident is ongoing from initial report until closure whether suspected or verified.

Closed but managed: An incident can be closed with NIS but still ongoing within the organisation, being managed below NIS thresholds and no perceived risk of escalation above NIS thresholds in the future. At this point the final report check box should be checked.

Closed: This would correspond to when the incident is closed within the OES. At this point the final report check box should be checked.

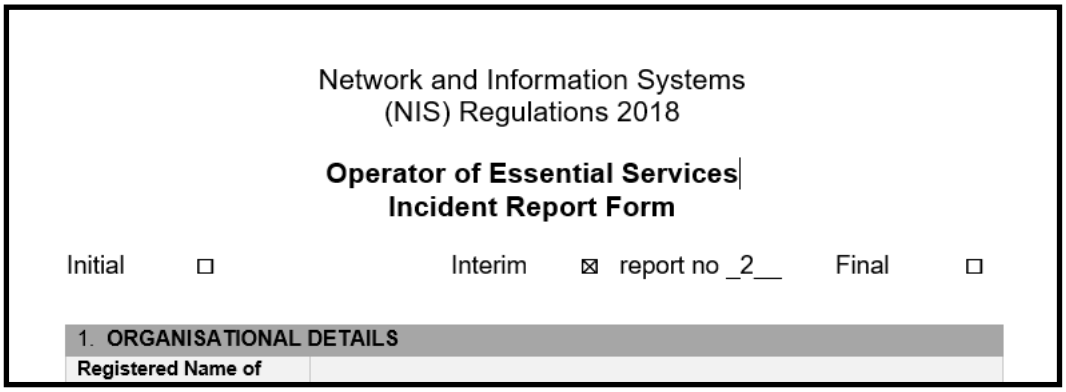
2.2 Interim reporting

Interim reports are required to update the NISCA C&E on progress of the incident.

The frequency of an interim report is:

- every calendar month[4] from the date of the last report until the incident is closed, or;
- where more information becomes available on the nature of the incident if within the calendar month, or;
- as soon as there is any significant escalation or de-escalation in the risk or impact of the incident; or
- as advised by the competent authority.

The interim report checkbox should be ticked, and the relevant interim report number inserted.



Network and Information Systems
(NIS) Regulations 2018

Operator of Essential Services
Incident Report Form

Initial ☐ Interim ☒ report no _2__ Final ☐

1. ORGANISATIONAL DETAILS	
Registered Name of	

For clarity the numbering of interim report should start at 1 and should not include the initial report in the sequence.

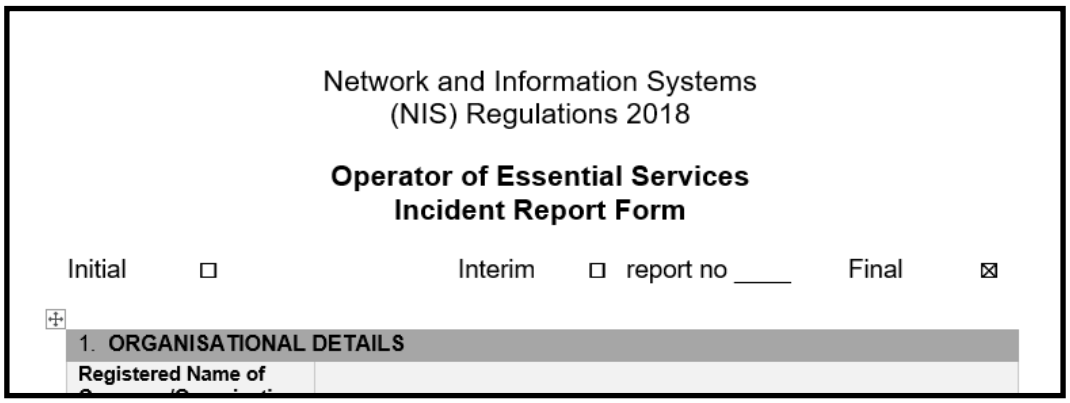
The interim report update should be added to the initial report and subsequent updates dated and added chronologically. This allows for the history of the incident progress to be retained in one place for future reference.

[4] A calendar month would be on the anniversary day of the initial report e.g., if reported on the 30th Jan the each 30th day or the closest date to that within the month e.g. 28th Feb.

4. INCIDENT Report:	
Please provide a summary of the incident, including any impact to services and/or users: Add interim updates as incident progresses.	
01/01/2023	Initial incident summary report
15/01/2023	First interim report, number 1, updating on any new information.
15/02/2023	Next interim report, number 2, one month later from last report
20/02/2023	Next interim report, number 3, due to escalation of incident.
20/03/2023	Next interim report, number 4, one month later from last report
30/04/2023	Next interim report, number 5, due to de-escalation of incident.
30/05/2023	Next interim report, number 6, one month later from last report
15/06/2023	Final report on closure of incident (this can be closed but managed or closed)

2.3 Final reporting

A final incident report should be submitted by the OES when the incident has been successful closed by the OES or is deemed closed but managed, i.e., the incident remains open within the OES but can be closed from a NIS incident perspective as it is very unlikely to escalate to a significant level and service levels have returned to pre-incident levels. A final report should be made within one month of the OES decision to close being made.



Network and Information Systems
(NIS) Regulations 2018

Operator of Essential Services
Incident Report Form

Initial ☐ Interim ☐ report no ____ Final ☒

1. ORGANISATIONAL DETAILS	
Registered Name of	

The final box should be ticked to indicate that no further reports are to be tendered.

Should this incident escalate beyond manageable levels then the incident should be re-opened, and the user submit the next Interim Incident Report number until conclusion, including final reporting.

3 Post Incident Review

The Initial and subsequent incident notifications are designed to ensure the OES meets the requirements under regulation 11(3b) however DoF has duties under regulation 11(5) to assess what further action, if any, is required regarding the incident.

Once a final report is submitted by the OES and the incident closed a post incident review report is required by NISCA C&E, no later than **one month after the final report date** or as agreed with NISCA C&E.

Where a final report determines the incident "closed but managed" the NISCA C&E will require the OES to provide:-

- an **Interim Post Incident Review Report** no later than **one month of the final report date** or as agreed with NISCA C&E; and/or
- a **Final Post Incident Review Report** no later than **one month of the incident being closed within the OES** or as agreed with NISCA C&E**.**

The purpose of the Post Incident Review is to:

- establish the cause of the incident and whether the incident was preventable;
- assess whether effective and reasonable risk management was in place;
- to determine whether the OES had in place appropriate and proportionate security measures; and
- assess how the company responded to and managed the incident to mitigate impact.

The Post Incident Review from the OES should build on the information submitted in the Initial incident report, as well as any interim reports, and include as a minimum:

- A complete overview of the incident including any additional company investigations into the root cause analysis, impact, and nature of the incident;
- Details of any lessons learned from the event, including actions taken or being taken to prevent a recurrence of the event or to update response plans;
- Estimated timescales of the implementation of any lessons learned and completion of any mitigating actions in order of prioritisation;
- Confirmation the incident and lessons learnt has been discussed at OES corporate board level and any new risks have been incorporated into the company's risk management plan; and
- Any further relevant information that the company feel would aid the assessment of the incident by the competent authority.

4 Information Sharing

Information sharing is permitted under regulation 6(1) where NIS CA C&E is a NIS enforcement authority and may share information with other Northern Ireland Departments, NIS enforcement authorities, relevant law-enforcement authorities, the CSIRT, and public authorities in the EU if that information sharing is:

(a) necessary for:
  (i) the purposes of these Regulations or of facilitating the performance of any functions of a NIS enforcement authority under or by virtue of these Regulations or any other enactment;

(ii) national security purposes; or
(iii) purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution;

(b) limited to information which is relevant and proportionate to the purpose of the information sharing.

Information shared under regulation 6(1) may not be further shared by the person with whom it is shared for any purpose other than a purpose mentioned above unless otherwise agreed by the NIS Competent Authority.

When sharing information with a public authority in the EU as stated above, the NIS CA C&E will not share confidential information, or information which may prejudice the security or commercial interests of operators of essential services or digital service providers.

The NISCA C&E will maintain a record of all NIS incident reports submitted to them and an annual report identifying the number and nature of NIS incidents notifications received. The annual report will be shared with NCSC as the Single Point of Contact (SPoC) for the UK under the NIS Regulations, under regulation 11(9).

In addition to notifying the NCSC in their role as CSIRT and SPoC, NISCA C&E has obligations under the NIS Regulations to share information on any incidents reported as meeting the NIS Incident thresholds within each sector.

Where an incident has the potential to impact the continuity of an essential service within another part of the UK, NISCA C&E will notify the relevant UK competent authority responsible for the sector.

If, after notification to the CSIRT, the incident has the potential to significantly impact on the continuity of the essential service of other EU Member States then the CSIRT will inform the relevant authorities in that EU Member State. However, the CSIRT is not required to inform other Member States in this way if the information submitted is deemed confidential and/or prejudice the security or commercial interests of the company.

Where it is deemed that it is necessary to inform the public of a NIS incident, this will be done in consultation with the OES and the CSIRT and will only be done if it is the view that public knowledge will aid in handling the incident or preventing a future incident occurring.

The NISCA C&E branch will consider their obligations in sharing information with other stakeholders, including potential criminal investigation and other legal obligations, e.g., PSNI, ICO, other regulators, other NICS departments.

5 Incident Review

The NISCA C&E reserves the right to review and probe further into a NIS incident for the purpose of verifying OES compliance with the requirements which would include assessing or gathering evidence of potential or alleged failures to comply with the requirements of these Regulations. The Head of the NISCA C&E branch will decide on any appropriate next steps, be it no action, advice, or formal enforcement action. Any decision on enforcement or further action will be taken forward in consultation with the NIS Compliance and Enforcement Panel in DoF.

It should be noted 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. Key factors for determining whether enforcement action should be taken following an incident, whether

appropriate and proportionate security measures and procedures were in place and being followed, and whether proportionate and appropriate mitigation measures were in place to limit the likelihood or impact of the incident. Upon an initial assessment of the information received via incident reports and post incident reviews or at any time during the incident the NISCA C&E may decide to conduct an independent incident review, the purpose of which is to assess compliance with the NIS Regulations in relation to:

- Appropriate and proportionate technical and organisational measures to manage risks;
- Appropriate and proportionate measures to prevent and minimise the impact of incidents;
- Appropriate and proportionate technical and organisational measures having regard to the state of the art, to ensure a level of security of network and information systems appropriate to the risk posed; and
- Application of any relevant guidance issued by the competent authority.

Failure to report an incident that meets the NIS incident notification requirements would however be an infringement of the NIS Regulations and may result in enforcement action.

The NISCA C&E may share the results of an incident review with the OES concerned if appropriate. For example, where an OES may find this information useful to improve the resilience of their systems.

6 NIS Competent Authority Feedback and closure

The NIS Competent Authority will formally acknowledge closure of incidents and will detail if there is no further action, or any follow up action that is to be taken by the OES or NIS Competent Authority.

Annex A – Incident Thresholds for Northern Ireland Sectors

Electricity Generation	*Unauthorised access to a control system or the loss of (or potential loss of) more than 350MW.*

Electricity Transmission	*Loss of control leading to, or likely to lead to, loss of bulk supply point.*

Electricity Distribution	*Loss of control or unplanned single incident loss of supply to 8,000 customers for more than 3 minutes.*

Electricity Interconnect	*Loss of control or unauthorised or unplanned loss of capacity greater than 350MW / 51% (whichever happens first).*

Electricity Supply	*Any unplanned shut off or single incident loss of supply, for a period greater than 24 hours, affecting either:* *a. 10% or more of the customer base; or* *b. 2,000 customers or more.*

Oil storage	*When at least 25% of throughput capacity is lost for at least 24hrs.*

Gas Conveyancing	*Any incident that has, or is likely to have, a loss or degradation to the conveyancing of gas that impacts end user demand.*

Gas Distribution	*Any incident that has an impact to the essential service that: -* • *Has any interruption of gas supply to at least one priority customer; or* • *Has an interruption of gas supply to 2,000 or more customers for at least 24 hours.*

Rail Transport	*A single incident which results in 30% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations.*

	A single incident which results in more than 20,000 delay minutes over a period of one week or in an amended timetable being run that is equivalent to that number of delay minutes.

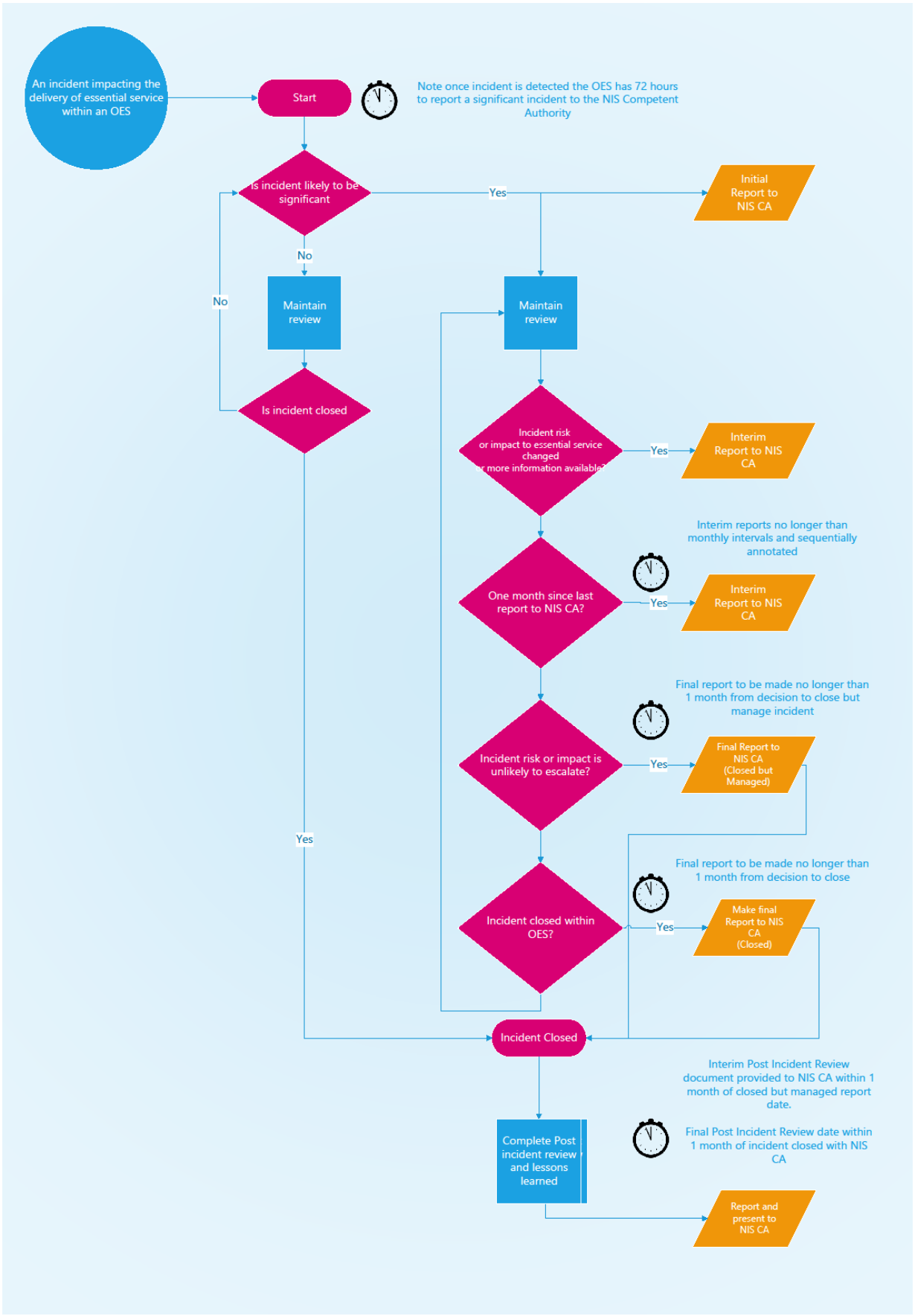
Health	*Any unauthorised, malicious, suspicious or accidental action that impacts Network & Information Systems of essential services that results in an immediate or imminent** • *Loss, interruption, or impact to systems or services of more than 1 day that impacts the delivery of public health and social care; or* • *Loss, interruption or impact to systems or services that impact the health, safety or welfare of patients/clients, resulting in moderate or greater increase in treatment/care provision, semi-permanent or greater harm/disability, or immediate or imminent risk to life.* **Imminent within 1 day.*

Drinking Water	*Any unauthorised, malicious, suspicious, or accidental action that impacts network and information systems that results in an immediate or imminent* impact to;* • *The loss of supply to more than 4,000 properties for more than 6 hours; or* • *Impact to water quality resulting in Do Not Drink advice to more than 500 properties: or* • *Impact to water quality resulting in Boil advice to more than 10,000 properties.* **Imminent within 1 day.*

NIS Competent Authority

WATER HEALTH ENERGY TRANSPORT

Annex B – Flow chart for NIS incident reporting



NIS Competent Authority

WATER HEALTH ENERGY TRANSPORT

Version 1.2/2024