EUROPEAN
COMMISSION

Brussels, 28.10.2019
COM(2019) 546 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems

1. Introduction

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union[1] (NIS Directive) is the first internal market instrument aimed at improving the resilience of the EU against cyber-security risks. Based on Article 114 of the Treaty on the Functioning of the European Union, the Directive aims at ensuring the continuity of services allowing the Union's economy and society to function properly. In order to do so, the Directive introduces concrete measures building cyber-security capabilities across the EU and mitigating growing threats to network and information systems used to provide essential services in key sectors.

Following its entry into force in August 2016, Member States had until 9 May 2018[2] to adopt national measures necessary to comply with the provisions of the NIS Directive. The Directive promotes a risk management culture among companies or other entities providing essential services which are defined, pursuant to Article 5, as "operators of essential services" (OES). Operators which fall in the scope of the Directive are required to take appropriate and proportionate technical and organisational measures to manage the risks posed to their security of network and information systems and to notify serious incidents to competent authorities.

The co-legislators have delegated implementation of the NIS Directive to the Member States who are supposed to define essential services and identify operators of essential services in their territories. Hence Article 5(7) of the Directive requires Member States to report to the Commission on the results of this identification. In order to allow for a coordinated reporting, both the Commission[3] and the Cooperation Group established by the Directive[4] provided guidance to Member States concerning the identification process.

In accordance with Article 23(1), the present report assesses the consistency of the approaches taken by Member States in the identification of operators of essential services. As

[1] OJ L 194, 19.7.2016, p. 1.
[2] By September 2019, all 28 Member States have notified full transposition.
[3] *Communication from the Commission to the European Parliament and the Council: Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, COM(2017) 476.
[4] The NIS Cooperation Group, which is composed of Member States, the Commission and ENISA (the European Union Agency for Cybersecurity), has created a separate work stream with the aim of exchanging information and best practices on OES identification amongst Member States.

the consistency of OES identification and the risk of fragmentation in the internal market in this area are closely linked, this report will also feed into the wider assessment of the NIS Directive, as stipulated in Article 23(2), which provides for the Commission to periodically review the overall functioning of the Directive and to assess the list of sectors and sub-sectors subject to the identification of OES and the types of digital services covered by the Directive. The first such reports is to be submitted by 9 May 2021.

1.1 Purpose of the report

Due to their important role for the economy and society as a whole, operators of essential services must demonstrate a particularly high level of resilience against cyber-incidents. In this regard, a consistent approach in OES identification by Member States is important for several reasons:

1. **To reduce the risks related to cross-border dependencies:**

   A failure to consistently identify important operators providing services cross-border may result in an uneven level of cyber-resilience between different Member States, increasing the risk that a cross-border incident would damage critical infrastructures or cause the loss of the life of citizens.[5] For example, energy transmission operators or top-level domain registries, which are both part of the list of types of entities in Annex II, are entities which make the most of the internal market by providing cross-border services to consumers and businesses. A consistent identification of such providers across the Union could therefore help prevent cyber-threats from propagating throughout the internal market.[6]

2. **To guarantee a level playing field for operators in the internal market:**

   The NIS Directive requires Member States to establish security requirements and incident notification procedures for OES. As the Directive follows a minimum harmonisation approach with regard to OES, Member States are free to impose

[5] For instance, it took WannaCry, a ransomware cryptoworm, in May 2017 only a single day to spread to over 150 countries and infect an estimated 200 000 computers.

[6] According to the NIS Cooperation Group, the openness of the internal market for services can lead to "cross-border risks and dependencies that fundamentally affect the availability, integrity and confidentiality of such services".

requirements on operators that are higher than those provided for in the Directive. While enhancing the resilience of Member States, such measures may generate additional regulatory costs for the concerned operators. It is therefore important that operators providing similar services of similar relevance are subject to similar regulatory treatment.

3. **To reduce the risk of divergent interpretations of the Directive:**

   The Directive has been designed in such a way as to give Member States room for manoeuvre in selecting the relevant entities to account for national specificities. At the same time, this approach increases the risk of divergent implementation of the provisions of the Directive and can potentially lead to inconsistencies in the measures adopted by Member States. This is especially important for companies that are active in several countries and that therefore have to meet the regulatory requirements of more than just one Member State.

4. **To develop a comprehensive overview of the level of cyber-resilience across the EU:**

   OES are subject to supervisory activities aimed at verifying the effective implementation of security policies as well as the notification of significant incidents. Supervision favours the development of stronger public-private cooperation, leading to the development of a shared knowledge about cyber-security preparedness within a Member State. Thanks to the Cooperation Group, the sharing of national experience, including information about incidents notified[7], can be aggregated at EU level and contribute to a more accurate assessment of main threats and needs. However, in order to be effective, such information sharing exercise should be based on a common understanding on which entities should be identified as OES.

1.2 Identification procedure under the NIS Directive

The NIS Directive provides in its Annex II a list of seven sectors and their respective sub-sectors and types of entities which are relevant for the identification process (Table 1).

[7] According to Article 10(3) of the NIS Directive, Member States shall submit every year to the Group a summary report of incident notifications received.

Article 5(3) requires Member States to establish a list of essential services based on these sectors, subsectors and types of entities. The minimum harmonisation approach of the Directive allows Member States to go beyond the scope of Annex II and carry out identification in additional sectors and subsectors.

Sector	Subsector
1. Energy	(a) Electricity
	(b) Oil
	(c) Gas
2. Transport	(a) Air transport
	(b) Rail transport
	(c) Water transport
	(d) Road transport
3. Banking	
4. Financial market infrastructures	
5. Health sector	
6. Drinking water supply and distribution	
7. Digital Infrastructures	

Table 1: Sectors and subsectors listed in Annex II of the NIS Directive

Article 5(2) lays down three **criteria** to be used by Member States for the identification of operators of essential services:

1. The entity in question needs to provide a **service that is essential** for the maintenance of critical societal and/or economic activities. To that end, national competent authorities have to consult their previously established lists of essential services.
2. The service provided has to **depend on network and information systems**.

3. An incident would need to have significant **disruptive effects** on the provision of the relevant service. Article 6 specifies that the significance of an incident shall be assessed using **cross-sectoral factors** and, where appropriate, **sector-specific factors**.[8]

Furthermore, Article 5(4) of the Directive requires Members States to engage in consultation with one another if they find that a potential OES is providing services in more than one Member State. This mandatory procedure is meant to help Member States assess the potential impact of a cyber-incident affecting entities operating across borders as well as acting as safeguard for the companies affected by the procedure in different Member States.

1.3 Methodology of the report

The results of the report are based on an assessment conducted between November 2018 and September 2019. Many Member States had not made the information required to draw up the present report available to the Commission on time. The adoption of the report therefore had to be postponed beyond 9 May 2019, the adoption date envisaged by Article 23(1) of the NIS Directive. The data were gathered through multiple channels: information submitted by Member States based on a standardised template prepared by ENISA, standardised interviews with selected national authorities, and Cooperation Group meetings, including a workshop dedicated to the subject held on 19 March 2019.

Based on the information gathered, the report evaluates how consistent the identification approaches of Member States are with one another by

1. comparing the different identification methodologies chosen by national authorities,
2. examining the lists of essential services and thresholds chosen by Member States,
3. analysing the numbers of OES in each Member State.

The report also evaluates how the provisions of the Directive regarding the cross-border consultation procedure (Article 5(4)) and the *lex specialis* principle (Article 1(7)) have been implemented. The report provides a factual analysis of the process of identification carried

[8] Examples of cross-sectoral factors are the number of users relying on a service or an entity's market share. Examples of sector-specific factors are the number of autonomous systems connected to an Internet Exchange Point (IXP) or a financial institution's number of transactions per year.

out by the Member States accompanied by preliminary conclusions and open questions for further reflection.

1.4 Data availability

The provisions of the NIS Directive require Member States to provide only a limited set of data to the Commission. For instance, national authorities are not required to submit the names of the identified operators, which makes it difficult for the Commission services to compare the results of the identification process in terms of the completeness of the list and the impact on companies of the same size and belonging to the same sector.

Under the terms of Article 5(7) all Member States should have provided the input necessary for this report no later than 9 November 2018. However, only 15 countries had submitted substantial data by that date (see annexed table in section 4.1). Following repeated reminders by the Commission, the gaps in the data remained significant. The Commission has therefore sent letters of formal notice to 6 Member States[9] on 26 July 2019, inviting them to submit the missing data within two months' time.

At the date of publication of this report 23 Member States had submitted all the data required under Article 5(7): Bulgaria, Croatia, Cyprus, the Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, France, Ireland, Italy, Lithuania, Luxembourg, Latvia, Malta, the Netherlands, Poland, Portugal, Sweden, Slovakia and the United Kingdom. The other 5 Member States (Austria, Belgium, Hungary, Romania and Slovenia) have only partially provided data on national OES identification, as they have not been able to complete their identification process in time for the publication of this report.

[9] Austria, Belgium, Greece, Hungary, Romania and Slovenia.

2. OES identification in the Member States

The NIS Directive lays down a framework for the identification of operators of essential services that provides Member States with discretion to take into account national specificities. As a result, Member States have developed a wide variety of identification practices.

2.1 Methodologies used by Member States

Member States have devised different methodologies to identify operators, making full use of the flexibility provided by the NIS Directive. One of the elements influencing national methodologies was the pre-existence of a framework, such the Council Directive 2008/114/EC on critical infrastructures[10] or other national provisions on "vital operators". In such cases, Member States used their prior experience as a point of reference and incorporated specificities related to the NIS Directive into existing methodologies.

Differences in national methodologies fall in the following main categories: essential services, use of thresholds, degree of centralisation, authorities in charge of identification and assessment of network and information systems dependence. Due to their importance for assessing OES identification consistency, separate sections have been dedicated to analysing essential services and thresholds. The other criteria are dealt with within this section.

Degree of centralisation

Most Member States have opted to delegate some of the decision making as regards various elements of the identification process to sectoral authorities (ministries, agencies etc.). The degree of decentralisation varies from case to case with most Member States nominating a single authority in charge of providing guidance to sectoral authorities and consolidating information. However, some countries have chosen to keep the identification process in the hands of a single authority. There are also cases with an extremely high degree of decentralisation where the sectoral authorities are responsible for developing their own methodologies.

[10] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The objective of the Directive is to strengthen the protection of critical infrastructures in the energy and transport sectors.

Many Member States have carefully weighed the different aspects of the institutional setup of OES identification. Conflict of interest avoidance has been cited by authorities as one of the merits of centralised identification: operators are apparently more reluctant to disclose relevant information to sectoral regulators as they fear that this information might also be used for other regulatory purposes.

Decentralised approaches on the other hand seem to foster dialogue amongst NIS competent authorities (both cyber-security and sectoral), helping them better identify the implications of cross-sectoral dependencies. Moreover, sectoral authorities have usually a deeper understanding of the sectors than the lead authorities.

Identification procedure (top-down vs. bottom-up)

Another important distinction can be drawn between Member States in which public authorities conduct the identification process (top-down identification) and Member States where market operators are called upon to verify by themselves whether they meet the requirements as operators of essential services (so-called bottom-up identification or self-identification). For the latter approach to work effectively, Member States should set fines that are high enough to dissuade operators from not coming forward, as provided for by Article 21 of the NIS Directive. In most cases the identification process is top-down. However, in practice authorities often partly rely on certain self-assessment elements, such as questionnaires to be filled out by potential OES.

If the rules and thresholds governing OES identification are explicit and transparent, both top-down identification and bottom-up identification should yield similar results. Choosing one approach over the other should therefore in principle not have any impact on consistency.

Assessment of network dependence

As explained in section 1.2, Article 5(2)(b) requires Member States to assess an operator's dependence on network and information systems as part of the OES identification procedure. Many Member States, when applying those criteria, consider dependence on network and information systems to be a given in today's digital economy. However, some authorities chose more elaborate practices, for example by conducting detailed assessments or by asking operators to self-evaluate the degree of their dependence.

2.2 Identification of services

Recital 23 of the NIS Directive explicitly mentions the lists of essential services as input to be used in the "assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency". As the lists of essential services drawn up by Member States serve as basis for the identification of operators, differences in the identified services could lead to an inconsistent identification of operators across Member States, especially if specific services provided in all countries are only identified by some Member States.

The numbers of services identified by Member States as covered by Annex II of the NIS Directive that have been reported to the Commission vary greatly between Member States (numbers for all Member States can be found in the annex in section 4.2). With an average of 35 services per Member State, the number of identified services ranges from 12 to 87, as shown in Figure 1. While larger Member States do tend to identify slightly more services than smaller Member States, there does not seem to be a strong correlation between the size of a Member States and the number of services identified. This is to be expected, as in practice consumers and companies usually have access to the same types of services in all Member States, irrespective of a country's size.

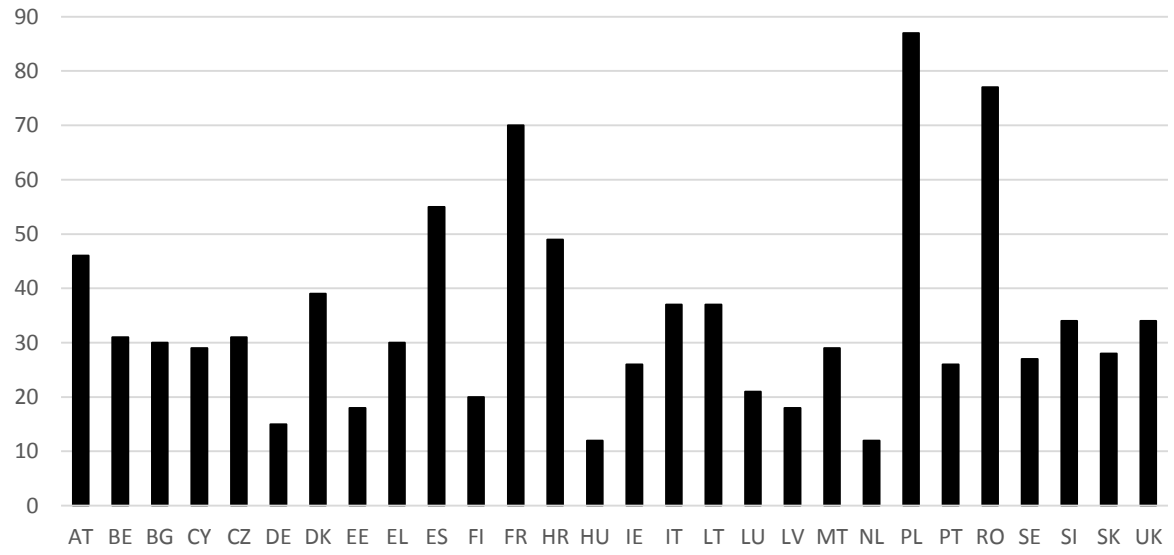

Figure 1: Overall number of essential services identified by Member States

The number of identified services not only varies when looking at Member States as a whole but also when taking a closer look at sectors and subsectors. For example, in the banking

sector, the number of identified services ranges from 1 to 21. As depicted in Figure 2, the range of identified services differs significantly between countries within most sectors and subsectors.

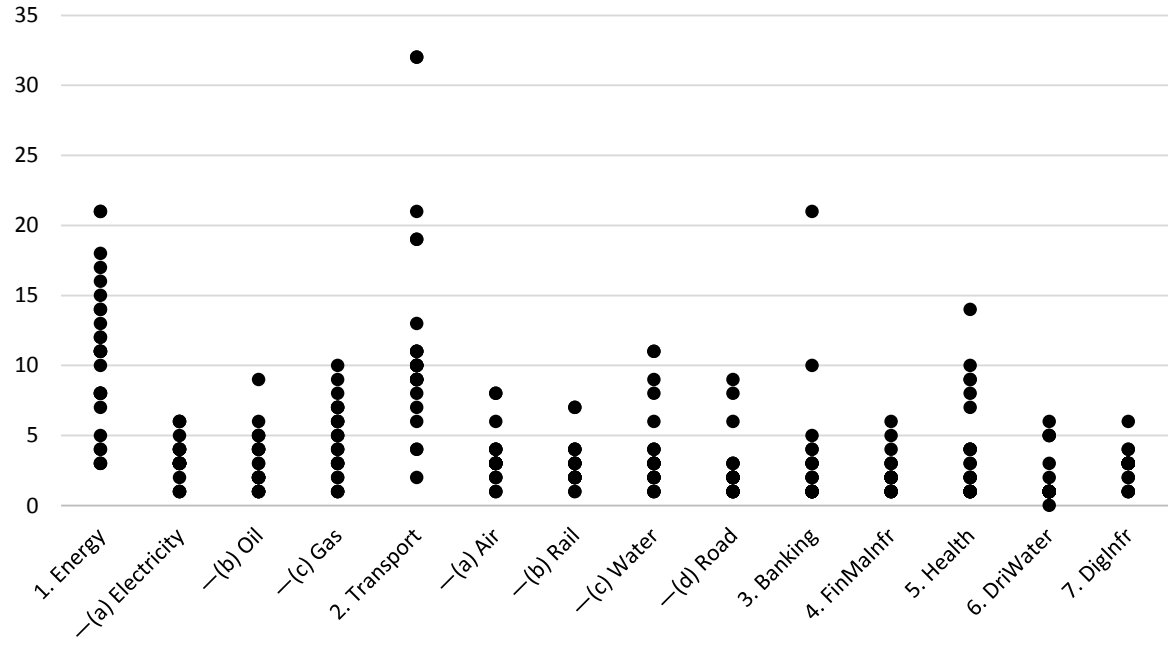

Figure 2: Number of services identified by Member States in each sector and subsector. Each data point represents the number of identified services by a Member State in the respective (sub)sector.[11]

To some extent, the numbers displayed in Figure 2 reflect different methodological approaches between countries. For instance, some Member States have chosen a more granular approach in identifying services than other Member States, leading to higher numbers in such Member States. The data that the Commission has received from the Member States, however, shows clearly that the differences in the numbers are also a result of inconsistencies in the approaches chosen by Member States, as the examples of the electricity and the rail transport subsectors demonstrate:

[11] Identical data points are plotted on top of one another. That is why not all 28 data points are visible on the plots. For example, 17 Member States have identified exactly three essential services under Digital Infrastructures.

Estonia (least granular approach)	Portugal	Denmark	Bulgaria (most granular approach)
Electricity supply	Distribution system operators	Electricity Distribution	Distribution of electricity
			Ensuring the functioning and maintenance of a distribution system for electrical energy
	Transmission system operator	Electricity Transmission	Transmission of electricity
			Operation, maintenance and development of an electricity transmission system
	(consistency gap)	Electricity Production	Electricity production
	(consistency gap)	*(consistency gap)*	Electricity Market

Table 2: Illustrative examples of approaches chosen by Member States in the identification of essential services in the electricity subsector

Table 2 compares some of the ways in which Member States have identified essential services in the electricity subsector. Some countries (such as Estonia) have chosen a very general heading allowing for the identification of basically any operator they deem essential within the electricity subsector. Other countries (such as Portugal, Denmark and Bulgaria) have opted for a much more granular approach. For instance, Bulgaria has drawn up an extremely detailed list of services, which even includes a service not covered by Annex II (electricity markets). Portugal and Denmark, however, have followed a granular approach choosing not to include certain services that others have included. This could result in an uneven playing field between OES within the internal market.

Consistency gaps, such as the ones identified in Table 2, are the result of different national implementations of the NIS Directive and in the case of sectors not falling under Annex II (such as electricity markets) a consequence of its minimum harmonisation approach. Consistency gaps therefore do not imply that Member States who have not identified a certain service have necessarily failed to correctly apply the provisions of the Directive.

Table 3 presents the approaches chosen by four countries vis-à-vis the rail transport subsector. While France has drawn up a very detailed and comprehensive list of services

essential to the functioning of rail transport, the other three countries have only selected a small subset of these services. In the case of Poland, it is not entirely clear which services fall under the categories of "freight railway transport" and "passenger railway transport". Their designations are so general that they might just as well include some of the services identified by France, such as "control and management of rail traffic". It is worth pointing out that the Commission has no means at its disposal to explore further such cases: the NIS Directive does not require national authorities to disclose information that is more detailed.

Finland	France	Ireland	Poland
State infrastructure management	Infrastructure maintenance	Infrastructure managers	*(consistency gap)*
(consistency gap)	Rolling stock maintenance	*(consistency gap)*	*(consistency gap)*
Traffic management services	Control and management of rail traffic	*(consistency gap)*	Preparing train timetables
(consistency gap)	Freight and hazardous materials	Railway undertakings	Freight railway transport
(consistency gap)	Passenger transport		Passenger railway transport
(consistency gap)	Metros, tram and other light rail services (including underground services)		*(consistency gap)*
(consistency gap)	Rail services	*(consistency gap)*	*(consistency gap)*

Table 3: Illustrative examples of approaches chosen by Member States in the identification of essential services in the rail transport subsector

The Member States included in Table 2 and Table 3 were only chosen for illustrative purposes and because their methodological approaches make for easy comparison. Most other Member States have chosen similar services and therefore exhibit similar "consistency gaps". In fact, "consistency gaps" such as the ones in the electricity and rail transport subsectors exist across all Member States and sectors included in Annex II of the Directive. Most of this inconsistency stems from services only identified in some but not all the Member States. The full lists of services in the electricity and rail transport subsectors encompassing all Member States can be found in the annex of this report.

2.3 Thresholds

Even though most Member States do apply thresholds to identify OES, the role that such thresholds play varies from country to country. In regard to cross-sectoral thresholds, it is possible to define thresholds relying on

- a single quantitative factor (e.g. number of users relying on a service) to determine whether an entity is to be considered an OES within a certain service,
- a larger set of quantitative factors (e.g. number of users relying on a service plus market share),
- a combination of quantitative and qualitative factors.

Moreover, the Directive allows Member States to apply sector-specific thresholds in addition to cross-sectoral ones. This gives national authorities more freedom in the identification process in order to take account of national and sectoral specificities. At the same time, it gives rise to a very complex mix of thresholds, which can have negative impact on overall OES identification consistency.

An example of this diversity of approaches is provided in Table 4. It illustrates that the thresholds chosen by Member States in the Digital Infrastructure sector do not only vary quantitatively (for example, in Germany DNS providers are identified as OES if they manage at least 250 000 domains, while Poland has set a threshold of only 100 000 domains) but also qualitatively (for example "number of connected autonomous systems" vs. "market share").

Consistently chosen quantitative thresholds alone do not guarantee full consistency between national approaches. Given the fact that thresholds are in some Member States just one of the criteria used to identify OES, the outcomes of the identification process could still be very different, even in the presence of similar thresholds. For instance, some Member States use complex scoring systems with several factors feeding into a single formula.[12] Such factors might for example include an entity's dependence on network and information systems or some of the factors referred to in Article 6(1) of the NIS Directive. In addition, some Member States do not use thresholds at all or only use thresholds in the preliminary phase of the

[12] For example, one Member State has developed seven factors (four so-called "factors depending on the operator" and three "factors depending on the impact") which feed into a single formula. If the final value of the calculation surpasses a certain threshold, the operator in question is recognized as an OES.

assessment. These considerations are valid not only for the Digital Infrastructure sector but also across all sectors included in Annex II.

Setting the right threshold can be a challenge, especially when it comes to sectors that are characterised by the existence of many small operators. An example of such diversity are the many small-scale health care facilities (e.g. clinics or emergency medical services), which provide an essential service to a relatively low number of users but whose unavailability, caused by a cyber-security incident, could result in patients' loss of life. Another problem arises when the functioning of supply chains depends on services provided by operators that constitute small but nonetheless essential links in the chain (for example in sectors such logistics[13]). One Member State is exploring the use of criteria linked to the importance or criticality of the service provided as a potential solution to this problem.

[13] The logistics sector is not covered by Annex II of the NIS Directive.

Country	Internet Exchange Points (IXP)	DNS providers	Top-Level-Domain registries
Use of predominantly sector-specific thresholds			
AT	connected autonomous systems > 100	DNS resolvers: 88 000 users; Author. DNS: 50 000 domains	50 000 domains
DE	connected autonomous systems > 300	DNS resolvers: 100 000 users; Author. DNS: 250 000 domains	*(service not identified)*
DK	av. daily data volume > 200 gbit/s	DNS resolvers: 100 000 users; Author. DNS: 100 000 domains	500 000 domains
EE	*(service not identified)*	*(service not identified)*	Registry of the country's TLD
FI	*(service not identified)*	*(service not identified)*	Registries of the country's and a region's TLD
FR	*(no official threshold)*	*(no official threshold)*	*(no official threshold)*
HR	connected members > 15	DNS service for country TLD	Registry of the country's TLD
IE	*(threshold unknown)*	DNS resolvers: 100 m queries/24h; Author. DNS: 50 000 domains	Registry of the country's TLD
MT	25% of market share	DNS resolvers: 78 000 requests/day; Author. DNS: 7 800 domains	750 000 requests/day
PL	connected autonomous systems ≥ 100	Author. DNS: 100 000 domains	TLD registries for at least 100 000 subscribers
SE	*(service not identified)*	DNS resolvers: 100 000 users; Author. DNS: 25 000 domains	250 000 domains
SK	*Autonomous system (AS) connecting at least two other AS with 2 Gbps*	DNS resolvers: 3 m queries/24h; Author. DNS: > 1 000 domains	Registry of TLDs
UK	market share > 50%, or interconnectivity to global internet routes ≥ 50%	DNS resolvers: 2 000 000 clients/day; Author. DNS: 250 000 domains	TLD registries ≥ 2 billion queries/day
Use of cross-sectoral thresholds			
CY	50 000 users, or 5% of subscribers of the market	50 000 users, or 5% of subscribers of the market	50 000 users, or 5% of subscribers of the market
LT	inhabitants > 145 000	inhabitants > 145 000	inhabitants > 145 000
LU	100% market share	13 500 contracts	100% market share

Table 4: Thresholds chosen by 16 Member States in the Digital Infrastructure sector

2.4 Number of identified operators

The lists of essential services and the thresholds are the most important determinants for a consistent identification of OES. The previous sections have shown that in both cases Member States have applied the provisions of the NIS Directive in various ways, suggesting that this may result in a consistency problem when it comes to subsequently identify OES. This section will compare the numbers of identified operators in the Annex II sectors and subsectors in the Member States.

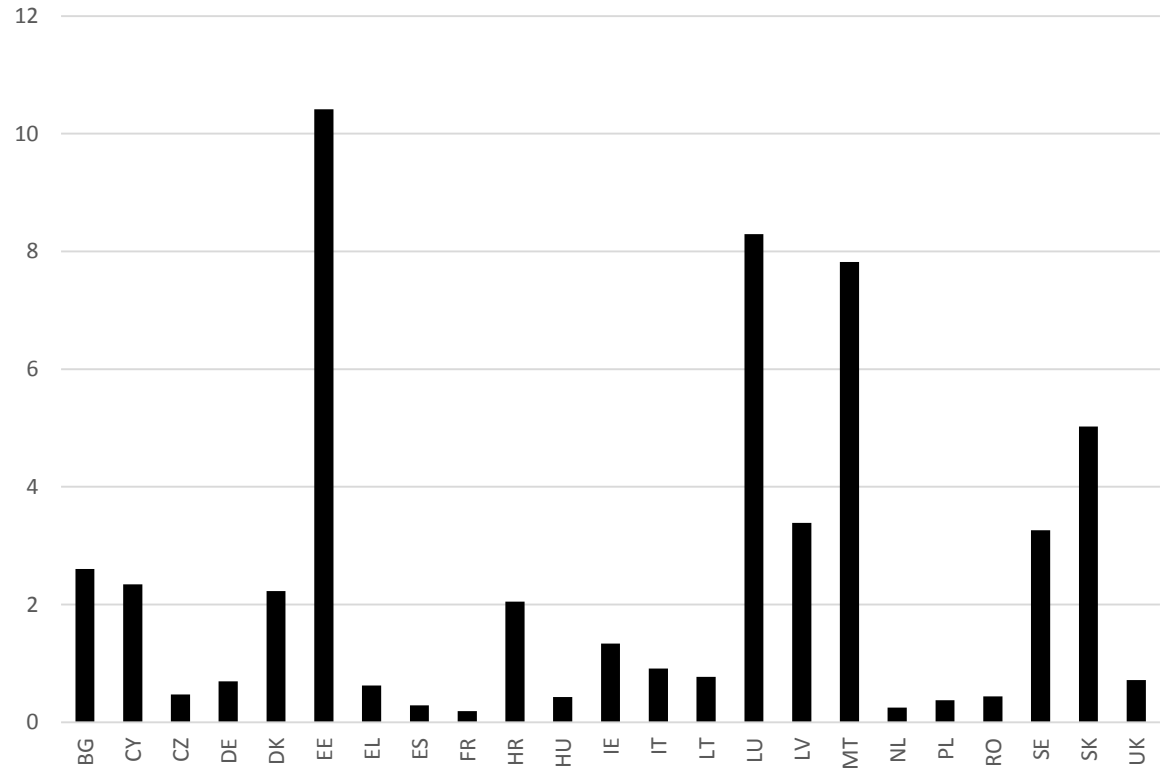

Figure 3: OES identified by Member States across all sectors in Annex II (per 100 000 inhabitants, outliers and missing data omitted for clarity)

The total numbers of OES reported to the Commission by Member States range from 20 to 10 897 with an average of 633 OES per Member State (numbers for all Member States can be found in section 4.2 of the annex of the present report). Overall, there is a clear positive relationship between the size of a country and the number of identified operators. However, this does not sufficiently explain the large differences in the numbers reported by Member States. In order to account for the relationship between size and population, Figure 3 compares the numbers of identified OES across Member States per 100 000 inhabitants. It

suggests that the approaches taken by Member States to identify operators have yielded very different results.

A more in-depth study of the sectors and subsectors reveals significant differences across Member States in the identified numbers across all the sectors covered by Annex II (Figure 4). For example, in the Energy sector, the number spans from 0.3 operators to 29 operators per 1 000 000 inhabitants. Numbers in the banking sector range from 0.07 operators to 51 operators per 1 000 000 inhabitants (not taking into account Member States that have not identified a single OES in that sector).

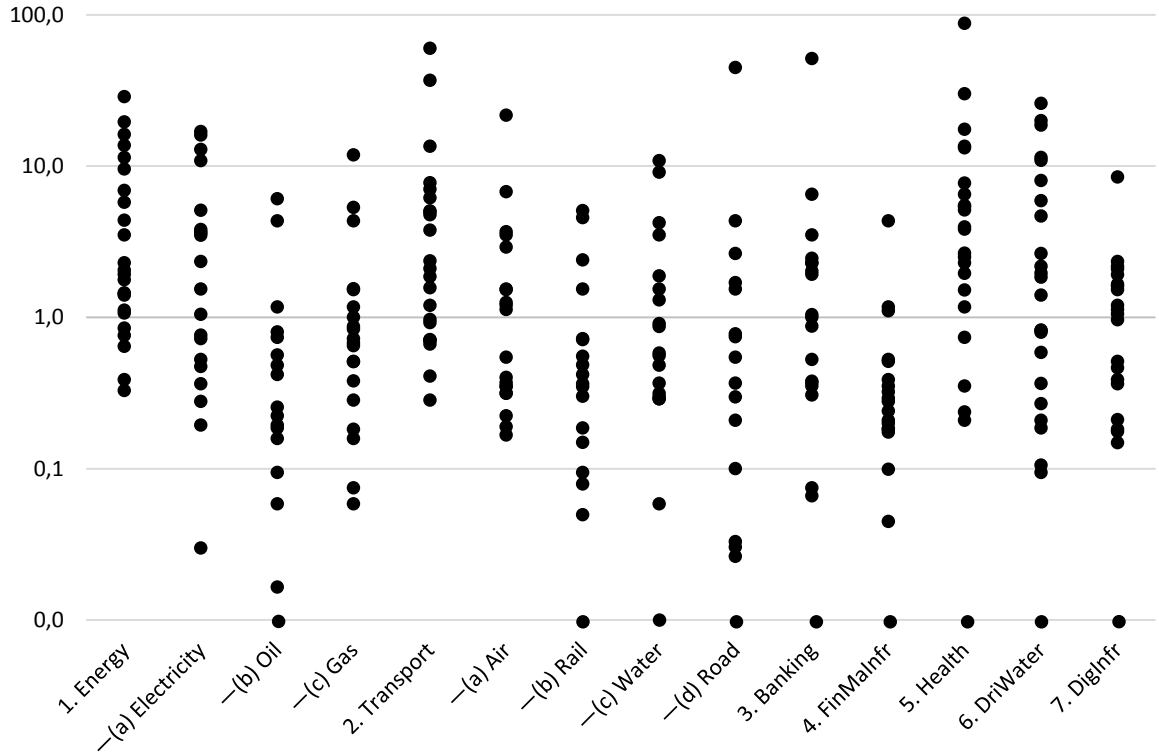

Figure 4: Number of OES identified by 25 Member States in each sector and subsector (per 1 000 000 inhabitants, on a logarithmic scale, outliers omitted for clarity). Each data point represents the number of identified OES by a Member State in the respective (sub)sector.[14]

[14] Identical data points are plotted on top of one another. That is why not all 25 data points are visible on the plots. For example, both Denmark and the Netherlands have identified 0.35 OES per 1 000 000 inhabitants in the air transport subsector.

2.5 Application of the Directive to other sectors than those included in Annex II

A study of the data submitted reveals that 11 out of 28 Member States have identified essential services in sectors not falling under the scope of Annex II of the Directive. Out of these 11 Member States, 7 have identified a total of 157 OES providing services not covered by the types of entities in Annex II.

Additional sector	Examples of entities	Number of Member States
Information infrastructures	Data centres, server farms	5
Financial services (entities not listed in Annex II)	Insurance and reinsurance companies	4
Government services	Electronic services for citizens	4
Heat	Heat producers and suppliers	3
Wastewater	Collection and treatment facilities	3
Logistics	Postal services	2
Food	Producers, trading venues	2
Environment	Disposal of hazardous waste	2
National security/emergency services	112, crisis management	2
Chemical industry	Suppliers and producers of substances	2
Social services	Entities in charge of social benefits	1
Education	Authorities in charge of national exams	1
Collective catering	Distribution management	1
Water	Hydraulic structures	1

Table 5: Sectors chosen by Member States in addition to the ones listed in Annex II

Information infrastructures (identified by five Member States), financial services provided by entities not listed in Annex II (identified by four Member States) and government services (identified by four Member States) are the most popular categories (Table 5).

Given how essential cyber-resilience is for the functioning of the economy and society as a whole, a number of Member States have decided to make use of the opportunity to cover sectors other than only those listed in Annex II. The fact that several Member States chose to apply the NIS Directive to additional sectors gives rise to the question whether the current

scope of Annex II is appropriate in order to meet the objective of protecting all operators in the Union that are critical for society and the economy.

2.6 The cross-border consultation procedure

Article 5(4) of the NIS Directive requires Member States to engage in consultation with each other before reaching a final decision regarding the identification of operators providing services in more than one Member State. The Cooperation Group has issued a reference document in July 2018 in order to help Member States conduct proper cross-border consultations.[15]

Based on the information received, only very few national authorities have chosen to contact their counterparts in other Member States and only two Member States have contacted other Member States in a comprehensive manner. In addition, just a few Member States have indicated to have reached out to other authorities in a less systematic manner. In spite of the high importance of cross-border services in the internal market, most Member States that have contacted other Member States have done so only for a very limited number of operators. Despite limited use of the procedure by Member States, many national authorities have expressed interest in the cross-border consultation process and consider it an important element of the NIS identification framework. In fact, several Member States have expressed concern that without effective cross-border consultation operators might be forced to deal with a multitude of different regulatory requirements or be put at a disadvantage vis-à-vis other less tightly regulated OES active in the market.

Together with the national authorities, the Commission has identified several reasons why the consultation procedure is so far not being used as intended:

- Many Member States took longer to identify their OES than expected. Early adopters therefore felt unable to consult those countries.
- The lack of secure channels to transfer information: some Member States expressed reluctance to communicate with their counterparts considering the names of operators as classified information.

[15] *Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact*, Cooperation Group Publication 07/2018.

- The considerable number of existing cross-border dependencies, which resulted in the need to contact a significant number of Member States concerned, especially in the case of pan-European operators.
- The lack of a common understanding of goals and scope of the cross-border consultation exercise: while some Member States regard it merely as a tool to inform each other about OES identifications with cross-border impact, others see its purpose as aligning thresholds and regulatory requirements. Recital 24 of the Directive suggests that it is most of all a procedure to jointly assess the criticality of an operator for the purpose of the identification process.
- Another problem arises when a Member State is contacted by two other Member States regarding the same operator. In such a case, the Member State in question might not be able to align its rules with both Member States at the same time. For this purpose, Recital 24 envisages multilateral discussions. It is important that Member States make use of this possibility to ensure consistency.

2.7 Consideration of the *lex specialis* principle in the identification process

The Commission has identified some level of inconsistency amongst Member States with regard to the application of the *lex specialis* principle. This has led to an uneven application of the Directive, resulting on the one hand in the identification of OES where sector-specific rules apply and on the other hand in insufficient OES identification in some Annex II sectors.

Article 1(3) stipulates that the NIS Directive does not apply to undertakings subject to the requirements of the Telecom Framework Directive[16]. However, some Member States appear to have identified OES providing services that should actually be regulated under the Telecom Framework Directive, such as internet access and telephony services.

In addition, according to Article 1(7) the provisions of the NIS Directive on security requirements and incident notification do not apply to operators that are already regulated by sector-specific Union legal acts laying down obligations of at least equivalent effect.

[16] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services.

While most Member States have identified OES in the banking and financial markets sectors, a few Member States have not identified OES, claiming that operators are providing services covered by *leges speciales*.

The Commission is still in the process of gathering detailed information about the application of the *lex specialis* principle under the NIS Directive. It is currently conducting in-depth checks of the national legislation and country visits in order to assess the current level of transposition and implementation, including regarding the *lex specialis* provisions. On that basis, the Commission intends to further discuss the *lex specialis* principle in the Cooperation Group with a view to achieving a better alignment across Member States.

3. Conclusions

This report evaluates the approaches chosen by Member States to identify operators of essential services (OES) under the NIS Directive. Its goal is to assess the level of consistency between the practices of Member States in view of the possible impact of the current framework on the functioning of the internal market and the management of the risks associated with cyber-dependence.

The analysis conducted shows that the NIS Directive has served as catalyst in many Member States paving the way for real change in the institutional and regulatory landscape with regard to cyber-security. In addition, the obligation to identify operators of essential services has triggered a comprehensive assessment of the risks associated with operators active in critical activities and modern network and information systems in almost all the Member States. This can be considered an achievement for the Union as a whole in line with the objectives of the Directive.

For the purpose of this report, the Commission has examined the national identification methodologies, the services national authorities deem as essential, the identification thresholds, and the numbers of OES identified in the various sectors covered by the Directive:

- **Member States have developed a variety of methodologies** when it comes to the overall approach to the identification of OES (section 2.1) but also regarding the definition of essential services and the setting of thresholds. This can have a negative impact on the consistent application of the NIS provisions across the Union with possible consequences for the well-functioning of the internal market and the effective handling of cyber-dependencies.

- In addition, it seems that there **are diverging interpretations by Member States as to what constitutes an essential service under the NIS Directive**, with Member States applying different levels of granularity (see section 2.2). This makes it difficult to compare the lists of essential services. In addition, **the scope of the Directive risks being fragmented**, with some operators being exposed to additional regulation (because they have been identified by their respective Member State) while others providing similar services remaining excluded (because they have not been identified). In order to address

these inconsistencies, further work based on the experience of Member States could lead to a more aligned list of essential services.

- Moreover, the report has also found significant inconsistencies in the way thresholds are applied by Member States (section 2.3). A further **alignment of thresholds on EU level** could help alleviate this problem. Such work could for example be undertaken by sectoral work streams under the Cooperation Group, taking into account national specificities, such as the special requirements of small Member States.

- The fact that some countries have made use of the possibility to identify essential services in additional sectors or subsectors beyond those covered by Annex II **highlights that there are other sectors potentially vulnerable to cyber-incidents than considered by the NIS Directive** (section 2.5). The identification of OES in sectors, such as information infrastructures, financial services not covered by entities listed in Annex II and government can improve the cyber-resilience of organisations in such sectors. However, if only a subset of Member States identifies OES in such sectors, this could have negative consequences for the internal market and the level playing field, which it is supposed to ensure.

The many methodologies and best practices that national authorities have devised are of particular value and should be taken into account in the future, for example in the work of the Cooperation Group and the continuous identification of OES by Member States. However, the current level of diversity could have a negative impact on achieving the Directive's goals.

The Commission draws the preliminary conclusion that, while the NIS Directive has set into motion a crucial process to increase and improve risk management practices of operators in critical sectors, there is a considerable degree of fragmentation across the Union when it comes to the identification of OES. This is partly due to the design of the Directive and partly due to the different implementation methodologies used by the Member States.

Member States should seek to apply the provisions of the NIS Directive in a manner as consistent as possible, making full use of guidance documents developed by the Commission and the Cooperation Group. The Commission has therefore identified several national actions that could help alleviate the problems highlighted in this report:

- Many Member States have not completed the OES identification process within the timeframe set by the Directive. Moreover, on the date of publication of this report 23

Member States had submitted all the data required under Article 5(7). An additional 5 Member States had provided partial information. The Commission **urges the national authorities in charge of identification to complete the process** as quickly as possible and to transmit the information necessary to the Commission in the shortest delay.

- Competent authorities should regularly review their lists of essential services and **ensure that all existing essential services are identified** so that the number of "consistency gaps" regarding essential services across the internal market is reduced.

- Member States should more actively **engage with each other in order to align thresholds** where possible and especially in sectors with a strong cross-border dimension, such as transport or energy. This can be achieved via the cross-border consultation procedure provided for in Article 5(4) of the NIS Directive but also by making better use of the existing structures of the Cooperation Group.

- National authorities should consult each other in order to ensure that cross-border operators **face similar security and incident reporting requirements** in the internal market. Moreover, Member States should contact such operators to gather more information about regulatory divergence. Enhanced cyber-resilience should not come at the cost of regulatory fragmentation. Where necessary, Member States should also engage in multilateral discussions, as envisaged by Recital 24 of the NIS Directive.

In addition to national actions, there are a number of measures that could potentially be taken at Union level and that would lead to increased consistency. The Commission will launch discussions to improve the uneven and at times fragmented identification landscape. Some of the potential measures are:

- **The role of the NIS Cooperation Group should be strengthened** in order to promote a common understanding on how to implement the Directive in a more consistent manner. For this purpose, the Commission will propose that the existing dedicated work stream on identification of OES reviews swiftly its **guidelines to better tackle existing inconsistencies**. The Cooperation Group should also explore the creation of additional sectoral work streams[17] with a view to increasing coherence

[17] Work streams on energy and on digital infrastructures have been created in June 2018 and July 2019.

between Member States and the use of a tailor-made communication tool to enhance collaboration within the group.

- Only very few Member States are currently making use of the **cross-border consultation procedure** when it comes to identifying operators that are providing essential services in more than one Member State. In order to enhance the exchange of information, the Cooperation Group should review its reference document on the modalities of the consultation process in cases with cross-border impact and agree on a consistent interpretation of the scope, objectives and procedures of such exercise. At the same time, the Commission will look into ways allowing for a **secure exchange of information between competent authorities**.

- There appears to be a certain degree of inconsistency in the application of the provisions of the Directive on *lex specialis* amongst Member States. The Commission will therefore make use of the structures of the Cooperation Group to **discuss cases where the application of the *lex specialis* principle may not be correct**.

Actions taken at Union level should guarantee a coherent framework, taking into account both sectoral activities envisaging specific or higher requirements on cyber-security and other European legislation.

4. Annexes

4.1 Overview of the available data by Member State

Member State	Submission date	List of services	Numbers of OES	Thresholds
AT	Late submission	Delivered	MISSING	Delivered
BE	Late submission	Delivered	MISSING	MISSING
BG	Late submission	Delivered	Delivered	Delivered
CY	On time	Delivered	Delivered	Delivered
CZ	Late submission	Delivered	Delivered	Delivered
DE	On time	Delivered	Delivered	Delivered
DK	On time	Delivered	Delivered	Delivered
EE	On time	Delivered	Delivered	Delivered
EL	Late submission	Delivered	Delivered	Delivered
ES	On time	Delivered	Delivered	Delivered
FI	On time	Delivered	Delivered	Delivered
FR	On time	Delivered	Delivered	No official thresholds
HR	On time	Delivered	Delivered	Delivered
HU	On time	Partially delivered	Partially delivered	Partially delivered
IE	Late submission	Delivered	Delivered	Delivered
IT	Late submission	Delivered	Delivered	Delivered
LT	On time	Delivered	Delivered	Delivered
LU	Late submission	Delivered	Delivered	Delivered
LV	Late submission	Delivered	Delivered	Delivered
MT	Late submission	Delivered	Delivered	Delivered
NL	Late submission	Delivered	Delivered	Delivered
PL	On time	Delivered	Delivered	Delivered
PT	On time	Delivered	Delivered	Delivered
RO	Late submission	Delivered	Partially delivered	MISSING
SE	On time	Delivered	Delivered	Delivered
SI	Late submission	Delivered	MISSING	Delivered
SK	On time	Delivered	Delivered	Delivered
UK	On time	Delivered	Delivered	Delivered

4.2 Numbers of services and OES identified by each Member State

Member State	Identified OES	Services under Annex II	Additional services
AT	0	46	0
BE	0	31	0
BG	185	30	3
CY	20	29	17
CZ	50	31	12
DE	573	15	12
DK	128	39	0
EE	137	18	6
EL	67	30	0
ES	132	55	18
FI	10897[18]	20	0
FR	127	70	20
HR	85	49	2
HU	42	12	0
IE	64	26	0
IT	553	37	0
LT	22	37	0
LU	49	21	0
LV	66	18	0
MT	36	29	2
NL	42	12	0
PL	142	87	0
PT	1250	26	0
RO	86	77	0
SE	326	27	0
SI	0	34	2
SK	273	28	7
UK	470	34	0

[18] Due to Finland's identification methodology, a very large number of OES were identified in the health sector.

4.3 Services identified by Member States in the electricity subsector

Member State	Identified services
AT	– Electricity production facilities – Control systems in production facilities – Distribution grids – Transmission grids
BE	– Production, transport and distribution companies – Electricity distribution – Electricity transport
BG	– Production of electricity – Transmission of electricity – Operation, maintenance and development of an electricity transmission system – Distribution of electricity – Ensuring the functioning and maintenance of a distribution system for electrical energy – Electricity Market
CY	– Generation / Supply – Distribution / Transmission – Electricity Market Services
CZ	– Electricity production – Electricity sale – Transmission system operation – Distribution system operation
DE	– Power supply
DK	– Electricity Transmission – Electricity Distribution – Electricity Production
EE	– Electricity supply
EL	– Electricity supply – Electricity distribution – Electricity transmission
ES	– Electricity generation – Electricity transmission – Electricity distribution – Centres for operation and control of electric systems
FI	– Transmission service, – Distribution of electricity in the distribution network – Electricity supply through high voltage distribution networks
FR	– Sale or resale of electricity to wholesale and end customers – Distribution of electricity – Transmission of electricity
HR	– Production of electricity – Transmission of electricity – Distribution of electricity
HU	– Electricity
IE	– Distribution system operators – Electricity undertakings – Transmission system operators
IT	– Generation – Trading – Transmission – Distribution
LT	– Electricity production service – Electricity transmission service – Electricity distribution service – Electricity supply service

LU	– Electricity supply – Electricity distribution – Electricity transmission
LV	– Electricity generation – Electricity distribution – Electricity transmission
MT	– Provision of electricity to consumers – Transmission and/or distribution of electricity to consumers – Electricity generation to consumers
NL	– Transmission and distribution of electricity
PL	– Electric power generation – Electric power transmission – Electric power distribution – Trade in electric power – Electric power storage – Quality-assurance services and management of energy infrastructure
PT	– Distribution system operators – Transmission system operators
RO	– Production of electricity – Supply of electricity to consumers – Operation of centralized electricity markets – Transport of electricity – Operation of the power system – Distribution of electricity
SE	– TSO – DSO – Production – Wholesale
SI	– Production of electricity in hydroelectric power plants – Production of electricity in thermal power stations, nuclear power plants – Transmission of electricity – Distribution of electricity – Trade of electricity
SK	– Electricity company – Transmission system operator – Distribution system operator
UK	– Electricity supply – Electricity transmission – Electricity distribution

4.4 Services identified by Member States in the rail transport subsector

Member State	Identified services
AT	– Rail infrastructures – Railway cargo transport – Railway passenger transport – Railway stations
BE	– Infrastructure managers – Railway undertakings
BG	– Providing, maintaining and managing service facilities – Rail transport by railway carriers – Providing guidance on rail transport
CY	No identification in this subsector
CZ	– Railway operation – Operation of railway transportation or service facility
DE	– Rail
DK	– Rail infrastructure management – Rail transport
EE	– Railway infrastructure manager – Railway transport service
EL	– Railway infrastructure management – Rail services
ES	– Railway service management – Railway transport management – Railway network services – Railway information and telecommunication management
FI	– State infrastructure management – Traffic management services
FR	– Rail services – Control and management of rail traffic – Infrastructure maintenance – Freight and hazardous materials – Passenger transport – Rolling stock maintenance – Metros, tram and other light rail services (including underground services)
HR	– Managing and maintaining rail infrastructure, including traffic management and control-command and signalling subsystem – Rail transport services of goods and/or passengers – Managing service facilities and providing services in service facilities – Providing additional services necessary for rail transport of goods or passengers
HU	No identification in this subsector
IE	– Infrastructure managers – Railway undertakings
IT	No identification in this subsector
LT	– Carriage of passengers and luggage by rail service – Rail freights service – Railway infrastructures development, management and maintenance service
LU	– Rail infrastructure management – Cargo and passenger rail transport
LV	N/A
MT	N/A
NL	No identification in this subsector

PL	– Preparing train timetables – Passenger railway transport – Freight railway transport
PT	– Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council. – Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU.
RO	– Traffic control and management – Freight transport – Transport of dangerous goods – Passenger transport – Metro, tramway and other light rail services – Maintenance of railway infrastructure – Maintenance of rolling stock
SE	– Infrastructure management – PAX transport – Cargo transport
SI	– Passenger rail transport, interurban – Freight rail transport – Service activities incidental to land transportation (operation of railway stations etc.)
SK	– Infrastructure operators – Railway companies
UK	– Rail services – High speed rail services – Metros, trams and other light rail services (including underground services) – International rail services