Council of the European Union

Brussels, 14 September 2017
(OR. en)

12205/17
ADD 1

CYBER 128
TELECOM 208
DATAPROTECT 142
JAI 786
MI 630
CSC 206

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	13 September 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2017) 476 final ANNEX 1
Subject:	ANNEX to the 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

Delegations will find attached document COM(2017) 476 final ANNEX 1.

Encl.: COM(2017) 476 final ANNEX 1

EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 476 final

ANNEX 1

ANNEX

to the

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

TABLE OF CONTENTS

ANNEX 4
1. Introduction. 4
2. National strategy on security of network and information systems. 5
2.1. The scope of the national strategy. 5
2.2. Content and procedure for adoption of the national strategies. 6
2.3. Process and issues to be addressed. 6
2.4. Concrete steps that Member States must undertake before the transposition deadline. 8
3. NIS Directive: National competent authorities, single contact points and Computer Security Incident Response Teams (CSIRTs). 10
3.1. Type of authorities. 11
3.2 Publicity and additional relevant aspects. 11
3.3. NIS Directive, Article 9: Computer Security Incident Response Teams (CSIRTs). 17
3.4. Tasks and requirements. 17
3.5. Assistance for the development of CSIRTS. 18
3.6. The role of the single point of contact. 18
3.7. Penalties. 19
4. Entities under obligations concerning security requirements and incident notifications. 20
4.1. Operators of essential services (OES). 20
4.1.1. Type of entities listed in NIS Directive Annex II. 20
4.1.2. Identification of operators of essential services. 22
4.1.3. Inclusion of additional sectors. 23
4.1.4. Jurisdiction. 24
4.1.5. Information to be submitted to the Commission. 24
4.2. Security requirements. 30
4.3 Notification requirements. 30
4.4. NIS Directive, Annex III: Digital Service Providers. 31
4.4.1. Categories of DSPs. 31
4.4.2. Security requirements. 34
4.4.3. Notification requirements. 34
4.4.4. Risk-based regulatory approach. 35
4.4.5. Jurisdiction. 35
4.4.6. Exemption of Limited Scale digital service providers from the scope of the security requirements and notification. 36

5. The relationship between the NIS Directive and other legislation. 36
5.1. NIS Directive, Article 1(7): The provision of *lex specialis.* 36
5.2 NIS Directive, Article 1(3): Telecom providers and trust service providers. 40
6. Published National Cyber-Security Strategy Documents. 41
7. List of good practices and recommendations issues by ENISA. 44

ANNEX

1. Introduction.

This Annex aims to contribute to an effective application, implementation and enforcement of the NIS Directive (EU) 2016/1148 on the security of network and information systems across the Union[1] (hereinafter referred to as "NIS Directive" or the "Directive") and to help the Member States to ensure that EU law is applied effectively. More particularly, its specific objectives are threefold: (a) to offer greater clarity to national authorities on the obligations contained in the Directive that apply to such authorities, (b) to ensure the effective enforcement of the Directive's obligations applying to entities under obligations concerning security requirements and incident notifications, and (c) to overall contribute to create legal certainty for all relevant actors.

To this end, this Annex provides guidance on the following aspects, which are key to achieve the goal of the NIS Directive i.e., to ensure a high common level of security of network and information systems within the EU, underpinning the functioning of our society and economy:

- Member States' obligation to adopt a national strategy on security of network and information systems (section 2);
- The setting up of national competent authorities, single contact points and Computer Security Incident Response Teams (section 3);
- The security and incident notifications requirements applicable to operators of essential services and to digital service providers (section 4); and
- The relationship between the NIS Directive and other legislation (section 5)

To prepare this guidance, the Commission has used input and analysis gathered during the preparation of the Directive, input from European Agency for network and information security ("ENISA") and Cooperation Group. It has also used experiences from specific Member States. When appropriate, the Commission has taken into account the guiding principles for interpreting EU law: the wording, context and objectives of the NIS Directive. Given that the Directive has not been transposed, no ruling of the Court of Justice of the European Union (CJEU) or national courts has yet been rendered. Therefore, it is not possible to use case-law as guidance.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. The Directive entered into force on 8 August 2016.

Compiling this information in a single document may allow Member States to have a good overview of the Directive and take this information into account when devising their national legislation. At the same time, the Commission stresses that this Annex is not binding and does not intend to create new rules. The final competence to interpret EU law lies with the CJEU.

2. National strategy on security of network and information systems.

Pursuant to Article 7 of the NIS Directive, Member States are required to adopt a national strategy on the security of network and information systems that can be considered equivalent to the term National Cyber Security Strategy ("NCSS"). The function of a national strategy is to define the strategic objectives and appropriate policy and regulatory actions in relation to cybersecurity. The concept of NCSS is widely used internationally and in Europe, notably in the context of ENISA's work with Member States on national strategies which recently resulted in an updated NCSS Good Practice Guide.[2]

In this section the Commission specifies how the NIS Directive enhances Member States' preparedness by requiring to have in place robust national strategies on the security of network and information systems (Article 7). This section addresses the aspects: (a) the scope of the strategy, and (b) the content and procedure for adoption.

As further described below, the correct transposition of Articles 7 of the NIS Directive is fundamental for the achievement of the Directive's objectives and it necessitates the allocation of adequate financial and human resources for this purpose.

2.1. The scope of the national strategy.

Pursuant to the wording of Article 7, the obligation to adopt a NCSS only applies to the *'sectors referred to in Annex II* (i.e., electricity, transport, banking, financial market, health, drinking water supply and distribution and digital infrastructure) *and to the services referred to in Annex III*' (online marketplace, online search engine and cloud computing service).

Article 3 of the Directive specifically sets forth the principle of minimum harmonisation, pursuant to which Member States may adopt or maintain provision with a view to achieving a higher level of security of network of information systems. The application of this principle to the obligation to adopt a "NCSS" enables Member States to include more sectors and services than those covered in Annex II and III of the Directive.

In the Commission's view and in the light of the objective of the NIS Directive, i.e., to achieve a high common level of security of network and information systems within the Union[3], it would be advisable to develop a national strategy that encompasses all relevant dimensions of society and economy, and not only the sectors and digital services covered

[2] ENISA, *National Cyber-Security Strategy Good Practice* 2016). Available at https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[3] See Article 1(1)

respectively in Annex II and III of the NIS Directive. This is in line with international best practices (see ITU Guidance and OECD analysis referred to later) and the NIS Directive.

As further explained below this is particularly the case regarding public administrations responsible for sectors and services other than those listed in the Directive's Annexes II and III. Public administrations may process sensitive information, which warrant the need of being covered by NCSS and management plans preventing leaks and ensuring the adequate protection of this information.

2.2. Content and procedure for adoption of the national strategies.

Pursuant to Article 7 of the NIS Directive, a NCSS needs to include at least the following:

i) objectives and priorities of the national strategy on the security of network and information systems;
ii) a governance framework to achieve the objective and priorities of the national strategy;
iii) the identification of measures relating to preparedness, response and recovery, including cooperation between public and private sectors;
iv) an indication of relevant education, awareness-raising and training programmes;
v) an indication of research and development plans;
vi) a risk assessment plan to identify risks; and
vii) a list of the actors involved in the implementation of the strategy.

Neither Article 7 nor the corresponding recital (29) specify the requirements for adoption of an NCSS or provide more granularity on the content of the NCSS. As far as process is concerned and additional elements related to the content of the NCSS, the Commission considers the approach set out below as one appropriate way of adopting a NCSS. This is based on the analysis of Member States and third countries' experiences of how Member States have developed their own strategies. A further information resource is ENISA's NCSS training tool available as video clips and downloadable media on its website[4].

2.3. Process and issues to be addressed.

The process of drafting and the subsequent adoption of a national strategy is complex and multifaceted, requiring sustained engagement with cybersecurity experts, civil society and the national political process if it is to be effective and successful. A *sine qua non* is senior administrative support at least at State Secretary or equivalent level in the lead ministry, as well as political sponsorship. In order to successfully adopt a NCSS, the following a five step process (see Figure 1) can be considered:

First step - **Establishment of guiding principles and strategic goals arising from the strategy.**

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

First of all, national competent authorities should define some key elements to be included in the NCSS, namely what are the desired outcomes, in the Directive parlance (Art. 7(1)(a) *'objectives and priorities'*, how do such outcomes complement national social and economic policies and are they compatible with the privileges and obligations arising from being a Member State of the European Union. Objectives should be specific, measurable, achievable, realistic and time-bound (SMART). An illustrative example is the following: "*We will ensure that this [time bound] strategy is founded upon a rigorous and comprehensive set of metrics against which we measure progress towards the outcomes we need to achieve*"[5]

The above also encompasses a political assessment as to whether a significant budget can be obtained to resource the implementation of the strategy. It also entails a description of the intended scope of the strategy and the various stakeholder categories from public and private sectors who should be involved in the drafting of the various objectives and measures.

This first step could be achieved through focused workshops with senior ministry officials and politicians moderated by cyber specialists with professional communication skills who can highlight the implications of no or weak cyber security for a modern digital economy and society.

Second step - **Development of the strategy's content.**

The strategy should contain enabling measures, time-based actions and key performance indicators for resulting evaluation, refinement and improvement after a defined implementation period. These measures should support the objective, priorities and outcomes set forth as guiding principles. The need to include enabling measures is set forth in Article 7(1)(c) of the NIS Directive.

It is recommended that a steering group chaired by the lead ministry be formed to manage the drafting process and facilitate input. This could be achieved through a number of drafting groups of relevant officials and experts around key generic themes, for example risk assessment, contingency planning, incident management, skills development, awareness raising, research and industrial development etc. Separately, each sector (for example energy, transport etc.) would also be invited to assess the implications of their inclusion, including resourcing, and involve the designated operators of essential services and key digital service providers in determining priorities and submitting proposals to the drafting process. Involvement of sectoral stakeholders is essential also bearing in mind the need to ensure a harmonised implementation of the Directive across different sectors, while at the same time allowing for sectoral specificity.

Third step - **Development of a governance framework.**

In order to be efficient and effective, the governance framework should be based on key stakeholders, identified priorities in the drafting process and on the constraints and context of the national administrative and political structures. It would be desirable to have direct

[5] Extract from the UK's National Cyber Security Strategy, 2016 -2021, page 67.

reporting to the political level, with the framework having a decision-making and resource allocation capability, as well as input from cybersecurity experts and industry stakeholders. Article 7(1)(b) of the NIS Directive refers to the governance framework and specifically requires *'the responsibilities of the government bodies and the other relevant actors*'.

Fourth step - **Compilation and review of the draft strategy.**

At this stage, the draft strategy should be compiled and reviewed by using strengths, weaknesses, opportunities and threats (SWOT) analysis, which could define whether it would be necessary to revise the content. Following the internal review, stakeholder consultation should take place. It would be essential to also undertake a public consultation to highlight the importance of the proposed strategy with the public, receive input from all possible sources and seek support for the resourcing required to subsequently implement the strategy.

Fifth step – **Formal adoption.**

This final step involves formal adoption at political level with an enabling budget that reflects the seriousness which the Member State concerned attaches to cybersecurity. To achieve the objectives of the NIS Directive and, in communicating the national strategy document to the Commission pursuant to Article 7(3), the Commission encourages Member States to provide information on the budget. Commitments concerning budget and necessary human resources are absolutely critical for the effective implementation of the strategy and the Directive. As cybersecurity is still a rather new and rapidly expanding area of public policy, new investments are required in most cases even if the overall situation in public finances calls for cuts and savings.

Advice on the process and content of national strategies is available from various public and academic sources, for example ENISA[6], the ITU[7], the OECD[8], the Global Forum for Cyber Expertise and the University of Oxford[9].

[6] ENISA, *National Cyber-Security Strategy Good Practice* 2016). Available at https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU will also release a National Cyber Security Strategy Toolkit in 2017 (see presentation at http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Available at: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre and University of Oxford, Global Cyber *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Available at: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

2.4. Concrete steps that Member States must undertake before the transposition deadline.

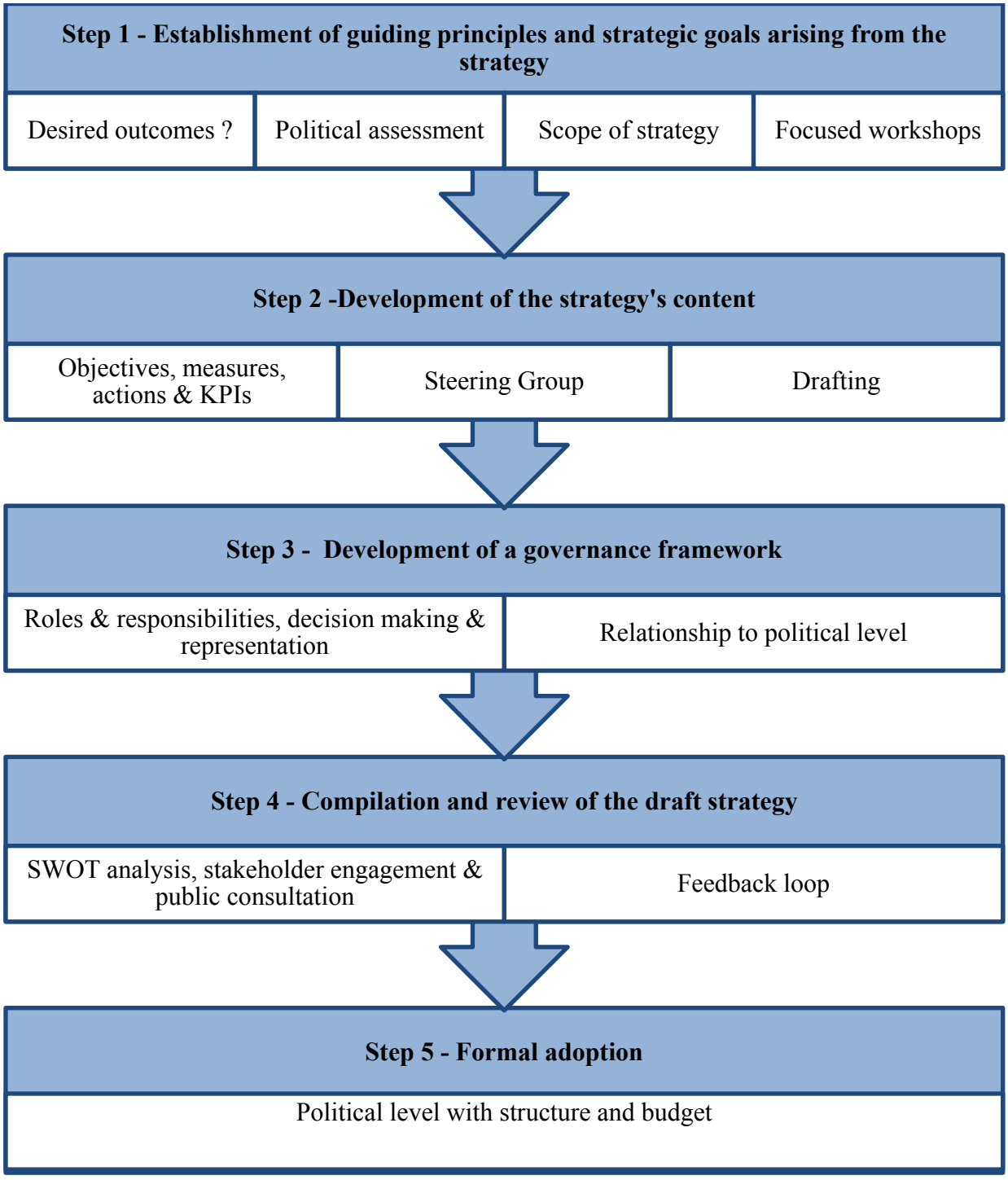
Prior to the adoption of the Directive, almost all Member States[10] had already published documents indicated as NCSS. Section 6 of this Annex lists the strategies currently in place in each Member State[11]. They usually include strategic principles, guidelines, objectives, and in some cases specific measures for mitigating risks associated with cybersecurity.

Given that some of these strategies were adopted prior to the adoption of the NIS Directive, they may not necessarily contain all the elements of Article 7. To ensure correct transposition, Member States will need to undertake a gap analysis by mapping the content of their NCSS to the seven distinct requirements listed in Article 7 across the scope of sectors listed in the Directive's Annex II and services listed in Annex III. Identified gaps can then be addressed through a revision of their existing NCSS or by deciding on a complete revision of the principles of their national NIS strategy from scratch. The guidelines provided above regarding the process for adoption of NCSS are also relevant for the revision and update of existing NCSS.

[10] Apart from Greece where a national cyber security strategy is under preparation since 2014 (see at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] This information is based on the overview of NCSS provided by ENISA at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Figure 1: 5-step-process to adopt NCSS



3. NIS Directive: National competent authorities, single contact points and Computer Security Incident Response Teams (CSIRTs).

Pursuant to Article 8(1), Member States are required to designate one or more national competent authorities, covering at least the sectors referred to in the Directive's Annex II and

the services referred to in its Annex III, with the task to monitor the application of the Directive. Member States can assign this role to an existing authority or authorities.

The section focuses on how the NIS Directive enhances Member States' preparedness by requiring to have effective national competent authorities and Computer Security Incident Response Teams (CSIRTs). More precisely, the section covers the obligation to designate national competent authorities including the role of the single point of contact. It discusses three topics: (a) possible national governance structures (e.g., centralised, de-centralised models, etc.) and other requirements; (b) the role of the single point of contact and (c) Computer Security Incident Response Teams.

3.1. Type of authorities.

Article 8 of the NIS Directive requires Member States to designate national competent authorities on security of networks and information systems, while explicitly recognising the possibility to designate *'one or more national competent authorities*'. Recital 30 of the Directive explains this policy choice: "*In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks link to the security of the network and information systems of operators of essential services and digital service providers under this Directive".*

Accordingly, Member States are free to choose to appoint one central authority dealing with all sectors and services covered by the Directive or several authorities, depending for example on the type of sector.

When deciding on the approach, Member States can draw on the experience from the national approaches used in the context of the existing legislation on critical infrastructure protection (CIIP). As described in Table 1, in the case of CIIP, Member States decided to adopt either a centralised or a decentralised approach when assigning competences at national level. National examples are used here for illustrative purposes only and with a view to bringing existing organisational frameworks to the attention of Member States. Hence, the Commission does not imply that the model used by respective countries for CIIP should be necessarily used for the purpose of transposition of the NIS Directive.

Member States may also opt for various hybrid arrangements involving elements of both centralised and decentralised approaches. The choices can be made in alignment with prior national governance arrangements for the various sectors and services covered by the Directive, or newly determined by the authorities concerned and by the relevant stakeholders identified as operators of essential services and digital service providers. The existence of specialist expertise on cyber security, resourcing considerations, the relations between the stakeholders and national interests (for example economic development, public security etc.) may also be important factors leading to the choices made by Member States.

3.2 Publicity and additional relevant aspects.

Pursuant to Article 8(7), Member States need to inform the Commission about the designation of national competent authorities and their tasks. This must be done by the transposition deadline.

Articles 15 and 17 of the NIS Directive requires Member States to ensure that competent authorities have specific powers and means to carry out the tasks set forth in such articles.

Furthermore, the designation of specific entities as national competent authorities needs to be made public. The Directive does not specify how such publicity must be carried out. Given that the objective of this requirement is to achieve a high level awareness by the actors covered by NIS and the general public, and based on experiences in other sectors (telecommunications, banking, medicines), the Commission considers that this could be met, for example, by means of a well-advertised portal.

Article 8(5) of the NIS Directive requires such authorities to have 'adequate resources' to carry out the tasks assigned by the Directive.

Table 1: National approaches to critical information infrastructure protection (CIIP).

In 2016, ENISA published a study[12] regarding the different approaches Member States follow to protect their critical information infrastructures. There are two profiles described as to the CIIP governance in Member States which can be used in the context of the transposition of the NIS Directive.

Profile 1: Decentralised approach –with multiple sector-based authorities being competent for specific sectors and services referenced in Annex II and III of the Directive.

The decentralised approach is characterised by:

(i) The principle of subsidiarity

(ii) Strong cooperation between public agencies

(iii)Sector-specific legislation

The principle of subsidiarity.

Instead of establishing or designating a single agency with overall responsibility, the decentralised approach follows the principle of subsidiarity. This means that the responsibility for implementation is in the hands of a sector-specific authority, which understands best the local sector and has an existing established relationship with stakeholders. Under this principle, decisions are taken by those closest to those being impacted.

Strong cooperation between public agencies.

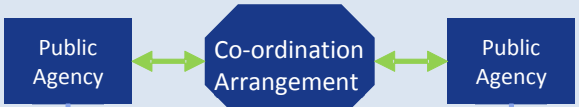
Because of the variety of public agencies involved with CIIP, many Member States developed cooperation schemes in order to coordinate the work and efforts of the different authorities. These cooperation schemes can take the form of informal networks or more institutionalised fora or arrangements. However, these cooperation schemes only serve the purpose of information exchange and coordination between the different public agencies, but have no authority over them.

Sector-specific legislation.

The countries that follow the decentralised approach across critical sectors often refrain from legislating for the purpose of CIIP. Instead, the adoption of laws and regulations remains sector-specific and therefore can vary greatly between sectors. This approach would have the advantage of aligning NIS-related measures with existing sector-based regulations to improve both the acceptance by the sector and the effectiveness of enforcement by the authority concerned.

There is a substantive risk of reduced consistency in the application of the Directive across multiple sectors and services with a purist decentralised approach. In this case, the Directive provides for a single national point of contact for liaison on cross border matters and this entity could also be tasked by the Member State concerned, with internal co-ordination and cooperation between multiple national competent authorities, in accordance with Article 10 of the Directive.

Figure 2 – decentralised approach.



3.3. NIS Directive, Article 9: Computer Security Incident Response Teams (CSIRTs).

Pursuant to Article 9, Member States are required to designate one or more CSIRT entrusted with the task of handling risks and incidents for the sectors listed in the NIS Directive's Annex II and the services listed in Annex III. Taking into account the minimum harmonisation requirement enshrined in Article 3 of the Directive, Member States are free to use the CSIRTs also for other sectors not covered by the Directive, such as the public administration.

Member States can opt for establishing a CSIRT within the national competent authority.[14]

3.4. Tasks and requirements.

The tasks of designated CSIRTs, set forth in Annex I of the NIS Directive, include the following:

- Monitoring incidents at a national level;
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
- Responding to incidents;
- Providing dynamic risk and incident analysis and situational awareness; and
- Participating in the network of the national CSIRTs (CSIRTs network) established under Article 12.

Specific additional tasks are set forth in Articles 14(3), 14(5), 14(6), 16(3), 16(6) and 16(7) in relation to incident notifications where a Member State decides that CSIRTs in addition to or instead of national competent authorities can undertake such roles.

In transposing the Directive, Member States have options regarding the role of CSIRTs with incident notification requirements. Direct mandatory reporting to CSIRTs is possible with advantages of administrative efficiency, alternatively Member States can opt to have direct reporting to national competent authorities with CSIRTs having a right of access to the reported information. CSIRTs are ultimately interested in problem solving in deterring, detecting, responding to and mitigating the impact of cyber incidents (including those not critical for mandatory reporting) with their stakeholders with regulatory compliance being a matter for national competent authorities.

Pursuant to Article 9(3) of the Directive, Member States also need to ensure that such CSIRTs have access to a secure and resilient ICT infrastructure.

[14] See Article 9(1) last sentence.

Article 9(4) of the Directive requires Member States to inform the Commission about the remit and main elements of the incident handling process of the designated CSIRTs.

The requirements of CSIRTs designated by the Member States are provided in Annex I of the NIS Directive. A CSIRT has to ensure a high level of availability of its communication services. Its premises and the supporting information systems shall be located in secure sites and be able to ensure business continuity. Moreover, the CSIRT should be enabled to participate in international cooperation networks.

3.5. Assistance for the development of CSIRTS.

The Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF) can provide for significant EU funding in assisting Member State CSIRTs to improve their capabilities and cooperating with each other through an information exchange co-operation mechanism. The cooperation mechanism under development in the SMART 2015/1089 project is intended to facilitate swift and effective operational cooperation on a voluntary basis between Member State CSIRTs, namely in support of the tasks entrusted to the CSIRTs Network under Article 12 of the Directive.

Details of the relevant calls for proposals for capacity building of Member State CSIRTs are available via the website of the Innovation and Networks Executive Agency (INEA) of the European Commission.[15]

The CEF Cybersecurity DSI Governance Board provides an informal structure for policy level guidance and assistance to Member States' CSIRTs for the purpose of capacity building, and for the implementation of the voluntary cooperation mechanism.

A newly established CSIRT or one appointed to fulfil the tasks at Annex I of the NIS Directive can rely on the advice and expertise of ENISA to improve its performance and efficiently deliver its work[16]. In this regard, it is worth to point out that Member State CSIRTs could take as a reference some of the work that ENISA has recently carried out. In particular, as listed in section7 of this Annex, the Agency has issued a number of documents and studies describing good practices, recommendations at a technical level, encompassing CSIRT maturity level assessments, for various CSIRT capabilities and services. In addition, guidance and best practises have also been shared by networks of CSIRTs both at global (FIRST[17]) and European level (Trusted Introducer, TI[18]).

3.6. The role of the single point of contact.

Pursuant to NIS Directive Article 8(3), each Member State must designate a national single point of contact, which will exercise a liaison function to ensure cross–border cooperation

[15] Available at: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] See Article 9(5) NIS Directive.
[17] Forum of Incident Response and Security Teams (https://www.first.org/)
[18] https://www.trusted-introducer.org/

with the relevant authorities in other Member States and with the Cooperation Group and the CSIRT network[19] created by the Directive itself. Recital 31 and Article 8(4) explain the *rationale* for this requirement, i.e., to facilitate cross-border cooperation and communication. This is particularly needed given that Member States may decide to have more than one national authority. Thus, having a single point of contact would facilitate the identification and cooperation of authorities from different Member States.

The liaison role of the single point of contact is likely to involve interaction with the secretariats of the Cooperation Group and of the CSIRT Network in those cases where the national single point of contact is neither a CSIRT nor a member of the Cooperation Group. Furthermore, Member States need to ensure that the single point of contact is informed about the received notifications from operators of essential services and digital service providers.[20]

Article 8(3) of the Directive specifies that in case a Member State adopts a centralised approach, i.e. appointing only one competent authority, that authority will also have the role of the single point of contact. If a Member State opts for a decentralised approach, it could choose one of the different competent authorities to act as single point of contact. Irrespective of the institutional model chosen, whenever a competent authority, the CSIRT and the single point of contact are different entities Member States have an obligation to ensure effective cooperation among them in order to fulfil obligations laid down in the Directive.[21]

The single point of contact is required to submit by 9 August, 2018 and every year thereafter a summary report to the Cooperation Group on received notifications which shall include the number of notifications, the nature of the incidents and the measures taken by authorities, such as informing other affected Member States about the incident or the provision of relevant information to the notifying company for handling of the incident.[22] Upon request of the competent authority or the CSIRT, the single point of contact has to forward the notifications of operators of essential services to the single points of contact of other Member States affected by the incidents.[23]

Member States need to inform the Commission about the designation of the single point of contact and its tasks by the transposition deadline. The designation of the single point of contact is to be made public, in the same way as the national competent authorities. The Commission shall publish the list of designated single points of contact.

3.7. Penalties.

Article 21 gives a margin to Member States to decide on the type and nature of applicable penalties provided that they are effective, proportionate and dissuasive. In other words, Member States are in principle free to decide on the maximum amount for penalties laid down in their national legislation but the chosen amount or percentage should allow the national

[19] A network of national CSIRTs for operational cooperation between Member States under Article 12
[20] See Article 10(3)
[21] See Article 10(1)
[22] Idem
[23] See Article 14(5)

authorities to impose, in every concrete case, effective, proportionate and dissuasive penalties, taking into account different factors such as the graveness or frequency of the infringement.

4. Entities under obligations concerning security requirements and incident notifications.

Entities playing an important role for society and economy referred to in Articles 4(4) and 4(5) of the Directive as operators of essential services (OES) and digital service providers (DSPs) are required to take appropriate security measures and notify serious incidents to the relevant national authorities. The *rationale* is that impacts of security incidents in such services may constitute a major threat to the operation of such services which may cause major disruptions to economic activities and to society at large, potentially undermining user confidence and cause major damage to the economy of the Union.[24]

This section provides an overview of entities included in the scope of the NIS Directive's Annexes II and III and lists their obligations. The identification of operators of essential services is covered extensively, given the importance of this process for the harmonised implementation of the NIS Directive across the EU. It also provides extensive explanations to the definitions of digital infrastructures and digital service providers. It also examines the possible inclusion of additional sectors and further explains the specific approach with regard to DSPs.

4.1. Operators of essential services (OES).

The NIS Directive does not define explicitly which particular entities will be considered as OES under its scope. Instead, it provides criteria that Member States will need to apply in order to carry out an identification process which will ultimately determine which individual companies that belong to the type of entities listed in Annex II will be considered operators of essential services, and therefore subject to the obligations under the Directive.

4.1.1. Type of entities listed in NIS Directive Annex II.

Article 4(4) defines OES as public or private entities of the types listed in Directive's Annex II that meets the requirements of Article 5(2). In Annex II the sectors, subsectors and the type of entities are listed for which each Member States needs to carry out the identification process under Article 5(2)[25]. The sectors include, energy, transport, banking, financial market insfrastructures, health, water and digital infrastructure.

For most of the entities which belong to the 'traditional sectors' EU legislation contains well developed definitions to which Annex II makes a reference. However, for the sector of digital

[24] See recital 2
[25] See below under section 4.1.6. for more details on the identification process

infrastructure, listed under point 7 of Annex II, including Internet Exchange Points, Domain Name Systems and Top-level domain name registries, this is not the case. Therefore, with the aim to clarify these definitions, the following provides an detailed explaination of these definitions.

1) Internet Exchange Point (IXP).

The term Internet Exchange Point is defined in Article 4(13) and clarified further in recital 18 and can be described as a network facility that enables the interconnection of more than two independent technically stand-alone systems, with the primarily purpose to facilitate the exchange of internet traffic. The Internet Exchange Point can also be described as a physical location where a number of networks can exchange internet traffic with each other via a switch. The primary purpose of an IXP is to allow networks to interconnect directly, via the exchange, rather than through one or more third-party networks. The IXP provider is normally not responsible for the routing of the internet traffic. The rooting of the traffic is done by the network providers. The advantages of the direct interconnection are numerous, but the primary reasons are cost, latency, and bandwidth. Traffic passing through an exchange is typically not billed by any party, whereas traffic to an upstream Internet Service Provider (ISP) is. The direct interconnection, often located in the same city as both networks, avoids the need for data to travel over long distances to get from one network to another, thus reducing latency.

It should be noted that the definition of IXP does not cover physical points where only two physical networks interconnect with each other (i.e. the network providers such as BASE and PROXIMUS). Therefore when transposing the Directive Member States must differentiate between operators who are facilitating the exchange of aggregated internet traffic between multiple network operators and those who are single network operators, which physically interconnect their networks based on an interconnection agreement. In the latter case, the network providers are not covered by the definition in Article 4(13). A clarification on this matter can be found in recital 18 which states that the IXP does not provide network access or act as a transit provider or carrier. The last category of providers are undertakings providing public communications networks and/or services which are subject to the security and notification obligations of Article 13a and 13b of Directive 2002/21/EC and therefore excluded from the scope of the NIS Directive.[26]

2) Domain Name System (DNS).

The term domain name system is defined in Article 4(14) as *"a hierarchical distributed naming system in a network which refers queries for domain names"*. More precisely, the DNS can be described as a hierarchical distributed naming system for computers, services or any other resource connected to Internet which enables the encoding of domain names into IP (Internet Protocol) addresses. The main role of the system is to translate the assigned domain names into IP addresses. For this purpose, DNS is operating a data base and using name

[26] See section 5.2. for more details on the relationship between the NIS Directive and Directive 2002/21/EC

servers and resolver to enable this kind of "translation" of the domain names into operational IP addresses. Although the encoding of domain names is not the only one responsibility of the DNS, it is a core task of the system. The legal definition in Article 4(14) focuses on the main role of the system from the user's point of view without going into more technical details, as for example the operation of domain name space, name servers, resolvers, etc. Finally, Article 4(15) clarifies who is to be considered as a provider of DNS services.

3) Top –level domain name registry (TLD name registry).

The top-level domain name registry is defined in Article 4(16) as an entity administrating and operating the registration of internet domain names under a specific top-level domain. Such administration and management of domain names includes the encoding of TLD names into IP addresses.

IANA (Internet Assigned Numbers Authority) is responsible for the global coordination of the DNS Root, Internet Protocol addressing, and other Internet Protocol resources. In particular, IANA is responsible for the assignment of generic Top level domains (gTLD) e.g. '.com' and country code Top-level domains (ccTLD) e.g. '.be', to operators (registries) and the maintenance of their technical and administrative details. IANA maintains a global registry of allocated TLDs and plays a role in the promulgation of this list to Internet users world-wide as well as in the introduction of new TLDs.

An important task of the registries is to allocate second-level names to the so-called registrants under their respective TLD. These registrants are able also on their own to allocate third-level domain names if they chose to do so. The ccTLDs are designated to represent a country or territory based on the ISO 3166-1 standard. The "generic" TLDs do not normally have a geographic or country designation.

It should be noted that the operation of TLDs name registry can include the provision of DNS. For example, pursuant to the delegation rules of IANA, the designated entity dealing with ccTLD needs – *inter alia* – to supervise the domain names and to operate the DNS of that country[27]. Such circumstances need to be taken into account by the Member States when carrying out the identification process of operators of essential services under Article 5(2).

4.1.2. Identification of operators of essential services.

In accordance with the requirements of Article 5 of the Directive, each Member State is required to carry out an identification process with regard to all entities of the types listed in Annex II that have a legal establishment on the territory of that Member State. As a result of this assessment, all entities that fulfil the criteria laid down in Article 5(2) shall be identified as OES and be subject to the security and notification obligations of Article 14.

[27] Information available at: https://www.icann.org/resources/pages/delegation-2012-02-25-en

Member States have until 9 November, 2018 to identify operators for each sector and subsector. In order to support Member States throughout this process, the Cooperation Group is currently developing a guidance document with relevant information about the necessary steps and best practices related to the identification of OES.

Furthermore in accordance with Article 24(2), the Cooperation Group is to discuss the process, substance and type of national measures allowing for the identification of operators of essential services in specific sectors. A Member State may, prior to 9 November, 2018 seek to discuss its draft national measures allowing for the identification of operators of essential services at the Cooperation Group.

4.1.3. Inclusion of additional sectors.

Taking into account the minimum harmonisation requirement enshrined in Article 3, Member States can adopt or maintain legislation ensuring a higher level of security of network and information systems. In this regard Member States are in general free to expand the security and notification obligations under Article 14 to entities belonging to other sectors and sub-sectors than those listed in Annex II of the NIS Directive. Various Member States have decided or are currently considering whether to include some of the following additional sectors:

i) Public administrations

Public administrations may offer essential services in Directive's Annex II that meets the requirements of Article 5(2). In such cases, public administrations offering such services would be covered by the relevant security requirements and notification obligations. *A contrario*, when public administrations offer services that do not fall under the above scope, such services would not be covered by the relevant obligations.

Public administrations are responsible for the proper delivery of public services provided by governmental bodies, regional and local authorities, agencies and associated enterprises. These services often imply the creation and management of personal and corporate data about individuals and organisations, which can be shared and made available to multiple public entities. More broadly, a high level of security of network and information systems used by public administrations is an important interest for the society and economy as a whole. The Commission therefore takes the view that it would be sensible for Member States to consider inclusion of public administration in scope of the national legislation transposing the Directive, beyond the provision of essential services as set forth under Annex II and Article 5(2).

ii) Postal sector

The postal sector encompasses the provision of postal services such as the collecting, sorting, transport and distribution of postal items.

iii) Food sector

The food sector concerns the production of agricultural and other food products and it could include essential services such as the provision of food security and assurance of food quality and safety.

iv) Chemical and nuclear industry

The chemical and nuclear industry concerns in particular the storage, production and processing of chemical and petrochemical products or nuclear materials.

v) Environmental sector

Environmental activities encompass the provision of goods and services necessary to protect the environment and manage resources. Therefore activities are aimed at preventing, reducing and eliminating pollution and preserving the stock of available natural resources. Under this sector essential services could be the monitoring and control of pollution (e.g. of air and water) and meteorological phenomena.

vi) Civil protection

The objective of the civil protection sector is to prevent, prepare for and respond to natural and man-made disasters. The services provided for this purpose can be the activation of emergency numbers and the implementation of actions informing about, containing and responding to emergencies.

4.1.4. Jurisdiction.

Pursuant to Article 5(1), each Member State has to identify OES with an establishment on its territory. The provision does not specify further the type of the legal establishment but recital 21 clarifies that such establishment implies the effective and real exercise of activity through stable arrangements whereas the legal form of those arrangements should not be a determining factor. This means that a Member State can have jurisdiction over an operator of essential services not only in cases where the operator has its head office on its territory but also in cases where the operator has for example a branch or other type of legal establishment.

This has as a consequence that several Member States in parallel could have jurisdiction over the same entity.

4.1.5. Information to be submitted to the Commission.

For the purpose of the review that the Commission needs to carry out in accordance with Article 23(1) of the NIS Directive, Member States are required to submit to the Commission by 9 November, 2018 and every two years thereafter the following information:

- National measures allowing for the identification of OES;
- The list of essential services;
- The number of identified OES for each sector referred to in Annex II and the relevance of those operators for the sector; and

- Thresholds, where such exists, used to determine the supply level by reference to the number of users relying on that service as referred to in Article 6(1)(a) or the importance of the entity in accordance with Article 6(1)(f).

The review provided by article 23(1), which precedes the comprehensive review of the Directive reflects the importance that co-legislators attach to the correct transposition of the Directive in relation to the identification of operators of essential services to avoid market fragmentation.

In order to carry out this process in the best possible manner and the Commission encourages Member States to discuss this subject, as well as exchange relevant experience in the Cooperation Group. Furthermore, the Commission encourages Member States to share with the Commission - if necessary on a confidential basis - the lists of identified operators of essential services (which ultimately were selected) in addition to all the information that Member States are required by the Directive to provide to the Commission. Availability of such lists would facilitate and result in better quality of the Commission assessment of the consistency of identification process as well as would allow making comparison of approaches between the Member States, thus leading to a better achievement of the objectives of the Directive.

4.1.6. How to carry out the identification process?

As Figure 4 shows, there are six key questions that a national authority should examine when carrying out the identification process concerning a particular entity. In the following paragraph each question corresponds to a step to be undertaken in accordance with Article 5 in conjunction with Article 6, and also taking into account the applicability of Article 1(7).

Step 1 – **Does the entity belong to a sector/subsector & correspond to the type covered by Annex II of the Directive?**

A national authority should assess whether an entity established in its territory belongs to the sectors and subsectors listed in Annex II of the Directive. Annex II covers various economic sectors that are considered instrumental to ensure the proper functioning of the internal market. In particular, Annex II refers to the following sectors and subsectors:

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare providers (including hospitals and private clinics)
- Water: drinking water supply and distribution

- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries[28]

Step 2 – **Is a *lex specialis* applicable?**

As a next step, the national authority needs to assess whether the provision of *lex specialis* enshrined in Article 1(7) applies. In particular, the provision states that if there is an EU legal act imposing security and/or notifications requirements to digital service providers or operators of essential services which are at least equivalent to the corresponding requirements under the NIS Directive, the obligations under the special legal act should apply. Furthermore, recital 9 clarifies that if the requirements of Article 1(7) are fulfilled, Member States should apply the provisions of the EU sector-specific act including those relating to jurisdiction. A *contrario*, the relevant provisions of the NIS Directive would not apply. In this case, the competent authority should not continue with the identification process under Article 5(2).[29]

Step 3 – **Is the operator providing an essential service within the meaning of the Directive?**

Pursuant to Article 5(2)(a), the entity which is subject to the identification needs to provide a service which is essential for the maintenance of the critical societal and/or economic activities. When carrying out this assessment, Member States should take into account that one entity can provide both essential and non-essential services. This means that the security and notification requirements of the NIS Directive will apply to a certain operator only to the extent to which it provides essential services.

In accordance with Article 5(3), a Member State should compile a list of all essential services provided by OES within its territory. This list will need to be submitted to the Commission by 9 November 2018 and every two years thereafter.[30]

Step 4 - **Does the service depend on a network and information system?**

Furthermore, it should be clarified whether this service meets the second criterion of Article 5(2)(b) and in particular whether the provision of the essential service depends on network and information systems as defined in Article 4(1).

Step 5 – **Would a security incident have a significant disruptive effect?**

Article 5(2)(c) requires the national authority to assess whether an incident would have a significant disruptive effect on the provision of the service. In this context Article 6(1) lays down several cross-sectorial factors that need to be taken into account in the assessment. Furthermore, Article 6(2) rules that if appropriate, the assessment should consider also sector-specific factors.

[28]These entities are further explained in Section 4.1.1.

[29] More details on the applicability of *lex specialis* are provided in section 5.1

[30] See Article 5(7)(b)

The **cross-sectoral factors** listed in Article 6(1) are the following:

- The number of users relying on the service provided by the entity concerned;
- The dependency of other sectors referred to in Annex II on the service provided by that entity;
- The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
- The market share of that entity;
- The geographic spread with regard to the area that could be affected by an incident;
- The importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

With regard to the **sector-specific factors**, recital 28 provides some examples (see Table 4) which could provide helpful guidance to national authorities.

Table 4: Examples of sector-specific factors to be considered when determining significant disruptive effect in case of incident.

Sector	Examples of sector specific-factors
Energy suppliers	volume or proportion of national power generated
Oil suppliers	volume of oil supplied per day
Air transport (including airports and air carriers) **Rail transport** **Maritime ports**	proportion of national traffic volume; number of passengers or cargo operations per year.
Banking or financial market infrastructures	systemic importance based on total assets; ratio of total assets to GDP
Health sector	number of patients under the provider's care per year
Water production, processing and supply	volume and number and types of users supplied (including, for example, hospitals, public service organisations, or individuals); existence of alternative sources of water to cover the same geographical area

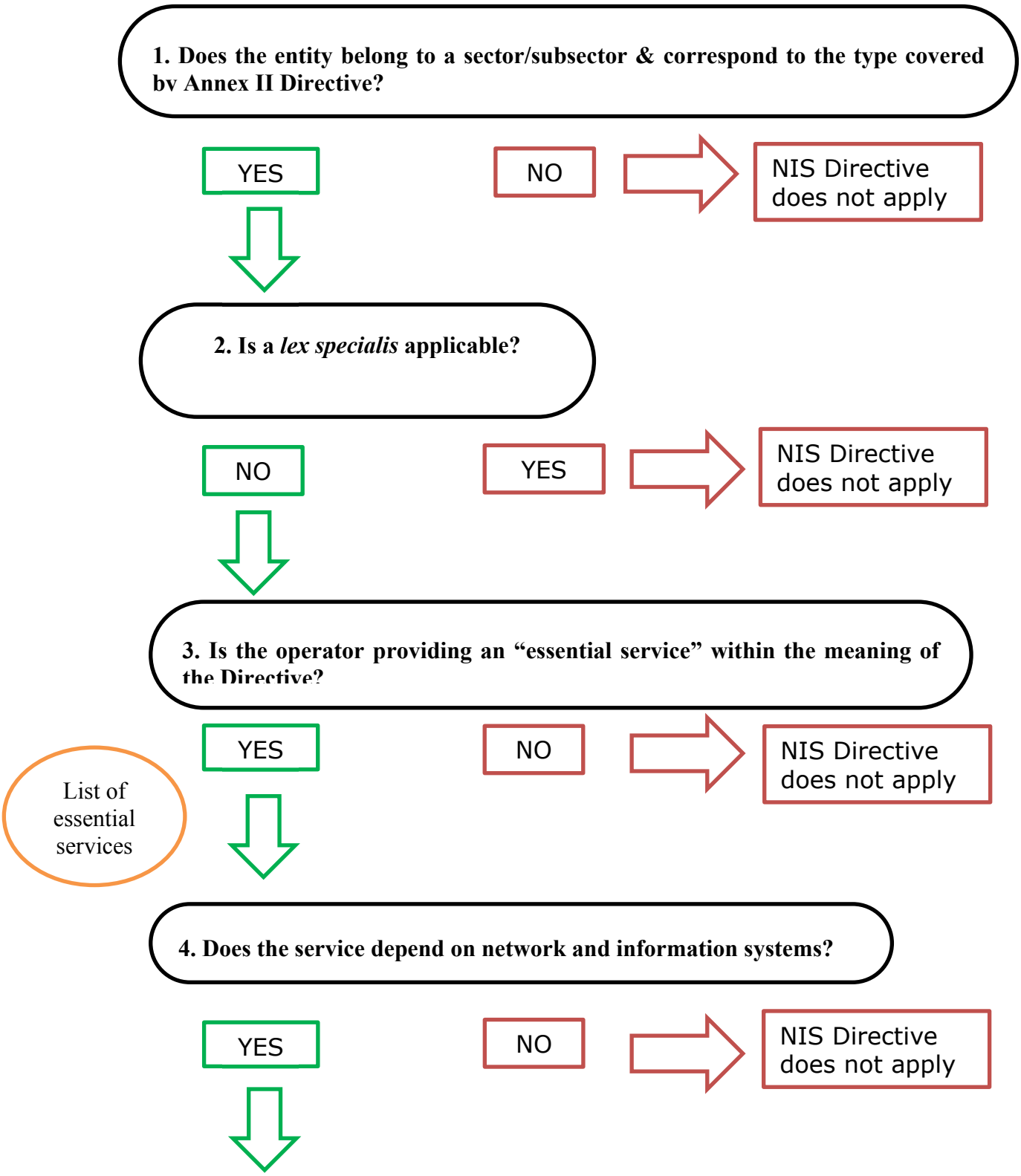
It should be outlined that when carrying out the assessment pursuant to Article 5(2), Member States should not add additional criteria than those listed in that provision because this could narrow the number of identified OES and jeopardise the minimum harmonisation for OES enshrined in Article 3 of the Directive.

Step 6 **- Is the operator concerned providing essential services in other Member States?**

Step 6 refers to cases where an operator provides its essential services in two or more Member States. Before the completion of the identification process, Article 5(4) requires the concerned Member States to engage in a consultation process.[31]

[31] For more details on the consultation process see section 4.1.7.

Figure 4: Identification process in 6 steps.



5. Would a security incident have a significant disruptive effect?

Cross-sectoral factors (Article 6(1))

- **Number of users** relying on the services
- **Dependency** of other essential sectors on the service
- Impact that incidents could have on **economy and societal activities** or **public safety**
- Possible **geographic spread**
- Importance of the entity for maintaining a sufficient **level of the service**

Sector-specific factors (examples mentioned in recital 28)

- **Energy**: volume or proportion of national power generated
- **Transport**: proportion of national traffic volume & number of operations per year
- **Health**: number of patients under the provider's care per year

YES

NO → NIS Directive does not apply

6. Is the operator concerned providing essential services in other Member States?

YES

NO → NIS Directive does not apply

Mandatory consultation with the MS(s) concerned

Adoption of national measures (e.g. list of operators of essential services, policy and legal measures).

4.1.7. Cross-border consultation process.

Where an operator provides essential services in two or more Member States, Article 5(4) requires that those Member States engage in consultation with each other before the completion of the identification process. The purpose of this consultation is to facilitate the assessment on the critical nature of the operator in terms of cross-border impact.

The desired outcome of the consultation is that the involved national authorities exchange arguments and positions and ideally come to the same result concerning the identification of the operator concerned. However, the NIS Directive does not preclude Member States reaching divergent conclusions whether a particular entity is identified as OES or not. Recital 24 mentions the possibility for Member States to request the assistance of the Cooperation Group in that matter.

In the Commission's view, Member States should strive to reach a consensus on these issues to avoid a situation that the same company is facing different legal status in various Member States. Divergence should be truly exceptional e.g. when an entity determined as OES in one Member State has a marginal and insignificant activity in another one.

4.2. Security requirements.

Pursuant to Article 14(1), Member States are required to ensure that OES, having regard to the state of art, take appropriate and proportionate technical and organisational measures to manage the risk posed to the security of network and information systems which the organisations use in the provision of their services. In accordance with Article 14(2), appropriate measures shall prevent and minimise the impact of an incident.

A dedicated work stream of the Cooperation Group is currently working on non-binding guidelines concerning the security measures for OES[32]. The guidance document is to be finalised by the Group by Q4 of 2017. The Commission encourages Member States to follow closely the guidance document to be developed by the Cooperation Group so that national provisions on security requirements would be aligned to the extent possible. Harmonisation of such requirements would greatly facilitate compliance by OES which often provide essential services in more than one Member State and the supervision tasks of national competent authorities and CSIRTs.

4.3 Notification requirements.

Pursuant to Article 14(3), Member States have to ensure that OES notify "*any incident having a significant impact on the continuity of the essential services"*. Consequently, the OESs

[32] For the purpose of this work stream, lists of international standards, good practices and risk assessment/management methodologies for all sectors covered by the NIS Directive were circulated and were used as input for the proposed security domains and security measures

should not notify any minor incidents but only serious incidents affecting the continuity of the essential service. As an incident, Article 4(7) defines "*any event having an actual adverse effect on the security of network and information systems"*. The term 'security of network and information systems' is further defined under Article 4(2) as "*the ability of network to resists, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."* Consequently, any event having an adverse effect not only on the availability but also on authenticity, integrity or confidentiality of data or related services could potentially be able to trigger the notification obligation. In fact, the continuity of the service as referred to in Article 14(3) can be compromised not only in cases where the physical availability is concerned, but also by any other security incident affecting the proper provision of the service[33].

A dedicated work stream within the Cooperation Group is currently preparing non-binding notification guidelines concerning the circumstances in which operators of essential services are required to notify incidents pursuant to Article 14(7) and the format and procedure of national notifications. The guidelines are intended to be finalised by Q4 of 2017.

Different national notification requirements may lead to legal uncertainty, more complex and cumbersome procedures and significant administrative costs for providers operating cross-border. The Commission therefore welcomes the work of the Cooperation Group. As is the case for security requirements, the Commission encourages Member States to follow closely the guidance document to be developed by the Cooperation Group so that that national provision on notification of incidents would be aligned to the extent possible.

4.4. NIS Directive, Annex III: Digital Service Providers.

The Digital Service Providers (DSPs) are the second category of entities included in the scope of the NIS Directive. These entities are considered to be important economic players due to the fact that they are used by many businesses for the provision of their own services, and a disruption of the digital service could have an impact on the key economic and societal activities.

4.4.1. Categories of DSPs.

Article 4(5) which defines digital service refers to the legal definition of point (b) of Article 1(1) of Directive (EU) 2015/1535 by narrowing the scope to the types of services listed in Annex III. In particular, Article 1(1) point (b) of Directive (EU) 2015/1535 defines these services as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" and Annex III of the Directive lists three specific types of services: online market place, online search engine and cloud computing service. In comparison to the operators of essential services, the Directive does not require Member States to identify the digital service providers, which would then be subject

[33] The same applies to DSPs.

to the relevant obligations. Therefore, the relevant obligations of the Directive, namely the security and notifications requirements set out in Article 16 will apply to all DSPs within its scope.

The following sections provide additional explanations concerning three types of digital services included in the scope of the Directive.

1. Online market place provider.

The online market place enables a large number and variety of businesses to perform their trade activities vis-à-vis the consumers and to engage in business-to-business relations. It provides companies with the basic infrastructure to trade online and across borders. They play a significant role in the economy notably by providing SMEs access to the wider EU digital single market. The provision of remote computing services facilitating its client's economic activity, including the processing of transactions and aggregation of information on buyers, suppliers and products can also belong to the activities of an online market place provider, as well as the facilitation of search for appropriate products, the provision of products, transactional expertise and matching buyers and sellers.

The term online market place is defined in Article 4(17) and further clarified in recital 15. It is described as a service that enables consumers and traders to conclude online sales or service contracts with traders, and it represents the final destination for the conclusion of those contracts. For example, a provider such as *E-bay* can be regarded as an online market place as it allow others to set up shops on its platform in order to make their products and services available online to consumers or businesses. Also, online application stores for distributions of applications and software programmes are considered as falling under the definition of online market place because they allow app developers to sell or distribute their services to consumers or other businesses. In contrast, intermediaries to third-parties services such as *Skyscanner* and price comparison services, which redirect the user to the website of the trader where the actual contract for the service or the product is concluded, are not covered by the definition of Article 4(17).

2. Online search engine provider.

The online search engine is defined in Article 4(18) and further clarified in recital 16. It is described as a digital service that allows users to carry out searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject. Search functionalities limited to in-site search and price comparison websites are not covered. For example the type of a search engine such the one provided by EUR LEX[34] cannot be regarded as a search engine within the meaning of the Directive as its search function is limited to the content of that concrete website.

[34] Available at: http://eur-lex.europa.eu/homepage.html

3. Cloud computing service provider.

Article 4(19) defines cloud computing service as "a digital service that enables access to a scalable and elastic pool of shareable computing services" and recital 17 gives further clarifications on the terms computing resources, scalable and elastic pool.

In a nutshell, cloud computing can be described as a particular type of computing service that uses shared resources in order to process data on-demand whereby shared resources refers to any kind of hardware or software components (e.g. networks, servers or other infrastructure, storage, applications and services) that are released on-demand to users for processing data. The term sharable defines computing resources where many users are utilizing the same physical infrastructure for processing data. The computing resource can be defined as sharable if the pool of resources used by the provider can be extended or reduced at any time, depending on the user requirements. Thus, data centres or single components within one data centre could possibly be added or removed if the total amount of computing or storage capacity needs an update. The term elastic pool can be described as workload changes by provisioning and de-provisioning resources in an automatic manner, such that at each point in time the available resources match the current demand as closely as possible"[35].

There are at present three main types of cloud service models which a provider can offer:

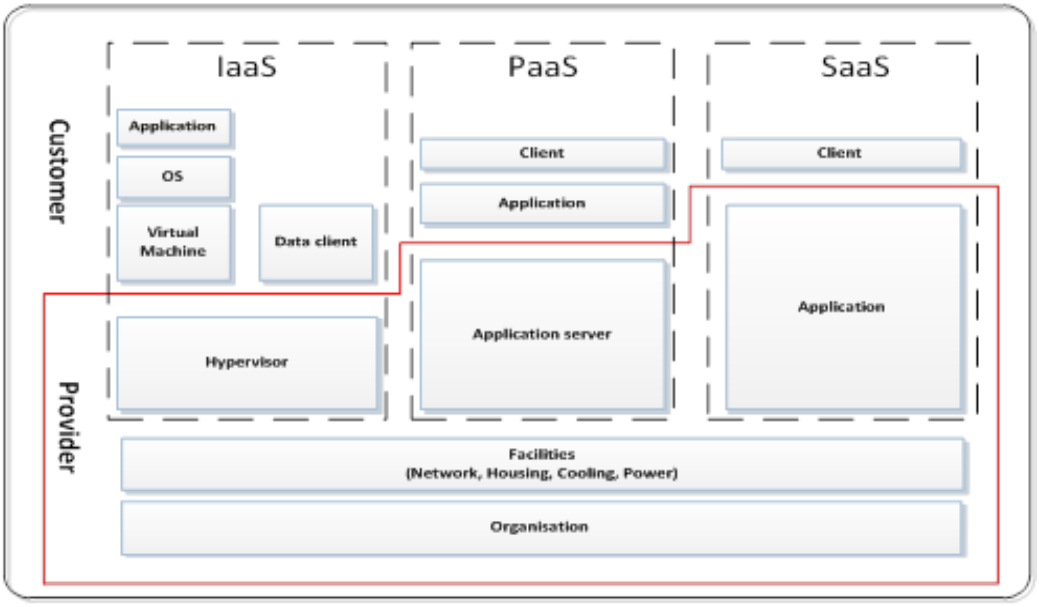
- Infrastructure as a Service (IaaS): A cloud service category in which the cloud capabilities type provided to the customer is an infrastructure. It includes the virtual delivery of computing resources in the form of hardware, networking and storage services. IaaS powers servers, storage, networks and operating systems. It provides enterprise infrastructure in which a business can store its data and run the applications needed for its daily operation.

- Platform as a Service (PaaS): A cloud service category in which the cloud capabilities type provided to the customer is a platform. It includes online computing platforms that allow companies to run existing applications or to develop and test new ones.

- Software as a service (SaaS): A cloud service category in which the cloud capabilities type provided to the customer is an application or software deployed over the Internet. This type of cloud services removes the need for the end user to buy, install and manage software, and has the advantage of making the software accessible from anywhere with an internet connection.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, "Elasticity in Cloud Computing: What It Is, and What It Is Not", available at: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. See also pages 2-5 of COM(2012) 529.

Figure 5: Service models and assets in cloud computing



Comprehensive guidelines on specific topics within the cloud area[36]and a guidance document on the basics of cloud computing[37] have been provided by ENISA.

4.4.2. Security requirements.

Pursuant to Article 16(1) Member States are required to ensure that DSPs take appropriate and proportionate technical and organisational measures to manage the risk posed to the security of network and information systems which the companies use in the provision of their services. Those security measures should take into account the state of the art and the following five elements: i) security of systems and facilities; ii) incident handling; iii) business continuity management; iv) monitoring, auditing and testing; v) compliance with international standards.

In this regard the Commission is empowered pursuant to Article 16(8) to adopt implementing acts specifying further those elements and ensuring a high level of harmonisation for these service providers. The implementing act is expected to be adopted by the Commission in autumn 2017. Furthermore, Member States are required to ensure that digital service providers take the necessary measures to prevent and minimise the impact of incidents with a view to ensuring the continuity of the their services.

4.4.3. Notification requirements.

DSPs should be required to notify serious incidents to the competent authorities or the CSIRTs. In accordance with Article 16(3) of the NIS Directive, the notification requirement

[36] Available at: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Available at: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

for digital service providers will be triggered in cases where the security incident has a substantial impact on the provision of the service. For determination of the impact, Article 16(4) lists in particular five parameters that need to be taken into account by the digital service providers. In this regard the Commission is empowered pursuant to Article 16(8) to adopt implementing acts providing more detailed descriptions of the parameters. The further specification of those parameters will be part of the implementing act specifying the security elements mentioned in point 2.2.4 which the Commission intends to adopt in the autumn.

4.4.4. Risk-based regulatory approach.

As outlined above, Article 17 stipulates that DSPs are subject to *ex post* supervisory control by the national competent authorities. Member States must ensure that competent authorities take action, when provided with evidence that a DSP is not complying with the requirements of Article 16 of the Directive.

Furthermore, pursuant to Article 16(8) and (9), the Commission is empowered to adopt implementing acts with respect to the notification and security requirements which will enhance the level for harmonisation for DSPs. Moreover, pursuant to Article 16(10) Member States are not allowed to impose any further security and notification requirements on DSPs than those provided in the Directive except for cases where such measures are necessary to safeguard their essential State functions, in particular to safeguard national security, and to allow for the investigation, detection and prosecution of criminal offences.

And finally, taking into account the cross-border nature of DSPs, the Directive does not follow the model of multiple parallel jurisdictions but an approach based on the criterion of main establishment of the company within the EU.[38] This approach allows for a single set of rules to be applied to DSPs with one competent authority responsible for supervision which is particularly important as many DSPs offer their services across in many Member States simultaneously. The application of this approach minimises the compliance burden on DSPs and ensures the proper functioning of the Digital Single Market.

4.4.5. Jurisdiction.

As explained above, pursuant to Article 18(1) of the NIS Directive, the Member State where the DSP has its main establishment has jurisdiction over the company. In cases where the concrete DSP offers services in the EU but is not established in the EU territory, Article 18(2) imposes on the DSP the obligation to designate a representative in the Union. In that case, the Member State where the representative is established will have jurisdiction over the company. In cases where a DSP provides services in a Member State but has not designated a representative in the EU, the Member State can in principle take actions against the DSP as the provider is infringing its obligations deriving from the Directive.

[38] See in particular Article 17 of the Directive.

4.4.6. Exemption of Limited Scale digital service providers from the scope of the security requirements and notification.

Pursuant to Article 16(11), digital service providers which are micro or small enterprises within the meaning of Commission Recommendation 2003/361/EC39 are excluded from the scope of the security requirements and notification set forth under Article 16. This means those businesses that employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million, are not bound by such requirement. When determining the size of the entity, it is not of relevance whether the concerned company provides only digital services within the meaning of the NIS Directive or also other services.

5. The relationship between the NIS Directive and other legislation.

This section focuses on the provisions on *lex specialis* enshrined in NIS Directive, Article 1(7), illustrating the three examples of *lex specialis* assessed by the Commission so far, and clarifying the security and notification requirements applied to telecommunications and trust service providers.

5.1. NIS Directive, Article 1(7): The provision of *lex specialis.*

Pursuant to Article 1(7) of the NIS Directive, the provisions on security and/or notification requirements for digital service providers or operators of essential services under the Directive are not applicable if an EU sector-specific legislation provides for security and/or notification requirements, which are at least equivalent in effect to the corresponding obligations of the NIS Directive. Member States need to consider Article 1(7) in the overall transposition of the Directive and provide information to the Commission on the application of *lex specialis* provisions.

Methodology.

When assessing the equivalence of a piece of EU sector-specific legislation with the relevant provisions of the NIS Directive, particular importance should be given to the question whether the security obligations in the sector-specific legislation comprise measures ensuring the security of network and information systems as defined in Article 4(2) of the Directive.

As far as notification requirements are concerned, Article 14(3) and 16(3) of the NIS Directive stipulate that operators of essential services and digital service providers need to notify without undue delay to the competent authorities or to the CSIRT any incident having a significant/substantial impact on the provision of the service. Here special attention needs to be paid to the obligations of the operator/digital service provider to include in the notification information enabling the competent authority or the CSIRT to determine any cross-border impact of a security incident.

[39] OJ L 24, 20.5.2003, p. 36

Currently there is no sector-specific legislation for the category of the digital service providers that provides for security and notification requirements comparable to those laid down in Article 16 of the NIS Directive that can be considered in the application of Article 1(7) of the NIS Directive[40].

As far as the operators of essential services are concerned, the financial sector and notably the sectors banking and financial market infrastructure as referred to in point 3 and 4 of Annex II are currently subject to security and/or notification requirements stemming from EU sector-specific legislation. This is due to the fact that security and soundness of IT and network and information systems used by financial institutions is an essential part of the operational risk requirements imposed on financial institutions by virtue of EU legislation.

Examples.

i) Payment Service Directive 2.

With regard to the banking sector and in particular as far as the provision of payment services by credit institutions as defined in point (1) of Article 4 of Regulation (EU) 575/2013 is concerned, the so-called Payment Services Directive 2 (PSD 2)[41] foresees security and notification requirements which are set out in Article 95 and 96 of that Directive.

More precisely, Article 95(1) requires payment service providers to adopt appropriate mitigation measures and control mechanisms that will allow the management of the operational and security risks relating to the payment services they provide. These measures should contain the establishment and the maintenance of effective incident management procedures, including procedures for the detection and classification of major operational and security incidents. Recital 95 and 96 of the PSD 2 clarifies further the nature of such security measures. From these provisions it is apparent that the prescribed measures aim at managing the security risks related to the network and information systems which are used in the provision of payment services. Therefore those security requirements can be regarded as at least equivalent in effect to the corresponding provision of Article 14(1) and (2) of the NIS Directive.

Concerning the notification requirements, Article 96(1) of the PSD 2 foresees an obligation for the payment service providers to report, without undue delay, serious security incidents to the competent authority. Furthermore, comparable to Article 14(5) NIS Directive, Article 96 (2) of the PSD 2 requires the competent authority to inform the competent authorities of other Member States if an incident is relevant for them. This obligation implies at the same time that the reporting of security incidents has to include information allowing the authorities to assess the cross-border impact of an incident. Article 96(3) (a) of the PSD 2 empowers in this

[40] This is without prejudice to the Notification of a personal data breach to the supervisory authority covered by Article 33 of the GDPR.
[41] Directive (EU) 2015/2366, OJ L 337, 23.12.2015, p.35

respect the EBA in cooperation with the ECB to develop guidelines on the exact content and the format of the notification.

Consequently, it can be concluded that pursuant to Article 1(7) NIS Directive, both security and notification requirements set out in Article 95 and 96 of the PSD 2 should apply instead of the corresponding provisions of Article 14 of the NIS Directive as far as the provision of payment services by credit institutions is concerned.

ii) Regulation (EU) 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

With regard to the financial market infrastructure, Regulation (EU) 648/2012 in conjunction with Commission Delegated Regulation (EU) 153/2013 contains provisions on security requirements for central counterparties (CCP) which can be regarded as *lex specialis*. In particular, the legal acts provide for technical and organisation measures related to the security of network and information systems which in terms of detail go even beyond the requirements of Article 14(1) and (2) of the NIS Directive and therefore can be regarded as fulfilling the requirements of Article 1(7) of the NIS Directive as far as the security requirements are concerned.

More precisely, Article 26(1) of Regulation (EU) 648/2012 states that the entity should have "*robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures."* Article 26(2) requires that the organisational structure has to ensure continuity and the proper functioning of the services and activities by using appropriate and proportionate systems, resources and procedures.

Furthermore Article 26(6) clarifies that a CCP needs to maintain "*information technology systems adequate to deal with the complexity, variety and type of services and activities performed so as to ensure high standards of security and the integrity and confidentiality of the information maintained".* Furthermore, Article 34(1) imposes the establishment, implementation and maintenance of an adequate business continuity policy and disaster recovery plan that should ensure the timely recovery of the operations.

These obligations are further specified in Commission Delegated Regulation EU/153/2013 of 19 December 2012 supplementing supplementing Regulation EU/648/2012 of the European Parliament and of the Council with regard to regulatory technical standards and requirements for central counterparties[42]. In particular Article 4 thereof imposes on CCP the obligation to develop appropriate risks management tools that would enable the managing and reporting on all relevant risks and specify further the type of measures (e.g.: employment of robust information and risk-control systems, the availability of resources, expertise and access to all relevant information for the risk management function, availability of adequate internal

[42] OJ L 52, 23.2.2013, p. 41

control mechanisms such as sound administrative and accounting procedures to assist the board of CCP in monitoring and accessing the adequacy and effectiveness of its risk management policies, procedure and systems).

In addition, Article 9 refers explicitly to the security of information technology systems and imposes concrete technical and organisational measures related to the maintenance of a robust information security framework for management of the IT security risks. Such measures should include mechanisms and procedures ensuring the availability of the services and the protection of the authenticity, integrity and confidentiality of data.

(iii) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.[43]

With regard to trading venues, Article 48(1) of Directive 2014/65/EU requires the operators to ensure continuity of its services in the event of any failure of its trading system. This general obligation has been recently further specified and complemented by Commission Delegated Regulation (EU) 2017/584[44] of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues[45]. In particular Article 23(1) of this Regulation stipulates that trading venues shall have in place procedures and arrangements for physical and electronic security designed to protect their systems from misuse or unauthorised access and ensure the integrity of data. These measures should allow for prevention or minimisation of the risk of attacks against information systems.

Article 23(2) requires further that the measures and the arrangements taken by the operators should allow for prompt identification and management of the risk related to any unauthorised access, system interferences hindering seriously or interrupting the functioning of information systems and data interferences that compromise the availability, integrity or the authenticity of data. Moreover, Article 15 of the Regulation imposes the obligation for trading venues to have in place effective business continuity arrangements to ensure sufficient stability of the system and address disruptive incidents. In particular, these measures should enable the operator to resume trading within or close to two hours and at the same time ensure that the amount of lost data is close to zero.

Article 16 states further that identified measures for addressing and managing disruptive incidents should be part of the business continuity plan of the trading venues and provides for particular elements that need to be considered by the operator when adopting the business continuity plan (e.g. establishment of a specific security operations team, carrying out of an impact assessment identifying the risks that is periodically reviewed).

[43] OJ L 173, 12.6.2014, p. 349
[44] OJ L 87, 31.3.2017, p. 350
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

In view of the content of these security measures, it appears that they are intended to manage and address the risk related to the availability, authenticity, integrity and confidentiality of data or provided services and as a result it can be concluded that the above mentioned EU sector-specific legislation contains security obligations that are in effect at least equivalent to the corresponding obligations of Article 14(1) and (2) of the NIS Directive.

5.2 NIS Directive, Article 1(3): Telecom providers and trust service providers.

Pursuant to Article 1(3) the security and notification requirements provided for in the Directive do not apply to providers which are subject to the requirements of Article 13a and 13b of Directive 2002/21/EC. Article 13a and 13b of Directive 2002/21/EC apply to undertakings providing public communications networks or publicly available electronic communications services. Consequently, as far as the provision of public communications networks or publicly available electronic communications services is concerned, the company has to comply with the security and notification requirements of Directive 2002/21/EC.

However, if the same company is providing also other services such as digital services (e.g. cloud computing or online market place) listed in Annex III of the NIS Directive or services such as the DNS or IXP pursuant to Annex II point 7 of the NIS Directive, the company will be subject to the security and notification requirements of the NIS Directive for the provision of these particular services. It should be noted that due to the fact that the providers of services listed in Annex II point 7 belong to the category of the operator of essential services, Member States are required to carry out an identification process pursuant to Article 5(2) and identify which individual providers of DNS, IXP or TLD services should comply with the requirements of the NIS Directive. This means that following such assessment, only those DNS, IXP or TLD providers that fulfil the criteria of Article 5(2) of the NIS Directive will be under the obligation to comply with the requirements of the NIS Directive.

Article 1(3) further specifies that the security and notification requirements of the Directive also do not apply to trust service providers which are subject to similar requirements under Article 19 of Regulation (EU) No 919/2014.

6. Published National Cyber-Security Strategy Documents.

	Member State	Title of the strategy and available links
1	Austria	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgium	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgaria	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Croatia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Czech Republic	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cyprus	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Denmark	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonia	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finland	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	France	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-

		strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Ireland	*National Cyber Security Strategy 2015-2017* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italy	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Germany	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Hungary	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Latvia	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lithuania	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxembourg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Netherlands	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Poland	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Romania	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)

22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slovak Republic	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spain	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Sweden	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	United Kingdom	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. List of good practices and recommendations issues by ENISA.

For Incident response

- ✓ Strategies for incident response and cyber crisis cooperation[46]

For incident handling

- ✓ Incident handling automation project[47]
- ✓ Good Practice Guide for Incident Management[48]

For incident classification and taxonomy

- ✓ Overview of existing taxonomies[49]
- ✓ Good practice guide of using taxonomies in incident prevention and detection[50]

For CSIRT maturity

- ✓ Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity[51]
- ✓ Study on CSIRT Maturity – Evaluation Process[52]
- ✓ Guidelines for national and governmental CSIRTs on how to assess maturity[53]

For CSIRT capacity building and training

- ✓ Good Practice Guide on Training Methodologies[54]

To find information about existing CSIRTs in Europe - Overview of CSIRTs by Country[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Available at:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] More information at: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Available at:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] More information at: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Available at:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Available at:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Available at:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Available at: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Available at:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] More information at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map