Cetome
Securing a Better Future

White Paper

# SCOPING THE NIS DIRECTIVE

April 2019

Author: Dr. Cédric LEVY-BENCHETON, CEO

# Table of Content

# INTRODUCTION

In a first article, we introduced the NIS Directive, one major cyber security regulation in these recent years.

In this article, we discuss on the applicability of the NIS Directive. We will see that the NIS Directive is all about securing the delivery of a service. Yet, its application could become tedious as most network and information systems work interdependently. For that purpose, we will explain how to refine the scope of the NIS Directive and present two methodologies to identify the critical assets in scope.

This article is part of a series that aims to better apprehend this directive.

## SECURING THE CONTINUITY OF ESSENTIAL SERVICES

The NIS Directive requires Operators of Essential Services (OESs) and Digital Service Providers (DSPs) to implement "appropriate and proportionate organisational and technical security measures to posed to the security of network and information systems which they use to operate their service."

Moreover, OESs and DSPs must take "appropriate measures to affecting the security of the network and information systems used for the provision of their service, with a view to ensuring the continuity of those services."

These two regulatory requirements emphasize the importance of protecting the service from cyber security risks. It demands a proactive approach to identify the scope, *i.e.* the assets that are essential to the service. It also reinforces the importance of resilience and incident handling in order to limit the potential impact on a service should a security incident occurs.

Hence, the intent of the NIS Directive is really about protecting the society from major disruptions due to a cyber incident. For that purpose, OESs and DSPs must identify their critical network and information systems, the security risks they face, and protect them with appropriate and proportionate security measures. In the spirit of the NIS Directive, these security measures will depend on business objectives.

## THRESHOLDS FOR INCIDENT NOTIFICATION

The NIS Directive requires OESs and DSPs to notify their competent authority or CSIRT of incidents having "significant impact on the continuity of their service, without undue delay." We call these incidents " ".

The is defined by competent authorities for the OESs and DSPs in their sector. In order to do so, competent authorities can establish thresholds using various parameters:

- the number of users affected by the disruption of the essential service;
- the duration of the incident;
- the geographical spread with regard to the area affected by the incident;
- [for DSPs only] the extent of the disruption of the functioning of the service;
- [for DSPs only] the extent of the impact on economic and societal activities.

By combining these parameters, it is possible to refine thresholds for various scenarios (local or national operator, short or long disruption, etc.).

In reality, most competent authorities will define NIS incident thresholds using one or two parameters. This keeps these thresholds measurable and gives OESs and DSPs the ability to react before an incident can cause a significant impact on their service.

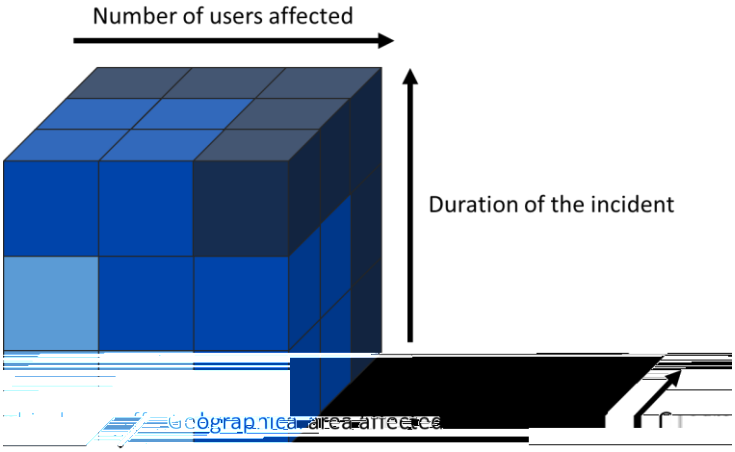



*Figure 1. Possible Combination of Incident Thresholds*

Nevertheless, incidents can evolve through time, and some minor incidents can rapidly escalate into a NIS incident. To limit this risk, OESs and DSPs should consider business continuity and resilience requirements in order to minimise the impact of a security event as soon as possible. We will explore this topic in a future article.

# REFINING THE SCOPE

## ASSETS IN SCOPE

The scope of the NIS Directive focuses on network and information systems that are used to provide a service. This means any network, hardware, software that are essential to deliver a service (*i.e.* which failure would affect the level of service). We will refer to them as " " in the rest of this article.

The NIS Directive defines these network and information systems as:

(a) *An electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;*
(b) *any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or*
(c) *digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;*

In summary, the scope of the NIS Directive applies beyond data. It considers physical devices, their dependencies and the systems in charge of their security. As such, the NIS Directive requires following a system-of-systems approach.

Note that the dependencies of critical assets must also be considered. These dependencies can be "cyber" or "non-cyber" such as power supply, air conditioning, etc.

### Incidents in Scope

A NIS Incident is an incident that has a significant impact on the continuous delivery of a service. In case of such incident, OESs and DSPs must notify their Competent Authority or CSIRT using a reporting template, without undue delay.

This means that the type of NIS Incident does not matter: any incident that causes a disruption must be notified. This makes sense, as it can be very difficult to analyse the root causes of an incident in the short timeframe allocated for notification.

For that purpose, OESs and DSPs must notify:

- Cyber attacks and voluntary incidents (e.g. ransomware, DDoS);
- Accidental incidents (e.g. configuration error, human error);
- Incidents with "non-cyber" root causes (e.g. interruption of power supply, natural disasters).

Note that a NIS Incident can be the result of one or several issues. The intention of the mandatory notification is to serve a purpose for lessons-learned and continuous improvement.

### What is Out of Scope?

The NIS Directive only considers network and information systems that are essential to provide a service. This means that non-essential assets fall out of scope. For example, an email server that does not directly contribute to the service would be out of scope.

Similarly, manual processes would fall out of scope. Manual processes are quite common in sectors where safety is involved.

In some Member States, some legacy assets can be left out of scope if there is a plan to replace them to reduce the risks they may introduce. Yet, this decommission must happen in a near future. For instance, planning the replacement of a legacy critical asset with known vulnerabilities in the next five years goes against the spirit of the NIS Directive.

However, it is important to consider a holistic approach during scoping. Some systems might present a risk even though they are out of scope. For example, an IoT CCTV system might not be essential to the service. Yet, it may contain vulnerabilities that can give an entry-point to an attacker to escalate an attack on critical assets. Hence, OESs and DSPs must assess these risks during their NIS Directive assessment.

## IDENTIFICATION OF CRITICAL ASSETS

The NIS Directive requires OESs and DSPs to secure their critical assets in order to minimise the risks that a security incident affects the delivery of their service. In theory, every organisation knows what is important to deliver its service (and run the business). In practice, it is not always easy to maintain an up-to-date asset inventory (if it exists), list all critical assets, their dependencies, and the necessary information to secure them.

Most of the Member States leave the identification of critical assets to operators, as they know better than anyone else what assets are important to them. However, in some Member States, competent authorities can establish a list of critical assets to secure at minimum in their sector.

For that purpose, several methodologies can help identify and categorise assets. These methodologies demand a certain degree of cooperation between different parts of the business. They contain implicit

requirements for people, process and techniques that would help comply with the NIS Directive: asset management, risk management, governance, resilience, etc.

Note that the NIS Directive applies to critical assets owned by the operator, even when managed by a third-party.

### Asset-based Methodology

*Disclaimer: I worked on a similar methodology for the identification of Critical Information Infrastructure assets and services when I was at ENISA. More information: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis*

In this first methodology, we present a three-step approach to identify critical assets.

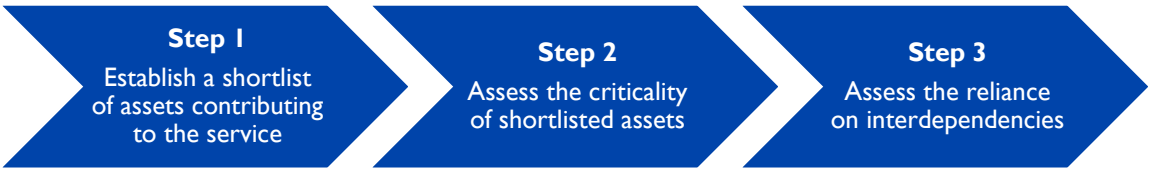



*Figure 2. Asset-based methodology*

In the first step, it is important to clearly identify the assets that contribute to the service. These assets can:

- Contribute to the operations (*e.g.* a SCADA system);
- Provide the assurance of service delivery (*e.g.* performance monitoring);
- Contribute to the security of these assets (*e.g.* firewall).

This first step should be straightforward for organisations with an up-to-date asset inventory. Others should take this opportunity to review their asset management.

In the second step, we perform a risk assessment to identify the criticality of shortlisted assets. The objective is to identify the assets that are essential to the service. For that purpose, the risk assessment must consider:

- The level of contribution to the service;
- The impact level to the service from the disruption of the asset.

Ideally, operators will rely on their existing risk models to assess the criticality of their assets.

In the third step, we go beyond the asset-based vision by integrating dependencies. These interdependencies comprise:

- Other Network and Information Systems (*e.g.* Cloud, ISP);
- Non-cyber systems (*e.g.* power supply, air conditioning).

This third step considers the wider environment in which critical assets operate. This includes the supply chain, the physical environment, etc.

This asset-based methodology is useful to identify the scope in a well-known environment as it reuses existing mechanisms (asset management, risk assessment, supply chain).

One shortcoming is that this methodology does not explicitly integrate the roles and responsibilities involved in the assessment process. Yet, it is important to involve the right stakeholders where and when needed.

### PROCESS-BASED METHODOLOGY

*Disclaimer: This methodology is suggested by the UK regulator "ofgem" in their guidance to OESs.*

The second methodology is a six-step approach that considers business objectives. By doing so, it is visible that cyber security aims to protect the business.

The first step requires the identification of business processes that are critical to the business, as well as their dependencies that have a high impact on its delivery.

To facilitate this step, it is possible to reemploy an existing business risk assessment.

The second step looks at the group of assets and geographical sites that are critical to service delivery. It should be done by evaluating the overall contribution to the service by a group of assets or sites: the highest their contribution is, the highest their criticality would be.

As in the first methodology, this step will be easier when relying on an existing asset inventory.

The third step maps the results of step 1 with the results of step 2. Hence, it highlights the contribution of each group of assets and geographical sites to the critical business processes.

This step implies the collaboration between stakeholders from different parts of the business.

In the fourth step, the owners of critical assets are identified. Operators must focus on roles and responsibilities for the assets or a geographical site, in particular for shared responsibilities (for example: who is responsible for the installation, the operation, the maintenance).

In this fourth step, the focus is on understanding the existing roles and responsibilities around these assets and sites to better apprehend the risks.

The fifth step demands to perform an impact-assessment on the service, the business and the NIS Directive requirements. This assessment shall consider how the disruption of a group of assets or a site could escalate into a higher risk to the organisation or even to the country.

For that purpose, it can be beneficial to evaluate the impact of specific scenarios. Ideally, every part of the organisation is involved in this fifth step, including executive management.

This sixth and last step integrates dependencies that support groups of assets and business functions. It demands to identify the dependencies that make operations successful.

As in the asset-based methodology, this step considers the wider environment in which these assets operates.

This process-based methodology is a high-level methodology that focuses on business requirements. As such, it can simplify the identification of critical assets. Moreover, some steps directly map to steps from the asset-based methodology.

This methodology still has shortcomings: it requires to perform a business risk assessment *a priori*; and having an up-to-date asset inventory would be key to successfully perform some steps.

# COMPLETENESS OF THE SCOPE

The scoping of the NIS Directive is an important step on the road to compliance. Hence, it is important to ensure the completeness of the scope: *i.e.* all assets that could cause a risk to the service are in scope.

For that purpose, we presented two methodologies that support the identification of critical assets, how they operate and their dependencies. The NIS Directive considers both “cyber” and “non-cyber” dependencies: Cloud services, power supply, air conditioning, staff, contractors, etc. These dependencies must be in scope when their disruption can affect service delivery.

A successful scoping will involve different stakeholders across the business. It will also go beyond the assets (in isolation or as a group of assets) and integrate how these assets work together and how they contribute to the business to support service delivery.

To refine their scope and ensure its completeness, operators may exchange with their peers on methodologies, good practices and traps. In some cases, competent authorities can also play a role. For instance, they could provide an overview on main critical assets in a sector or establish a list of assets to secure *at minima*.

# CONCLUSIONS

The NIS Directive requires the identification of critical assets that contribute to service delivery. This is an important step that will lead to the implementation of appropriate and proportionate security measures to mitigate the risks faced by these critical assets.

We have presented two methodologies for scoping the NIS Directive. To be successful, this scoping must go beyond the identification of individual critical assets and integrate dependencies and business functions.

In the next article, we will discuss on the UK implementation of the NIS Directive, the "NIS Regulations".

## ABOUT CETOME

Dr. Cédric LÉVY-BENCHETON is the CEO and founder of Cetome. Cédric has expertise in critical infrastructure, in particular around strategic advisory and the NIS Directive. Cédric previously worked at ENISA, the European Union Cyber Security Agency. Before that, Cédric designed critical networks for public transports.

Cetome is an independent security consultancy. We work with operators of essential services, infrastructure owners and solution vendors to ensure they are ready for the NIS Directive.

We support your NIS Directive journey. We make sure that your activity is secure against cyber risks in compliance with the requirements of the NIS Directive.

Our experts have worked at ENISA, the EU Cyber Security agency, where they directly contributed to the NIS Directive and developed security measures for several sectors in scope.

We have developed our services to help implement appropriate and proportionate technical and organisational security measures as required by the NIS Directive. We follow a holistic approach that goes beyond technical and considers critical assets, third-party suppliers and the staff.

We also provide awareness and training adapted to Competent Authorities, Operators of Essential Services, Digital Service Providers and their suppliers.

Cetome
Securing a Better Future

# The NIS Directive – The GDPR of Critical Infrastructure

Several recent cyber attacks have disrupted critical national infrastructure with an impact on our economy and our safety. For this reason, the European Union and its Member States (including the UK) have voted the NIS Directive to better protect our society from cyber risks.

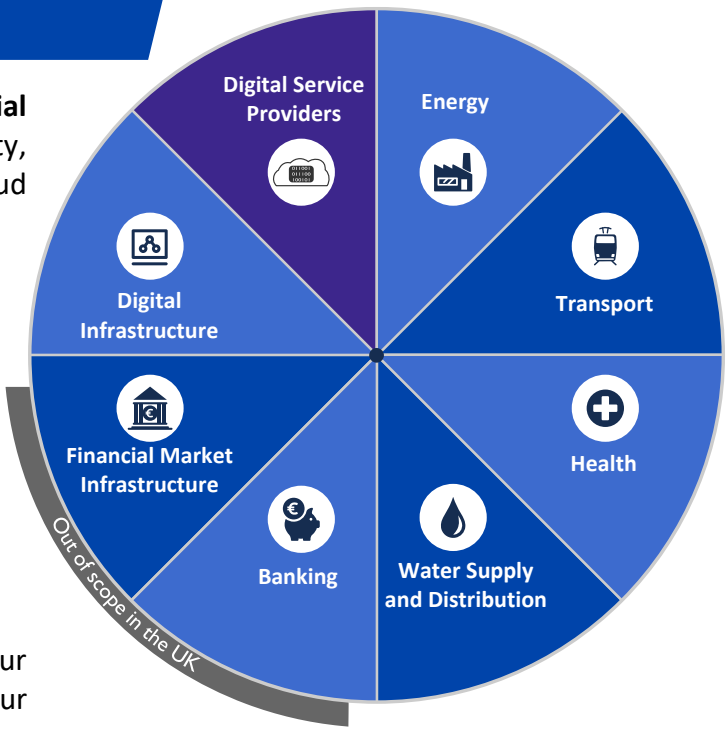
## Where does it apply?

The NIS Directive applies to **Operators of Essential Services** who provide a service vital to the society, and to **Digital Service Providers** who operate Cloud services, search engines or online marketplaces.

**The sectors in scope** must:

- Implement appropriate and proportionate organisational and technical security measures.
- Notify significant cyber incidents to their Competent Authority without delay.

or face an important penalty!




You must comply with the NIS Directive if your organisation meets the criteria established by your Competent Authority.

## Objectives of the Directive

- Understand and prevent **cyber risks** by securing network and information systems
- Augment the preparedness and **trust in critical infrastructure** across Europe and the UK
- Ensure the thorough implementation of **good security practices and cyber resilience**
- Handle incidents to **minimise impact on service** and develop lessons-learned

## Compliance Timeline

NIS Directive adopted by the European Parliament
**Summer 2016**

**May 2018**
Governments published their transposition into local regulation

Governments have identified Operators of Essential Service
**November 2018**

**Starting April 2019**
**Operators of Essential Services** must:

- Ensure they have a security governance
- Map their gaps and risks
- Identify appropriate and proportionate security measures
- Communicate an improvement roadmap to their regulator

**Operators of Essential Services** must:

- Complete the deployment of appropriate and proportionate security measures
- Measure their security performance
- Demonstrate improvements in compliance

**Before November 2020**

**Cetome** is an **independent security csD 1Sun** wcopec essdenial( )-[ssD Ser)-Vicest

ifrastrucsD Pu rraondsot vndors( Po esD Sure thme)