Sectorial implementation of the NIS Directive in the Energy sector

Report -
CG Publication 03/2019

Oct 2019

NIS COOPERATION GROUP

Contents

1 Introduction

The energy infrastructure is arguably one of the most complex and, at the same time, critical infrastructures that other business sectors depend upon to deliver essential services. Because of this dependency, a potential disruption for a long period can trigger a cascade of effects in other sectors of society.

In this light, the objective of this document is to collect information from the Member States on energy sector specific NIS Directive requirements. This will allow for a more consistent approach to energy cybersecurity at EU level as well as the identification of cascading effects, which might have a serious impact on many business sectors of society and even in other Member States´ economy.

This document is an output of Work Stream 8 led by experts from Austria, supported by experts from ENISA and involving the European Commission. It presents an overview of the status of implementation of Article 5 for the energy sector, analyses key findings, challenges and sectorial specificities. The document provides good practices and examples of implementation of the main NIS Directive requirements – identification criteria, security measures and incident reporting requirements specific for the energy sector.

The information collected for this document is a result of a survey[1] developed by ENISA, Austria and the European Commission. The members of the Cooperation Group have been invited to participate in this survey. Overall, fifteen Member States responded and provided valuable feedback.

[1] The survey is enclosed in Annex V.

2 Sectorial specificities

The energy infrastructure is inarguably one of the most complex and most critical infrastructures of a modern society and serves as the backbone for its economic activities and for its security. Given that the energy sector delivers crucial inputs to other sectors, there are important implications also for other parts of the economy. It is, therefore, indispensable to look at the particularities of the energy sector in order to assess its overall impact for economy and society at large also with regard to cybersecurity.

The main particularities of the energy sector are:

- **Cascading effects:** Electricity grids and gas pipelines are strongly interconnected across Europe and well beyond EU MS. Energy reliability at the European level relies on trans-European connectivity. Unlike other IT systems, control systems in the energy sector under attack cannot be easily shut down as an outage might trigger cascading effects into other different inter-dependent energy systems, sectors or other regions going way beyond the energy sector or else the region concerned.

- **Legacy systems:** The energy sector is composed of basic infrastructure such as transformers and generators on one hand, which were designed at a time well before cyber security considerations, and of more recent equipment used for automation and control strongly supported by more and more ICT. There is, therefore, a particular problem that a significant part of the energy infrastructure with a relatively long life span has been designed without due consideration of cyber-attacks and the increasing variety of other threats.

- **Real-time requirements:** A number of standard cyber security measures may be difficult to apply with a view to the real-time requirements of the energy sector where facilities cannot easily be shut off as the costs associated with such shut off would be seen as prohibitive.

According to the results of the survey, some of the sectorial specificities mentioned by the MS are:

- Interconnection of the grid systems: The interconnection of the grid systems plays a key role in all the subsectors of the energy sector. It is difficult though to assess the cross-border dependencies in detail.

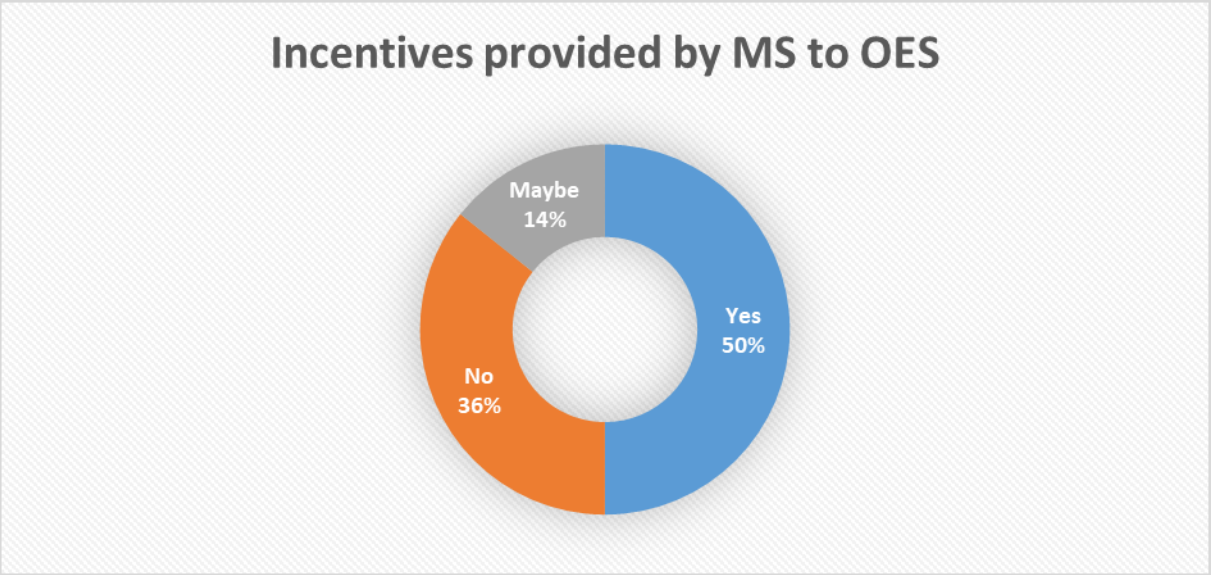
- Specificities of sub-sectors: In the sub sector oil it was challenging to assess the essentiality of the services for the society and economy since oil is different from the petroleum products, which are ultimately the energy source used by society and economy. An incident will not have such an immediate adverse effect compared to other (sub-)sectors in terms of supply.

- Ownership of the infrastructure: In thermal plants – different owners of the infrastructure have no exact overview of how much thermal energy is currently in the part of infrastructure owned by them. Sometimes, the plant operates in many sub-sectors making the ownership issue even more complex.

2.1 Incentives

Overall, from the fifteen participants, fifty percent answered that the Member State provides incentives to the private sector to enhance cyber security; thirty-six percent replied that the Member State do not provide any incentives at all, while fourteen percent replied that the Member State provides some short of incentives.

Figure 1 - Incentives by MS to OES



For example, Austria has already established a sector CSIRT (Austrian Energy CERT – AEC). The NIS Law provides the possibility to recognize the AEC as CSIRT in accordance with the NIS Directive allowing it to participate in the Operational Coordination Structure and the CSIRTs Network.

The NIS Law provides the possibility to establish sector-specific security requirements that can be formally acknowledged by the Federal Minister for the Interior. It is expected that these sector-specific security requirements will trigger a triple-down effect on energy undertakings not within the scope of the NIS Law as energy undertakings that will not be identified as Operators of essential services (OES) are involved in the work as well.

Another example is the Czech Republic, where the state provides workshops, exercises, methodology and supporting materials.

In Denmark, Electricity distribution system operators (DSO's) can incorporate some of their expenses to Cybersecurity in their revenue cap, which means that cyber security investments doesn't subtract from their economic surplus.

In Estonia, the state provides trainings, penetration testing, facilitate information sharing, etc. In Finland, there are no financial incentives to enhance cyber security of the Energy OESs. However, National Cyber Security Center and National Emergency Supply Agency have

technical support programs to enhance cyber security of the Energy sectors OES.

In France, OES have to be compliant with a dedicated security rules ordinance (Prime Minister Order of 14 September 2018), which describes the 23 rules they have to apply to their network and information systems which essential services are relying on. The Prime Minister can trigger a control on OES.

Fines applying in case of breach of the regulation are stipulated by law; they may be imposed on both companies and their directors. Moreover, ANSSI supports the OES with several services (publication of guidelines, audit, architecture support, technical services, etc.) to help them to improve their cybersecurity. OES receive also regular threat reports and information on vulnerabilities from the CERT-FR and ANSSI.

In Luxembourg, no direct financial or fiscal incentives are currently planned. In order to support and guide private companies in their journey of digitalization, Luxembourg has setup a comprehensive ecosystem with free or low-cost offerings. Such offerings are regular trainings, conferences, sensibilisation sessions, tools for risk assessment and management, public CERTs, Cyber Security Competence Center (C3), etc. In the NIS context, OES will benefit from a free, sector specific customised risk assessment and management tool with integrated reporting to the competent authority and later on from a centralised, one-stop notification platform for NIS, Telecom, GDPR and Critical Infrastructures. No fees will be recovered from OES.

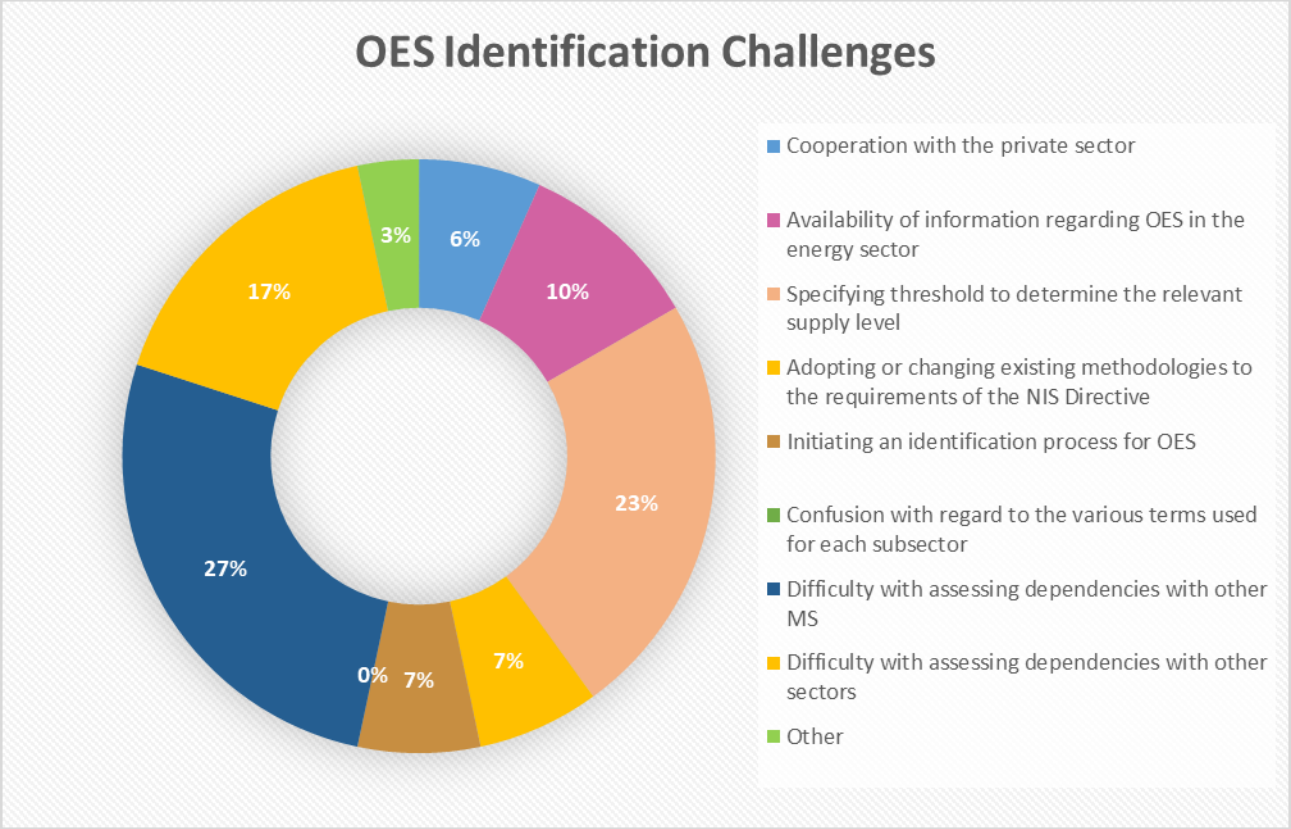
In Poland, a private-public partnership is about to start under the auspices of the Minister of Energy in order to stimulate and enhance their cyber security.

In Portugal, incentives include training, awareness and maturity models for the assessment of the measures and procedures implemented done with the support of the Portuguese National Cybersecurity Centre.

2.2 Challenges

The most common challenges reported by the MS regarding the OES Identification process are depicted in the graph below.

Figure 2 - OES Identification Challenges



Other important challenges reported by the MS:

- Missing availability of information regarding OES in the energy sector
- Lack of resources
- In the case of an operator driven approach, operators might not register as OES, even though they are.
- Energy sector is complex due to its sub-sectors including electricity, gas and oil. These sub-sectors contain different aspects and therefore all the characteristics must be taken into account.
- The process to identify OES requires appropriate but also resource demanding consultations.

2.3 Lessons Learnt from National Activities

Austria: Private-Public Dialogue Risk Management Process

In 2013, a Private-Public Dialogue (PPD) process was initiated with the aim of establishing a security standard in the industry for risks arising from the use of ICT. The PPD is based on the normative requirements of Risk Management according to ISO 31.000 and ONR 49.002-1-2 (PPD-RM process). The PPD process for controlling ICT risks in the energy industry

regulates the voluntary cooperation of all market participants active in Austria in the sense of the E-Control (Regulatory Authority for electricity and gas) market rules in the identification, evaluation and minimization of potential ICT risks for or in the energy industry. Through clearly defined responsibilities and a process framework for cooperation, hazards and risks are to be proactively communicated, managed and minimised. The risk management approach described provides the basis for implementing coordinated and economically justifiable ICT safety standards in the energy industry.

The PPD process therefore describes the interfaces between the legally regulated measures for implementing security of supply, the provisions of the NIS Directive, the requirements of the Austrian Programme for Critical Infrastructure Protection and coordinated industry standards from the perspective of ICT threats to the energy industry. The PPD-RM process is basically a voluntary commitment by companies and applies to the interaction between the NIS competent authorities and the OES in the electricity and gas sector in Austria. For the purpose of the PPD-RM process, a working committee was established consisting of representatives of the Federal Chancellery, the Federal Ministry for the Interior, the Federal Ministry of Defence and the Federal Ministry for Sustainability and Tourism, the E-Control as well as representatives of the electricity and gas industries. The committee has been expanded to include the Austrian Energy CERT (AEC).

The latest ICT risk analysis of the energy industry of the year 2018 merged the already existing two ICT risk analyses in the electricity and gas subsector. 225 relevant hazards were identified. These were subsequently assessed and analysed in terms of 69 common individual risks and a further 19 electricity-specific risks on the basis of the defined risk assessment criteria according to various aspects. The 69 common individual risks were combined into 16 aggregation risks in several iterations. Basically, two risk views were chosen: one was the primarily operational view with a view to security of supply in the energy industry and the other a reputational view of all types of disruptions. All risks were assessed in a "worst case", "best case" and in a "most likely case" (expectation view).

The individual risks (including the current-specific risks) were assigned to nine risk categories, which also represent the primary but not exclusive aggregation criterion. Within these risk categories, 36 recommendations were developed which were assigned to several stakeholders. In order to facilitate the implementation and monitoring of measures, the expert group proposed a process owner for all recommendations who would also coordinate or catalyse the implementation of the recommendations in three predefined future horizons.

The risk minimization measures resulting from the individual and aggregation risks were developed on the basis of a purely technical-organizational discourse. The aim of the process is to coordinate and define the minimum security standards in the energy industry through a joint development process with the NIS competent authority.

The Netherlands: public-private exercises to test cyber resilience

Since 2015, two public-private exercises were organised to simulate cyber incidents and test the operational resilience to these incidents. These exercises (aka ISODOOR) were organised by the Dutch National Coordinator for Security and Counterterrorism (NCTV), in close collaboration with various public and private partners. The ISODOOR I exercise was organised in June 2015 and was followed by ISODOOR II in October 2017, both events were 4-day

exercises and involved operational services, various ministerial departments and private partners from the telecom, energy and financial sectors. A third exercise is planned for the autumn/winter of 2019.

United Kingdom

In the UK, the Department for Business, Energy & Industrial Strategy (BEIS) engaged extensively with energy sector stakeholders to consider the requirements of the Directive and how best to make them work within the UK. BEIS held three industry workshops during the consultation period and has also provided regular updates at industry forums, including E3CC (Energy Emergency Executive Cyber Committee), DOCSG (Downstream Oil Cyber Security Group), OGISF (Oil and Gas Information Sharing Forum) and through EnergyUK. Energy sector stakeholders, Ofgem (national regulatory authority) and HSE (health and safety executive) were informally consulted in the preparation of defining the identification thresholds for OES and for incident reporting.

In the UK, the NIS Regulations 2018 require energy companies identified as OES to demonstrate active cyber security risk management, report incidents that disrupt energy supply, and take action to rectify those incidents. The Regulations identify a role for one or more regulatory bodies ('Competent Authority') to ensure compliance.

For the Energy Sector the Competent Authorities, as named in the Regulations, are BEIS for the oil sector and upstream gas sector, and Ofgem and BEIS acting jointly for the electricity sector and downstream gas sector. In addition, HSE undertakes compliance and enforcement functions for the oil sector and specified sections of the gas sector on behalf of BEIS.

Energy operators which meet thresholds set by BEIS must take appropriate and proportionate security measures to manage risks to their network and information systems and to notify serious incidents to the relevant authority.

The UK broad approach to the Regulations is to use NIS to reinforce much of our on-going work with industry, allowing for continued voluntary and collaborative efforts to improve levels of cyber security across the sector, within a more formal framework.

To ensure effective implementation, UK sought an approach which minimises the burden on industry as far as possible, whilst ensuring that appropriate and proportionate steps are taken by OES to manage the risks to their cyber security. All OES have completed Cyber Assessment Framework self-assessments the Framework developed by the National Cyber Security Centre, the designated CSIRT - of their cyber security arrangements. HSE and Ofgem are using these to inform their inspection planning priorities. BEIS will conduct an analysis exercise in August to produce an evidence base for future policy making under NIS.

DCMS (lead government department for the NIS Directive) is leading a cross-government review of the NIS Regulations which will report to the EU by May 2020. It will examine whether the regulation is currently fit for purpose for the energy sector. The review will also explore whether further changes (hardening and expansion) of the regulation are needed. Industry will be consulted as appropriate, using various forums and communications.

3 Governance

This chapter provides an overview of the status of implementation of OES identification in the energy sector by the EU MS by providing reference to the sector – specific definitions, appointed National Competent Authorities and relevant transposition laws and regulations. Definitions of energy essential services are provided in Annex I of this document.

3.1 Appointed National Competent Authorities (NCAs) in the MS

According to the NIS Directive, MS must designate one or more competent authorities to monitor the application of the NIS Directive at a national level. So far, most – if not all - of the EU MS have appointed single or multiple National Competent Authorities for the supervision of the sectors and subsectors mentioned in Annex II of the NIS Directive.

From the survey replies, most of the MS have appointed a single NCA for the identification of OES in the energy sector and its subsectors, while only three have appointed multiple NCAs for the subsectors.

The following table displays the NCAs for the energy sector that have been appointed to support the implementation of Article 5 in the MS and their responsibilities.

1. Incident reporting: the authority which receives the incident notification
2. Security measures: the authority which sets the security measures
3. Receiving and dealing with incident notification: might be different from the 'incident reporting' role
4. Supervision: the authority which oversees the implementation e.g runs audits
5. Supervisory body: the authority which coordinates every aspect of the NIS Directive implementation in the sector
6. Identification: the authority identifying the OES.

Table 1 - Energy sector NCAs

Country	Energy National Competent Authorities	Responsibilities
Austria	Federal Chancellery of Austria	2, 6
	Federal Ministry of the Interior	1, 3, 4
Belgium		
Czech Republic	National Cyber and Information Security Agency (NCISA)[2]	
Germany	Federal Office for Information Security – BSI	
Denmark	The Danish Energy Agency	
Estonia	Estonian Information System Authority	

[2] See: https://www.govcert.cz/en/

Finland	Ministry of Economic Affairs and Communications (ministry in charge of Energy authority)	
	Energy authority	1, 2, 3, 4
	National Cyber Security Centre Finland (NCSC-FI)	3
	Ministry of transport and communications	5, 6
France	National Agency for the Security of Information Systems (ANSSI) and the Ministry for the Ecological and Inclusive Transition	1, 2, 3, 4, 5, 6
Italy	Ministry of Economic Development – DG: High Institute for Information and Communication Technologies	1,2,3,4,5,6
Latvia	Ministry of Economics	6
Luxembourg	Electricity: Institut Luxembourgeois de Régulation (ILR) Gas: ILR Oil: Ministère de l'Énergie et de l'Aménagement du territoire & ILR	
The Netherlands	Ministry of Economic Affairs and Climate Policy	5, 6
	National Coordinator for Security and Counterterrorism	1, 3
	Radiocommunications Agency Netherlands	1, 3, 4 and to some extent also 2 (see footnote)[3]
Poland	Minister of Energy	
Portugal	For all subsectors: - Portuguese National Cybersecurity Centre; - Portuguese Energy Services Regulatory Authority;	1, 2, 3, 4, 5, 6 are under the exclusive legal competences of the Portuguese National Cybersecurity Centre

[3] For the energy sector, the Radiocommunications Agency Netherlands (AT) bases its audits on 'open norms'; the OES are responsible to ensure their cyber security and it is the responsibility of AT to supervise whether they fulfil their obligations.

	- Portuguese Directorate-General of Energy and Geology.	
Spain	For energy subsector: - National Center for Infrastructure Protection and Cybersecurity (NCIPC) - Ministry for Ecological Transition/Secretary of State for Energy - Spanish National Cybersecutity Institute[4]	2, 4, 5, 6 6 1, 3
Sweden	Swedish Energy Agency (Energy CA) Swedish Contingency Agency (National CA)	2, 3, 4, 5, 6 1, 2, 3
United Kingdom	Electricity: Department of Business, Energy and Industrial Strategy (BEIS) & Ofgem are Joint Competent Authorities. Gas: BEIS & Health & Safety Executive (HSE) upstream gas, BEIS & Ofgem downstream gas. Oil: BEIS & HSE	

Germany pursues an operator driven approach to identify OES in the energy sector. It is thus primarily up to the undertakings to check whether they fulfil the legal requirements (criteria) to qualify as OES in the energy sector. If requested, the Federal Office for Information Security (Bundeamt für Sicherheit in der Infomationstechnik – BSI) might give advice and assistance to untertakings in this process. In addition, undertakings might also seek help from the Federal Regulatory Authority (Bundesnetzagentur – BNetzA). However, these authorities are not involved in this process on a regular basis.

An advantage of the single competent authority approach is strong and clear command & control of a single government body that steers the identification process. The multiple competent authority approach on the other hand, is likely to have more detailed insights into the respective critical sector. This knowledge can also be of advantage during the identification process.

[4] INCIBE-CERT is the reference security incident response center for citizens and private law entities in Spain, operated by The Spanish National Cybersecurity Institute (INCIBE), under the Ministry of Economy and Business (MINECO) through the Secretary of State for Digital Advancement (SEAD). In the case of incident management affecting critical private sector operators, INCIBE-CERT is jointly operated by INCIBE and NCIPC, the National Center for Infrastructure Protection and Cybersecurity of the Ministry of Home Affairs

3.2 NIS Directive transposition laws

All the MS that participated in this paper by responding to the survey have transposed article 5 of the NIS Directive through either a new national law, ordinance, decree or amendment of an older legislation. The transposition legislation per country as outcome of the survey of work stream 8 is presented in a table in Annex II.

4 EU Associations and bodies of operators in the energy sector

The purpose of this section is to provide information relevant to the cyber security capabilities of the EU associations, organisations and bodies of energy operators with a role in the energy sector. To achieve this, a list of 'priorities' maps the role of associations, organisations or bodies that have participated in this survey.

4.1 Roles and responsibilities

The sectorial analysis presents the EU cybersecurity capacity in two distinct dimensions, namely policymaking and cybersecurity lifecycle (incident handling lifecycle).

In order to classify the roles and responsibilities related to cybersecurity capabilities for the EU associations, organisations and bodies of energy operators with a role in the energy sector the following categorisation of capabilities is being used as point of reference:

- **Implementation:** EU associations, organisations and bodies that undertake the implementation of the relevant policy and actions.

  Examples might include:

  - implementation of cybersecurity-related regulation;
  - drafting, update and issuance of regulation;
  - identification and anticipation of incidents;
  - auditing and assessment of the proper implementation of cybersecurity-related legislation;
  - real-time detection/response/recovery of cybersecurity incidents;
  - post-incident information sharing across pertinent stakeholders.

- **Support:** advise, facilitate or other means of supporting the implementation described above.
- **N/A:** no role
- **Other:** none of the above is valid but another type of classification exist in this case. For this selection, it was advised to participants to provide explanations that might be of help to identify further roles or actions and thus, possible extensions of this list.

4.2 Definitions of priorities

Based on key EU cyber security policy documents, i.e. the Cybersecurity Strategy for the European Union and the Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", a set of priorities has been identified. Also the "EE-BG-AT Trio Presidency Cybersecurity Work Programme" (Working Document WK7101/2017) was taken into consideration.

Table 2 - Definitions of priorities

PRIORITY	SHALL MEAN FOR THE PURPOSE OF THIS DOCUMENT
Build cyber resilience	Building EU resilience to cyber-attacks.
Cyber Crisis Management	EU support in case of a major cyber incident or attack and achieving resilience of the energy value chain through rapid emergency response.
Awareness raising	Raising awareness and promoting cyber hygiene and awareness.
Training	Training & Education and practical application in order to address the lack of cyber experts in the energy sector across EU; Step up efforts on NIS education and training; Coordinate the design and planning of training courses.
Incident handling, response and recovery	Coordination between NIS competent authorities/CSIRTs, law enforcement, defence, ENISA etc; Implementing the NIS Directive with a view to achieve resilience through rapid emergency response.
R&D	Research & development in general or fostering R&D investments and innovation.
Capacity building	Supporting the MS or the EU as per increasing cybersecurity capacities and cyber resilience against energy systems.
Situational awareness[5]	Achieving or providing the grounds for better situational awareness on part of MS regarding the current risks and responding to threats in cyberspace.
Standardisation / certification	Developing industrial and technological resources for cybersecurity with the aim to promote a Single Market for cybersecurity products.
Cyber exercises / cyber ranges	Promoting the usage and development of Cyber Ranges in providing MS and the EU with a robust cyber exercise programme or supporting the MS and the EU institutions, agencies or bodies in carrying out regular pan-European cyber exercises.
Develop and implement policy and regulations	Developing the EU strategic vision for cybersecurity and/or implementing cyber security regulations e.g. the NIS Directive, energy cyber security regulations etc.
Develop industrial and technological resources	Associations, organisations or bodies which develop industrial and technological resources for cybersecurity towards a Single Cybersecurity Market such as PPPs, Cybersecurity Research and Competence Centres etc.
Support information sharing and cooperation	Facilitating coordination between NIS competent authorities/CSIRTs, law enforcement and defence, ENISA etc.

ACER

The EU Agency for the Cooperation of Energy Regulators (ACER) supports awareness raising, trainings, situational awareness priorities and information sharing and cooperation. For the first priority, ACER, together with CEER and Florence School of regulation organises a Workshop on the topic every two years. It also**,** provides and supports training in the area of cyber security for the energy sector through the expertise of its staff. In terms of situation awareness, ACER organises and participates to thematic meetings on Cyber Security. ACER tries to facilitate the cooperation among all actors, trying to direct the stakeholders toward the appropriate counterparty. For example, when approached ACER directed the stakeholders to ENISA and/or to the National Competent Authorities.

ACER also develops and implement policy and regulations. It has contributed to the definition of the pillars for the Network code on Cyber Security rules for electricity. When the Clean

[5] Situational awareness is primarily in the responsibility of the Member States. The EU actors listed for this priority in the present mapping provide roles that can support Member States in this process.

Energy for All Europeans Package will be approved, ACER, on initiative of the European Commission, will be ordered to prepare the Framework Guidelines, which will be the basis for the Network Code.

CERT-EU

The Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) both supports and implements many of the priorities for the energy sector. CERT-EU supports building cyber resilience, although it is limited to CERT-EU constituents in the energy sector, and supports situational awareness by disseminating energy related reports to the relevant stakeholders. Furthermore, it is supporting the priority of development and implementation of policy and regulations through relevant activities in order to enrich them with its operational experience.

CERT-EU in cooperation with EC/DG CNECT, ENISA and other EU institutions participates in Crisis Management exercises. In terms of awareness raising, it is producing threat alerts on an ad hoc basis. EU institutions with a focus on energy are amongst the recipients of these alerts. CERT-EU is also implementing incident handling, response and recovery, but this is limited to EU institutions in the Energy sector (e.g. ACER). As regards to cyber exercises and cyber ranges capabilities, CERT-EU is participating in various cyber exercises with a European nexus (e.g. Cyber Europe, Lockedshields).

DG CNECT

The Directorate-General for Communications Networks, Content and Technology (DG CNECT) formulates and implements the overall policy related to the cybersecurity of the internal market. In addition, it supports the R&I agenda in the field through projects lunched under the EU Funding Programmes such as Horizon 2020 and Connecting Europe Facilities (CEF).

For the policy side, DG CNECT is responsible for the overall implementation of the NIS Directive, it provides the secretariat of the Cooperation Group and it coordinates the activities of the Working Groups established under the Cooperation Group. Along with DG ENER and Austria, it coordinates the activities of the Work Stream 8 on Energy - established in June 2018 - which brings together MS Authorities dealing with cybersecurity and energy.

DG CNECT is also responsible for the implementation of the Cybersecurity Act, which established an EU framework for the cybersecurity certification of ICT product, services and processes. According to the *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*[6] (September 2017) once the Framework is established, the Commission will invite the relevant stakeholders to focus on priorities areas, which may include high-risk applications, covering for example the energy sector (e.g. power plants). In the context of the work related to certification, DG CNECT will work together with ENISA, which is responsible for putting together future European schemes.

In addition, DG CNECT is also responsible for the funding for Cybersecurity under the CEF, which aims to strengthen the EU's capacity to cope with cyber threats jointly. Funding opportunities concern all phases of the risk management process (i.e. from preparedness actions to incident handling, response and recovery). The majority of the funding – earmarked through a yearly call – has revolved around the implementation of the Directive on security of

[6] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

the NIS Directive with beneficiaries being CSIRTs, OESs, NCAs. In the 2018 call, the majority of OESs belong to the energy sector, reflecting the increasing digitalization of the sector and the attention to cybersecurity.

More specifically on the research side, DG CNECT supports the preparation and implementation of relevant projects under Horizon 2020. For example, DG CNECT and DG ENER have co-drafted a call text for projects[7] aiming to make Electrical Power and Energy System (EPES) more resilient to growing and more sophisticated cyber and privacy attacks and data breaches. Relevant projects recently started or are about to start soon.

DG ENER

The Directorate-General for Energy (DG ENER) supports cyber resilience and capacity building by providing guidance on cybersecurity in the energy sector. Apart from supporting the aforementioned priorities, it implements many of them.

In April 2019, the Commission adopted a sector-specific guidance[8] that identifies the main actions required to preserve cybersecurity and be prepared to possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies.

Additionally, DG ENER raises awareness and increases information sharing

- at a higher-level via dedicated events like conferences and workshops (e.g. March 2017 in Rome; October 2018 Brussels; July 2019 Brussels);
- among MS: The Commission kicked-off a working stream under the NIS Cooperation Group dedicated to energy to bring together MS Authorities from the cybersecurity and the energy side.
- through enhanced cooperation with the specialised entities such as the European Energy Information Sharing and Analysis Centre on cybersecurity (EE-ISAC).
-

Further DG ENER works with dedicated expert groups on cybersecurity in the energy sector, such as the Smart Grids Task Force and with groups related to security of energy supply, such as the Electricity Coordination Group and the Gas Coordination Group.
In the Clean Energy for All European Package, the Commission has tabled several proposals that are relevant and will reinforce cyber security:

- The new regulation on electricity risk preparedness[9] will mandate MS to develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks.

The recast of the Electricity Regulation proposes to develop a network code on cyber security, to increase the resilience of the energy sector and protect the energy systems. Since 2017, a dedicated expert group is working to prepare the ground for such a network code.Further to this, according to the Regulation on Security of Gas Supply cyber-attacks have to be considered by MS in national and common risk assessments.

DG ENER participates in the planning of Cyber exercises / cyber ranges as well as in the exercises itself.

---

[7] Topic SU-DS04-2018-2020. Projects are 'EnergyShield', 'PHOENIX' and 'SDN-microSENSE'.
[8] Recommendation C(2019)240 final and staff working document SWD(2019)1240 final
[9] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019, p. 1–21. http://data.europa.eu/eli/reg/2019/941/oj

ENISA

The EU Cybersecurity Agency, ENISA, works closely together with Members States and private sector to deliver advice and solutions on many key areas, such as the Energy sector. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to Network and Information Security. Within its policy remit, ENISA has been supporting the field of European cyber incident and crisis management for several years, with activities ranging from crisis simulations to trainings, support to MS in developing their crisis plans and structures, international conferences and several studies. A large part of the prevention capacity building efforts of ENISA in this area is covered within the topic the cyber exercises. ENISA also supports information sharing and cooperation in the Energy sector through its involvement and membership in the EE-ISAC.

With the forthcoming Cybersecurity Act, ENISA will also support an implement activities related to certification.

ENTSO-E

Besides situational awareness, certification/standardization and development of industrial and technological resources, the European Network of Transmission System Operators (ENTSO-E) supports all the rest of the priorities existing in the provided list of the survey. ENTSO-E supports many priorities, such as supporting TSOs to build cyber resilience, but also implements cyber crisis management and policy and regulations. Out of all the responds of the survey, ENTSO-E has the strongest role, especially in terms of support.

ENTSO-G

For raising awareness, the European Network of Transmission System Operators for Gas (ENTSO-G) has a joint CS Task Force with GIE. Members and representatives of ENTSO-G are part of this joint TF. Through the same joint Task Force, ENTSO-G supports information sharing and cooperation by providing analysis of specific reports, such as the CEER report on cybersecurity.

Apart from ENTSO-G participation in the joint CS Task Force with GIE, some members of ENTSOG may be engaged in other priorities with the national bodies (e.g. BSI Germany or the NRA BNetzA).

FETSA

According to the information provided, the Federation of European Tank Storage associations (FETSA) supports information sharing and cooperation as well as publishes pertinent good practices through its member association.

GIE

Gas Infrastructure Europe (GIE), as an association, has a limited coverage on the listed priorities, supporting mainly awareness raising and information sharing and cooperation. However, vast majority of GIE members are strongly involved in cybersecurity via engagement with national regulatory bodies and agencies. GIE supports awareness raising programs with workshops, working groups on cyber security, and an annual event on cyber security, titled “Cyber Security Day”. Moreover, GIE supports activities on information sharing and cooperation with its Annual Conference, which includes a dedicated slot for cyber security.

IADC

The International Association of Drilling Contractors (IADC) is the forum for all oil and gas drilling industry stakeholders to connect, share knowledge, and develop solutions to critical issues. In the context of awareness raising, it strives to communicate and collaborate with its members and other organizations on cyber related matters and potential impacts to the industry. For capacity building purposes, IADC will facilitate and cooperate with its members' desires to increase their cybersecurity capacities and cyber resilience awareness and work with other organizations/bodies. Also, IADC will take receipt of EU member information/direction to facilitate situational awareness concerns among IADC's member companies and other organizations in the oil & gas drilling space, as may be considered necessary.

Though not directly charged with development of standards/certification, IADC has created cyber security guidelines for our members consideration and will engage with appropriate standards bodies to this end as appropriate. In terms of cyber exercises, IADC's member driven cybersecurity committee has conducted a cyber security exercise in the U.S. among IADC member companies. IADC also engages in consultative processes to provide necessary input in the formulation of policy and regulation. Finally, IADC is poised to information sharing and seeks cooperation among its members, along with other oil and gas upstream organizations/bodies.

4.3 Overview of EU institutions' and stakeholder activities in the Energy sector

Table 3 - EU Institutions' and stakeholder activities

PRIORITY	IMPLEMENTATION	SUPPORT	OTHER	N/A
Build cyber resilience		ENTSO-E CERT-EU EC ENISA		GIE FETSA ENTSO-G IADC
Cyber Crisis Management	ENTSO-E CERT-EU	ENTSO-E ENISA EC		GIE FETSA ENTSO-G IADC
Awareness raising	CERT-EU EC	ENTSO-E GIE ACER ENISA	ENTSO-G IADC	FETSA
Training		ENTSO-E ACER ENISA EC		GIE FETSA ENTSO-G EC IADC
Incident handling, response and recovery	CERT-EU	ENTSO-E ENISA		GIE FETSA ENTSO-G EC IADC
R&D	REA	ENTSO-E EC	ENISA	GIE FETSA ENTSO-G CERT-EU IADC
Capacity building		ENTSO-E DG ENER ENISA EC	IADC	GIE FETSA ENTSO-G CERT-EU
Situational awareness	EC	CERT-EU ACER ENISA	IADC	ENTSO-E GIE FETSA ENTSO-G

Standardisation / certification	ENISA* EC	ENISA* EC	IADC	ENTSO-E GIE FETSA ENTSO-G CERT-EU
Cyber exercises / cyber ranges	CERT-EU ENISA	EC	EC IADC	GIE FETSA ENTSO-G
Develop and implement policy and regulations	ENTSO-E ACER EC	ENISA	IADC	GIE FETSA ENTSO-G
Develop industrial and technological resources		ENISA*		ENTSO-E GIE FETSA ENTSO-G CERT-EU EC IADC
Support information sharing and cooperation	CERT-EU EC	ENTSO-E GIE ACER FETSA ENISA	ENTSO-G IADC	

**under the Cybersecurity Act*

From the above table it is evident that not all priorities are yet supported, and most importantly, implemented by EU institutions, EU bodies and European energy associations. ENTSO-E seems to support most of the priorities and in some cases implements some of them. On the other side, as statistics provide through the mapping table above, four out of the thirteen priorities are not supported, while six out of the thirteen priorities are not implemented by any of the respondents.

In order to achieve a thorough cybersecurity posture in the energy sector through a complete support from EU institutions it is necessary to address further the coverage of all cybersecurity capabilities.

5 Identification of essential services in the Energy sector

Before starting with the identification of OES, EU MS need to define which services they deem as essential for their country. As a starting point, EU MS can use Annex II of the NIS Directive, which outlines different essential services (e.g. *distribution of electricity*, *transmission of electricity*, *oil production* and *oil transmission*). The table in Annex III illustrates what the responding MS chose when defining what an essential service in their country is.

5.1 Identified Essential Services

The most common essential services identified by MS – including essential services provided by types of entities beyond Annex II of the NIS Directive – in the Energy sector are listed in the table below:

Table 4 - Identified Essential Services by MS

Subsector	Essential service
Electricity	Generation / Production Transmission Distribution Sale Quality-assurance services and management of energy infrastructure Storage facility Facility or system to control/consolidate electrical power Metering infrastructure
Gas	Production Storage Transport Distribution Sale Market area management Distribution area manager LNG system operation Gas extraction facility Long-distance gas pipeline network Transmission of gaseous fuels Trade in gaseous fuels or trade in gaseous fuels abroad LNG liquefaction and regasification, and imports and unloading of LNG Metering infrastructure

Oil	Extraction Storage Transmission Refining and treatment Production Processing Oil extraction facility Long-distance oil pipeline Facility for central control of multiple sites Facility or system of aggregators for fuel and fuel oil distribution Facility for central control of multiple sites Production of liquid fuels Crude oil pipeline transportation Pipeline transportation of liquid fuels Crude oil storage Crude oil trans-shipment Storage of liquid fuels Trans-shipment of liquid fuels Production of synthetic fuels

5.2 Identified essential energy services beyond Annex II of the NIS Directive

The majority of the participating countries have taken the opportunity to identify additional essential services in the energy sector that are beyond the scope of the NIS Directive. The table in Annex IV lists such services per country.

Overall, the table below reflects the essential services identified by MS beyond Annex II of the NIS Directive.

Table 5 - Essential Services beyond Annex II of NIS Directive

Subsector	Essential service
Thermal industry	Thermal energy production Operation of a thermal energy supply system
District heating & heat supply	Heat generation plant Combined heat and power plant District heating network Heat generation Heat trading Heat transmission Heat distribution
Mining	Extraction of natural gas Crude oil extraction Brown coal mining Hard coal mining Copper mining
Supplies and services	Supply of systems, machinery, devices, materials, raw materials and providing services to the energy sector.
Supervised and subordinate units	Production of radiopharmaceuticals Radioactive Waste Management Keeping strategic reserves and stocks of crude oil, crude oil products and natural gas "Research and development or implementation works or technological research for the energy sector"

5.3 Challenges

There are a number of unanswered questions when implementing the NIS Directive, which complicate its implementation for the EU MS. The table below presents a few challenges that were reported by the respondents.

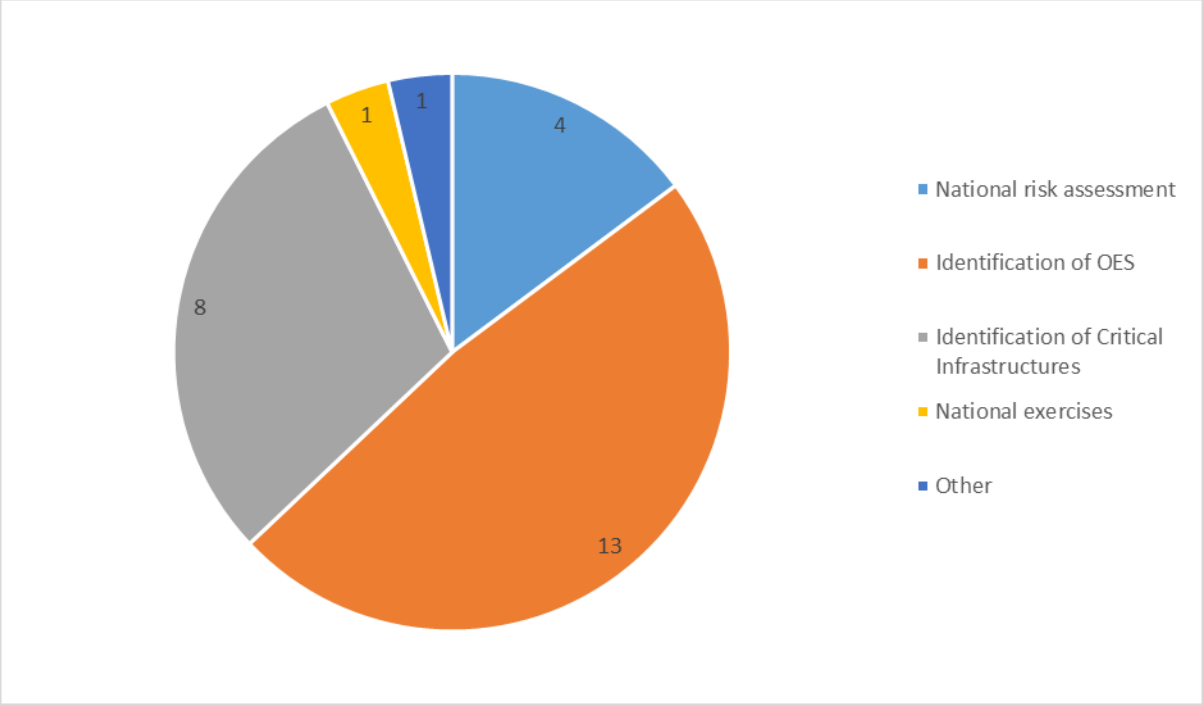
Table 6 - Implementation Challenges

Implementation challenges have been faced in regards to the oil sector. If the essential service is related to the obligation to hold emergency stocks in case of an oil crisis, the challenge arises that only downstream oil companies may be obliged to do in a MS, whereas there is no such obligation to hold emergency stocks for petrol stations. However, petrol stations are the last link in the service chain.
In the electricity sector, there can be implementation challenges with new wind- and solar power production facilities in case a MS decided to make the need for a license a criteria for identification as new wind- and solar power production facilities tend to not need licence to establish power production capacity. Thus, no NIS obligations can be imposed on these companies. However, this can be solved through national legislation.
In one MS, the biggest challenge remains the fact that providers are identified only in the relation to the network and information systems administrated. Thereby, it can be difficult to determine where the certain parts of the network end and begin.
It can also be challenging to convince stakeholders and contributors to stay high level and generic when determining the essential service. Breaking down the essential service definitions is not necessarily and objectively useful.
The main challenges reported by the sectorial authorities in a MS were on the criteria adopted to identify OES specially when considering the external (global) market (especially neighboring countries) and the need of equal criteria to ensure even market positions of operators in each country and the decision of including or not types of entities in this sector not included in Annex 2 of the NIS Directive that also provide essential services such as energy producers.

6 Methodologies to identify the OES in the Energy sector

MS have followed several methodologies to identify OES in the energy sector. In some cases MS have performed national risk assessments, national exercises or have used already developed methodologies like the identification of critical infrastructure from the ECI Directive. The graph below illustrates the methodologies chosen by the responding MS. It is worth noticing that a MS might have chosen more than one methodology to identify OES in the Energy sector.

Figure 3 - Identification Methodologies for OES in Energy

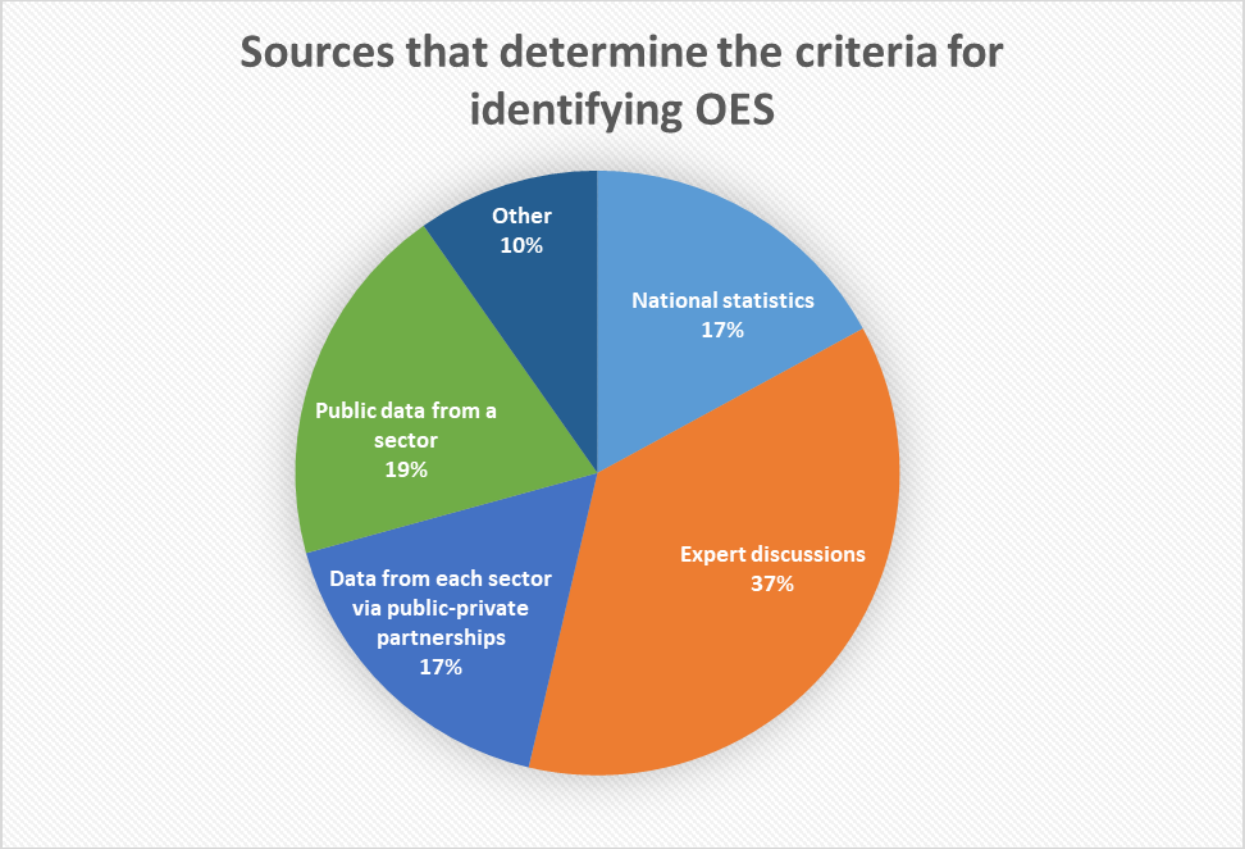


6.1 National approaches

Some of the countries that took part in this work already had methods and approaches in place before the release of the NIS Directive, while others have developed new methodologies. These methods were often similar (to varying degrees) to the concept of essential services as outlined in the Directive. Existing approaches either have been adjusted or are used as interim solution by EU MS, while working on an approach that will be more suitable to fulfil the requirements of the Directive. To determine the criteria for identifying OES, MS have taken under consideration several sources.

The graph below illustrates the sources that MS consulted in order to define which criteria would be used for their OES identification approach. A MS could consult one or several sources of the ones mentioned below.

Figure 4 - Sources for OES identification

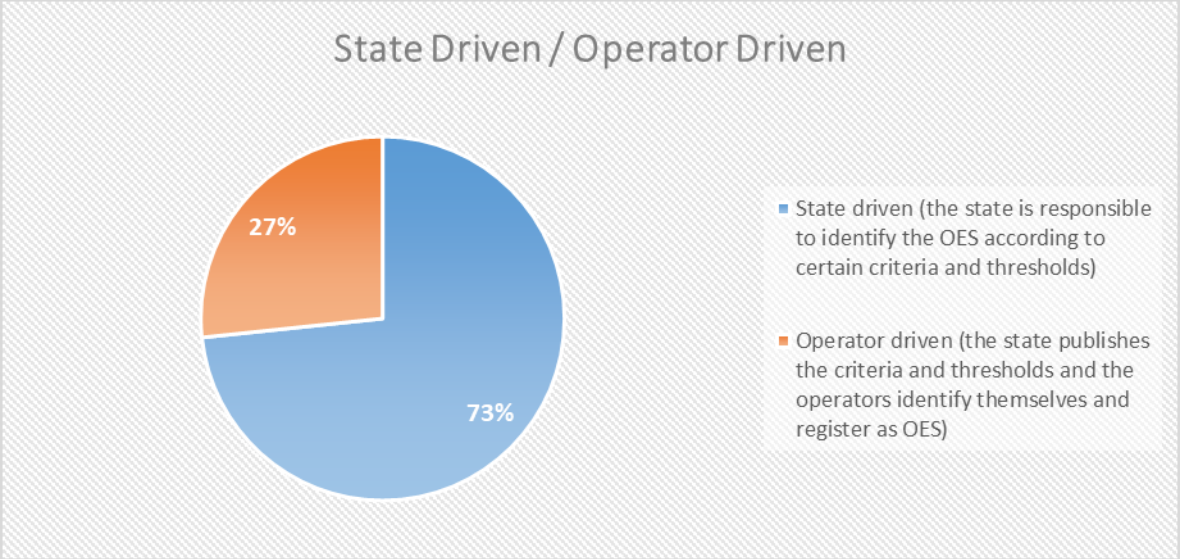


As already mentioned in several CG documents, MS usually follow two approaches to identify OES:

- The ***state-driven*** approach where the leading role is assumed by one or more governmental agencies/ministries that have the mandate to identify the Essential Services and OES - in most of the cases the responsible ministries.
- The ***operator-driven*** approach where operators self-assess if specific criteria are met and then register to the list of OES. This approach does not require the national authorities to identify individual operators of critical infrastructures – it is the operators' duty to notify the authorities when they fall under the predefined criteria.

The graph below shows the analogy base on the information gathered.

Figure 5 - State driven Vs Operator driven



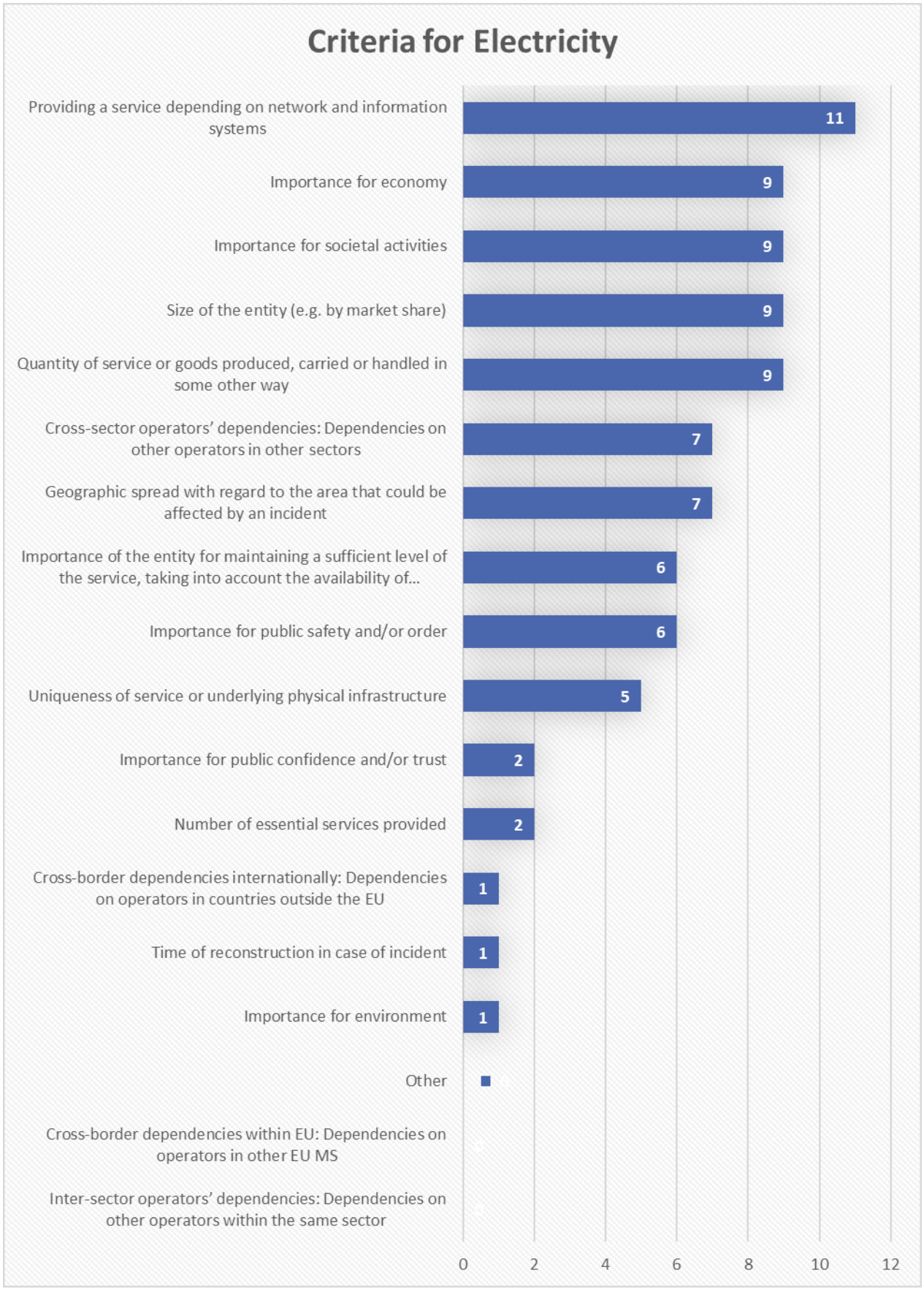
*An example of **a state driven** approach is that of France. In France, ANSSI exchanges directly with private operators at different stages of the process. In the designation process, a first step is to issue a letter of intention to each potential OES. This steps is always taken after previous informal contact between ANSSI and the operator. This letter indicates that the operator is approached for OES designation and asks if they have any comments about this designation, as well as the countries where they deliver an essential service operated from France.*

*An example of **an operator driven** approach is that of Germany. In accordance with the German law, it is up to the operators to identify themselves as OES on the basis of certain criteria and thresholds laid down in the BSI-KRITIS Ordinance/ Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). In other words, a criteria-based procedure is applied. In addition, the Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK) provides guidance to undertakings concerned. In 2017, it has published a guidance tool: Protecting Critical Infrastructures – A Seven Step Identification Process.*

6.2 Criteria and thresholds for Electricity

For the majority of the respondents, the most important criterion for identifying an OES in the Electricity subsector is the number of people relying on the services. As second and third criteria, of equal importance, come the provisioning of a service depending on network and information systems and the quantity of services or goods produced, carried or handheld in some other way.

Figure 6 - Identification Criteria for Electricity



A part the criteria used for the identification of an OES in the Electricity sub-sector, the participants of the survey also provided specific thresholds they use for validating the identification process. In the following table, all criteria and corresponding thresholds provided from the respondents are summarised. The table also reveals thresholds used for criteria other than the one used to create the previous statistic.

Figure 7 - Criteria & Thresholds for Electricity

Country	*Criteria*	*Thresholds*
Austria	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	Generation: 340 MW bottleneck capacity
	Number of people relying on the service provided	Distribution: 88.000 metering points
	Other	All TSOs, many of the above mentioned criteria play a role.
Belgium	Providing a service depending on network and information systems	
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	Importance for societal activities	
	Importance for economy	
	Importance for public safety and/or order	
	Importance for public confidence and/or trust	
	Importance for environment	
	Time of reconstruction in case of incident	
	Uniqueness of service or underlying physical infrastructure	
	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	
Czech Republic	Providing a service depending on network and information systems	N/A

	Quantity of service or goods produced, carried or handled in some other way	a) production facility with total installed generating capacity of at least 500 MW; b) a supporting services plant with total installed generating capacity of at least 100 MW
	Number of people relying on the service provided	The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause a serious limitation, disruption or unavailability of the type of service which would affect more than 50.000 people;
	Importance for economy	Economic loss greater than 0,25 % of GDP
	Importance for public safety and/or order	More than 100 casualties or 1.000 injured people in need of medical treatment
	Geographic spread with regard to the area that could be affected by an incident	Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	A serious limitation or disruption of another OES or CII element
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers
	Other	E.g. a technical control centre used in the oil transmission pipeline operation
Germany	Number of people relying on the service provided	500.000
Estonia	Quantity of service or goods produced, carried or handled in some other way	200 MW
	Number of people relying on the service provided	10.000 consumers
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	-
Latvia	Providing a service depending on network and information systems	N/A
	Size of the entity	Dominant market share

	Number of people relying on the service provided	10 000
	Geographic spread with regard to the area that could be affected by an incident	- the service provider is the only provider of such type of service in the territory of the Republic of Latvia - the service provider is the only provider of this type of service in one of the planning regions of Latvia
	The actual capacity installed by the service provider	exceeds 50 MW
	Length of the heat networks in the ownership of the service provider.	at least 100 km
Luxembourg	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	–
	Size of the entity (e.g. by market share)	>33%
	Number of people relying on the service provided	15.000
	Importance for societal activities	–
	Importance for economy	–
	Importance for public safety and/or order	–
	Uniqueness of service or underlying physical infrastructure	–
	Geographic spread with regard to the area that could be affected by an incident	–
	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	–
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	–
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	-
The Netherlands	Importance for societal activities	Set for TSO's/DSO's, no specific criteria or threshold. Production: not decided yet, but most likely the revised Decree will include in 2020 a threshold for generation capacity.
	Importance for economy	
Poland	Quantity of service or goods produced, carried or handled in some other way	Minimum 0.4% in annual electricity production; share of electricity sold by the company in relation to the total amount of electricity supplied to end users nationwide, minimum 3.5%.

	Size of the entity (e.g. by market share)	Percentage share of customers of a given operator in relation to the total number of customers nationwide: minimum 2.5%
	Number of people relying on the service provided	Number of users minimum 500 thousand per year
	Uniqueness of service or underlying physical infrastructure	Installed electricity generation capacity minimum 120 MW gross, or percentage share of electricity generated and sold in total electricity production nationwide; transmission network length of at least 5 km or having/managing a Main Power Supply Station.
Portugal	Providing a service depending on network and information systems	
	Number of essential services provided	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	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	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
Spain	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
	Importance for societal activities	
	Importance for economy	
	Importance for public safety and/or order	
	Number of people relying on the service provided	
	Size of the entity (eg. market share)	
Sweden	Providing a service dependent on network and information systems	Basic requirement. I.e. is affects all operators.
	Quantity of service or goods produced, carried or handled in some other way	Production in terms of system criticality, size of network, concessional responsibilities.
	Importance for societal activities	Societal dependencies derived from regional planning, according to some of the *Styrel plan* (crisis management prioritization classification for electricity) for DSOs.

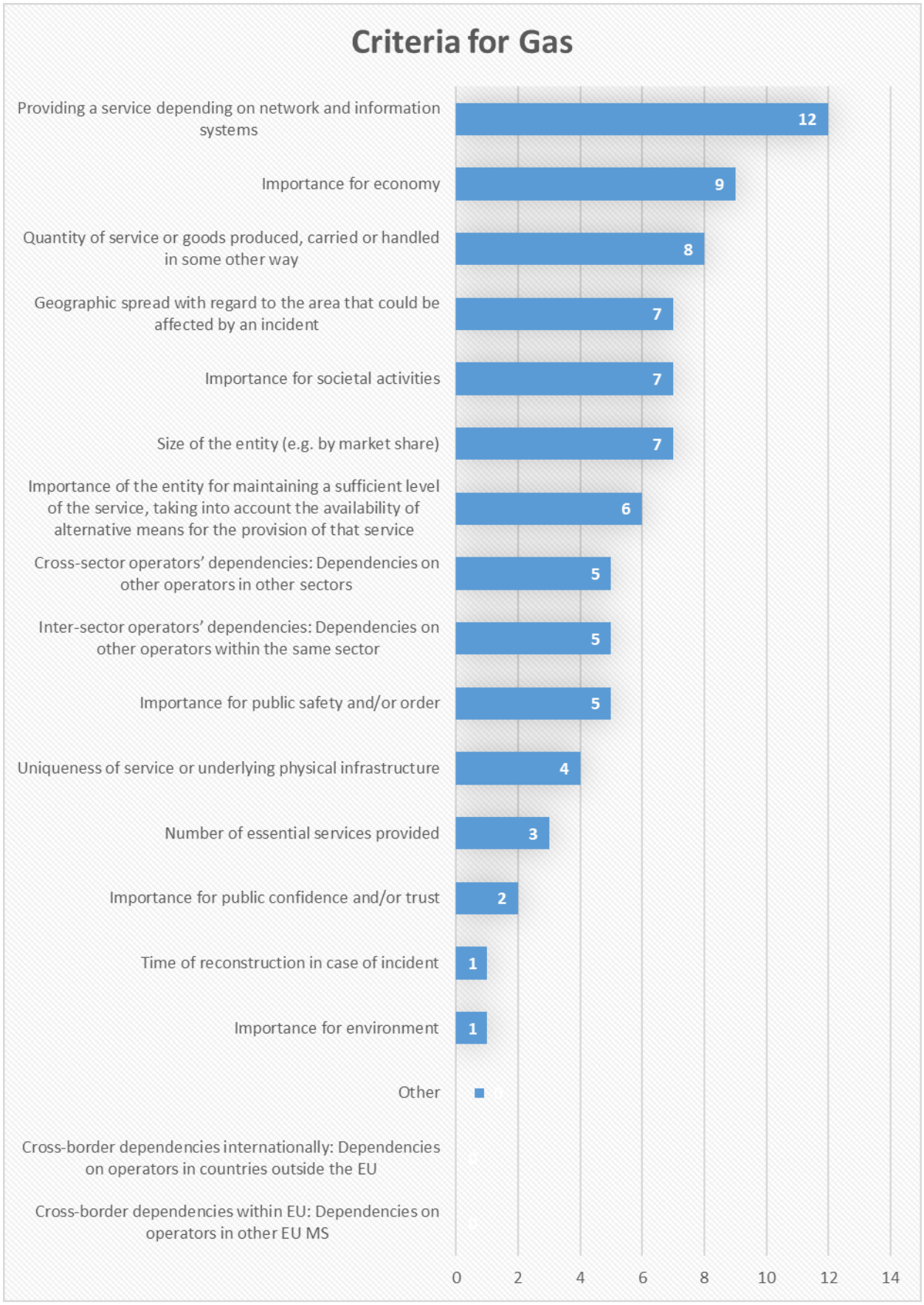
	Importance for economy	System criticality only. The thresholds are generally written from the perspective of the operators current market commitments, for the identification and for the incident reporting.
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	"All" TSOs, and same thresholds as; Importance for societal activities.
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	DSOs, and same thresholds as; Importance for societal activities.
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	TSO, larger DSOs and traders with balancing commitments.
	Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	TSO, larger DSOs and traders with balancing commitments.
United Kingdom	Providing a service depending on network and information systems	See Annex E NIS Policy Document Energy Sector GB[10]
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	

6.3 Criteria and thresholds for Gas

For the majority of the respondents, the most important criterion for identifying and OES in the Gas subsector is the provisioning of a service depending on network and information systems and then follows the quantity of service or good produced, carried or handheld in some other way. As in the case of the Oil sub-sector, the number of people relying on the service comes as third priority criterion in the Gas sub-sector.

[10] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

Figure 8 - Identification Criteria for Gas



Similarly, with the other sub-sectors, the participants of the survey provided specific thresholds they use for the corresponding criteria they selected in the survey for the identification of an OES in the Gas sub-sector. Among, other information, the below tables also shows thresholds used for any criteria the respondents may use and are classified as “other”.

Figure 9 - Criteria & Thresholds for Gas

Country	*Criteria*	*Thresholds*
Austria	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	Production: more than 20 % of annual domestic gas consumption Storage: working gas volume of more than 10.000 GWh per year Distribution: 88.000 metering points
	Other	All transmission pipelines
Belgium	Providing a service depending on network and information systems	
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	Importance for societal activities	
	Importance for economy	
	Importance for public safety and/or order	
	Importance for public confidence and/or trust	
	Importance for environment	
	Time of reconstruction in case of incident	
	Uniqueness of service or underlying physical infrastructure	
	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Inter-sector operators’ dependencies: Dependencies on other operators within the same sector	

	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	
	Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	
Czech Republic	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	Gas production or extraction amounting to annual production of at least 15 % of the annual consumption of the Czech Republic.
	Number of people relying on the service provided	The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause a serious limitation, disruption or unavailability of the type of service which would affect more than 50.000 people.
	Importance for economy	Economic loss greater than 0,25 % of GDP
	Importance for public safety and/or order	More than 100 casualties or 1.000 injured people in need of medical treatment
	Geographic spread with regard to the area that could be affected by an incident	Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	Serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	Serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	Serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element
	Other	E.g. a technical control centre used: - in the gas transmission system operation, - for the distribution system operation

Germany	Number of people relying on the service provided	500.000
Estonia	Number of people relying on the service provided	10.000 consumers
Latvia	Providing a service depending on network and information systems	n/a
	Size of the entity	Dominant market share
	Number of people relying on the service provided	10 000
	Geographic spread with regard to the area that could be affected by an incident	- the service provider is the only provider of such type of service in the territory of the Republic of Latvia - the service provider is the only provider of this type of service in one of the planning regions of Latvia
Luxembourg	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	–
	Size of the entity (e.g. by market share)	>33%
	Number of people relying on the service provided	15.000
	Importance for societal activities	–
	Importance for economy	–
	Importance for public safety and/or order	–
	Uniqueness of service or underlying physical infrastructure	–
	Geographic spread with regard to the area that could be affected by an incident	–
	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	–
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	–
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	-
The Netherlands	Importance for societal activities	Set for TSO's/DSO's, no specific criteria or thresholds.

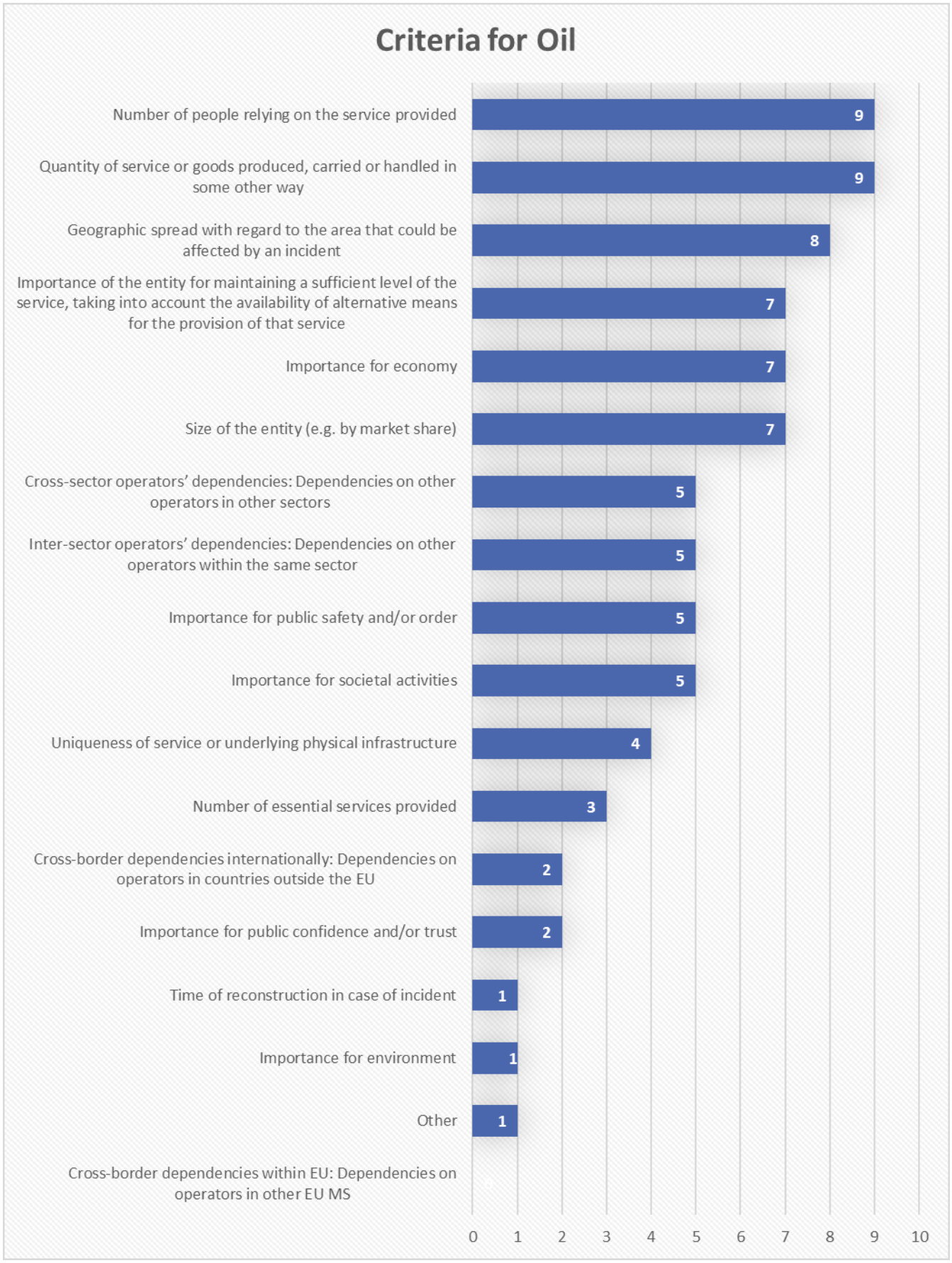
	Importance for economy	Set for the OES responsible for 'exploration and extraction' of Groningen-quality gas, no specific criteria or thresholds.
Poland	Quantity of service or goods produced, carried or handled in some other way	A quantity of gaseous fuels produced in the previous year, minimum 11 TWh; A volume of gaseous fuels transmitted in the previous year, minimum 110 TWh; A volume of natural gas imported in a previous year or ratio of natural a quantity of gaseous fuels produced in the previous year, minimum 11 TWh; A volume of gaseous fuels transmitted in the previous year, minimum 110 TWh; A volume of natural gas imported in a previous year or ratio of natural gas import to annual natural gas consumption in the previous year- minimum 60%- or natural gas fuels sold to end users in a previous year- minimum 27 TWh; A volume of gaseous fuels transmitted in the previous year, minimum 110 TWh; A volume of gaseous fuels distributed in the previous year, minimum 90 TWh; A volume of LNG regasified in the previous year, minimum 10 TWh.
	Uniqueness of service or underlying physical infrastructure	A level of working capacities provided to users in the previous year, minimum 30 TWh
Portugal	Providing a service depending on network and information systems	
	Number of essential services provided	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	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	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	

Spain	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
	Importance for societal activities	
	Importance for economy	
	Importance for public safety and/or order	
	Number of people relying on the service provided	
	Size of the entity (eg. market share)	
Sweden	Providing a service depending on network and information systems	Basic requirement
	Quantity of service or goods produced, carried or handled in some other way	TSO and all DSOs, all traders and intermediaries. For condensation, the threshold is set at 20 GWh/y.
	Number of people relying on the service provided	See above.
	Importance for economy	See above.
United Kingdom	Providing a service depending on network and information systems	See Annex E NIS Policy Document Energy Sector GB.pdf
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	

6.4 Criteria and thresholds for Oil

For the majority of the respondents, the two most important criteria for identifying and OES in the Oil subsector is the provisioning of a service depending on network and information systems as well as the quantity of service or good produced, carried or handheld in some other way. Interestingly, the number of people relying on the service comes as third priority criterion in the Oil sub-sector, in contrast with the case of the Electricity sub-sector that was identified as the most important criterion.

Figure 10 - Identification Criteria for Oil


Criteria for Oil
Number of people relying on the service provided
9
Quantity of service or goods produced, carried or handled in some other way
9
Geographic spread with regard to the area that could be affected by an incident
8
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
7
Importance for economy
7
Size of the entity (e.g. by market share)
7
Cross-sector operators' dependencies: Dependencies on other operators in other sectors
5
Inter-sector operators' dependencies: Dependencies on other operators within the same sector
5
Importance for public safety and/or order
5
Importance for societal activities
5
Uniqueness of service or underlying physical infrastructure
4
Number of essential services provided
3
Cross-border dependencies internationally: Dependencies on operators in countries outside the EU
2
Importance for public confidence and/or trust
2
Time of reconstruction in case of incident
1
Importance for environment
1
Other
1
Cross-border dependencies within EU: Dependencies on operators in other EU MS
0 1 2 3 4 5 6 7 8 9 10

Furthermore, the participants of the survey provided specific thresholds for the corresponding criteria they use for the identification of an OES in the Oil sub-sector. The table also reveals thresholds used for criteria other than the ones listed in the survey.

Table 7 Criteria & Thresholds for Oil

Country	*Criteria*	*Thresholds*
Austria	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	Extraction: more than 20 % of the annual domestic consumption Transmission: pipelines transporting more than 4 million tonnes per year Refining and processing: more than 8 million tonnes per year Storage: storing more than 10.000 tonnes compulsory emergency reserves
Belgium	Providing a service depending on network and information systems	
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	Importance for societal activities	
	Importance for economy	
	Importance for public safety and/or order	
	Importance for public confidence and/or trust	
	Importance for environment	
	Time of reconstruction in case of incident	
	Uniqueness of service or underlying physical infrastructure	
	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	

	Cross-border dependencies within EU: Dependencies on operators in other EU MS	
Czech Republic	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	a) A facility for oil production, processing, refining or treatment with installed annual production capacity of at least 3.000.000 tonnes ; b) A storage facility or set of storage facilities with capacity of at least 20.000 m3; c) An LPG storage facility with capacity of at least 20.000 m3; d) A pipeline with transmission capacity of at least 3.000.000 tonnes of product per year.
	Number of people relying on the service provided	The impact of a cyber security incident in the information system or in the electronic communications network on the functioning of which the service provision is dependent can cause a serious limitation, disruption or unavailability of the type of service which would affect more than 50.000 people;
	Importance for economy	Economic loss greater than 0,25 % of GDP
	Importance for public safety and/or order	More than 100 casualties or 1.000 injured people in need of medical treatment
	Geographic spread with regard to the area that could be affected by an incident	Disruption of public safety in a significant part of the administrative territory of a municipality with extended powers
	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	Unavailability of the type of service for more than 1.600 people which is irreplaceable in another way unless excessive costs were to be incurred

	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	A serious limitation or disruption of another OES or CII element
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	A serious limitation or disruption of another OES or CII element
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	A serious limitation or disruption of another OES or CII element
	Other	E.g. a technical control centre used in the oil transmission pipeline operation
Germany	Number of people relying on the service provided	500.000
Estonia	Quantity of service or goods produced, carried or handled in some other way	10 or more petrol stations
	Geographic spread with regard to the area that could be affected by an incident	Operating in 3 counties
Latvia	Providing a service depending on network and information systems	n/a
	Size of the entity	Dominant market share
	Number of people relying on the service provided	10 000
	Geographic spread with regard to the area that could be affected by an incident	- the service provider is the only provider of such type of service in the territory of the Republic of Latvia - the service provider is the only provider of this type of service in one of the planning regions of Latvia
Luxembourg	Providing a service depending on network and information systems	N/A
	Quantity of service or goods produced, carried or handled in some other way	–
	Size of the entity (e.g. by market share)	>33%
	Number of people relying on the service provided	15.000
	Importance for societal activities	–
	Importance for economy	–
	Importance for public safety and/or order	–

	Uniqueness of service or underlying physical infrastructure	–
	Geographic spread with regard to the area that could be affected by an incident	–
	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	–
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	–
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	-
The Netherlands	Other	Set for the Dutch Stockpiling Agency; threshold in the Stockpiling Act refers to the output on the Dutch market.
Poland	Quantity of service or goods produced, carried or handled in some other way	The amount of liquid fuels produced in the previous year, minimum 5 million tonnes, or the volume of crude oil processed in the previous year, minimum 5 million tonnes; volume of - crude oil pipeline transportation, minimum 10 million tonnes on a yearly average for the last 3 years; amount of liquid fuels transmitted/transhipment in the previous year, minimum 1 million tonnes a year; storage of minimum 500 thousand tonnes of crude oil on a yearly average for the last 3 years; an import of a minimum of 400.000 m3 of liquid fuels in the previous year, or the number of filling stations used to conduct business in the previous year: minimum 250 stations

	Uniqueness of service or underlying physical infrastructure	A total nominal capacity of storage facilities of the entity providing storage service, minimum 100 thousand m³.
Portugal	Providing a service depending on network and information systems	
	Number of essential services provided	
	Size of the entity (e.g. by market share)	
	Number of people relying on the service provided	
	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	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
Spain	Geographic spread with regard to the area that could be affected by an incident	
	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	
	Inter-sector operators' dependencies: Dependencies on other operators within the same sector	
	Cross-sector operators' dependencies: Dependencies on other operators in other sectors	
	Importance for societal activities	
	Importance for economy	

	Importance for public safety and/or order	
	Number of people relying on the service provided	
	Size of the entity (eg. by market share)	
Sweden	Providing a service depending on network and information systems	Basic requirement
	Quantity of service or goods produced, carried or handled in some other way	Volume on storing, handling and production. Importing/exporting/producing/refining/ processing/sales; in excess of; 500 000 t/y for fossil based, and 50 000 h/y for biofuels. Stocks, stores and depots; with combined capacity in excess of 100 000 m3, or 20 000 m3 in isolated areas, or 10 000 m3 for jet fuel. Pipelines or logistics with the capacity of handling in excess of; 500 000 t/y or 250 000 t/y for jet fuel.
	Importance for economy	Volume on storing, production.
	Cross-border dependencies within EU: Dependencies on operators in other EU MS	Common market Nordic/Baltic area
	Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	Common market Nordic/Baltic area
United Kingdom	Providing a service depending on network and information systems	See Annex E NIS Policy Document Energy Sector GB[11]
	Number of essential services provided	
	Quantity of service or goods produced, carried or handled in some other way	

[11] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

6.5 Dependencies

Regarding the approaches that MS follow for the identification of OES in the energy sector with cross-border impact, little or no information has been received by the MS on how do they assess these dependencies. In most of the cases, MS reported that the assessment takes place in close collaboration with the energy companies (normally in the context on national risk assessment) or under specific articles of the ECI Directive.

In any case, the process differs from one country to another. For example, in Sweden the energy markets are well connected in the Nordic/Baltic area, and the dependencies include non member states (i.e. Norway).[12] In other case, like in the Netherland, the evaluation is further complicated by the fact that each MS is responsible for the stability and security of its own energy supply, which should generally limit the vulnerability of each MS to incidents with OES from another MS.

Concluding, the process of assessment of cross border impact is currently on-going and most of the MS have no information to share for the time being.

[12] Sweden is in direct consultation with Norway on this topic, the OES are obligated to disclose such known dependencies and the Swedish Energy Agency's risk assessment does handle this topic, in order to prioritise the CA's supervisory responsibilities towards the sector.

7 Collaboration schemes

7.1 Public-private collaboration

There are various collaboration schemes across EU in the Energy sector when implementing the NIS Directive. In particular, the engagement and collaboration between the national authorities and the private sector differentiates in each MS. The table below provides an overview of the approaches in different countries as the respondents provided them.

Table 8 - Collaboration with private sector

Austria	On a general level, the Cyber Security Platform (CSP) which is administered by the Federal Chancellery is the main forum for private public dialogue. Apart thereof, energy sector representatives, experts and operators were consulted in several meetings specifically convened to work out the essential services and notification requirements.
Czech Republic	Formally (officialy) and unformally too.
Germany	For that purpose, there is a UP KRITIS Public-Private Partnership for Critical Infrastructure Protection.[13]
Denmark	Several workshops and face-to-face meetings with the oil sector.
Estonia	Offering services like technical and end user awareness trainings, penetration testing, risk management trainings, information sharing groups etc. Exercises with state and administrative supervision.
Finland	Energy authority (NCA) informed OES's of their role and responsibilities.
France	ANSSI exchanges directly with private operators at different stages of the process. In the designation process in France, a first step is to issue a letter of intention to each potential OES. This steps is always taken after previous informal contact between ANSSI and the operator. This letter indicates that the operator is approached for OES designation and asks if they have any comments about this designation, as well as the countries where they deliver an essential service operated from France.
Italy	The Ministry of Economic Development was already a main actor in the energy sector before the transposition of the NIS Directive. For instance, it grants the permits to the energy sector operators and is responsible for the security of the energy supply. Therefore, the

[13] See https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf;jsessionid=BA337A22C25854B7C9E3249A26451477.1_cid320?__blob=publicationFile

	private energy sector operators were already part of the Ministry constituency and were easily engaged.
Luxembourg	When the national law will be affective and prior to the official designation by the ILR, candidate OES will be informed during live meeting sessions about the identification methodology, the final findings, the security, reporting and notification requirements of the law and the way forward (support and future tools that will provided for risk assessment, reporting and notification, timing).
Latvia	Ministry of Economics was already the responsible authority for the development and implementation of energy sector policy, and collaboration with operators of energy sector was already made prior to the implementation of the NIS Directive. The Ministry of Economics identified OES based on the established criteria and then informed them about their status and responsibilities.
Netherlands	In cooperation with the relevant sector stakeholders, the ministry of Economic Affairs identified the relevant OES, which were included in a ministerial Decree. In addition, the ministry and relevant sector stakeholders developed together the applicable thresholds for the notification of incidents. Collaboration within the energy sector existed already before 2018, mainly via in working groups with sector organisations and the national cybersecurity center.
Poland	The private energy sector operators were engaged within the consultation process of the ordinance of 11 September 2018 on the list of essential services and thresholds of significance of the disruptive effect of an incident on the provision of essential services.
Portugal	The private sector OES in the energy sector for the subsectors of electricity, gas and oil were identified to be under the frame of Law 46/2018, of August 13 which transposes the NIS Directive to the Portuguese legal order and implementing regulations. The supervision of the application of the implementing regulations on security requirements and requirements for the notification of incidents as done by the OES is under the frame of exclusive competences of the Portuguese National Cybersecurity Centre as the National Cybersecurity Authority. The collaboration with the OES in the private sector is done either by direct approach of the National Cybersecurity Centre or with the cooperation of the national sectorial authorities when considered necessary.
Spain	The National Center for Infrastructure Protection and Cybersecurity of the Ministry of Home Affairs as National Energy authority (NCA) inform OES's of their role and responsibilities.
Sweden	The energy CA have had a dialogue with potential operators continuously during the process, mainly through the trade organizations, ending up with a series of formal referrals from the NCA towards the end of the process and announcement of 2nd

	legislation. The NCA has organized all the sectorial CA with collective work and discussions regarding all aspects of the implementation. The energy CA has coordinated with the other two regulatory agencies for the energy sector in Sweden, in order to get the best situational awareness and not to duplicate any regulations or disproportionately add to the administrative burden for the OES.
United Kingdom	BEIS, HSE and Ofgem work together to co-ordinate communications with OES, to ensure they were aware of the NIS Regulations and the designation thresholds. We use established industry groups to deliver events and communications, to support and co-ordinate specific NIS areas of work and topics of interest. We also attend industry events e.g. trade associations, and conferences. We work closely with the National Cyber Security Centre who plan and host some of these. We typically use email and teleconferences otherwise to communicate with single OES where there is an issue or topic for discussion.

7.2 EE – ISAC

The European Energy - Information Sharing & Analysis Centre (EE-ISAC)[14] is an industry-driven, information sharing network of trust. Both private utilities and solution providers and (semi) public institutions such as academia, governmental and non-profit organizations share valuable information on cyber security & cyber resilience.

EE-ISAC enables the European utility industry in many different ways. It facilitates long lasting relationships of trust with partners across the entire value chain where all involved industry partners and suppliers benefit from open dialogues. In addition, EE-ISAC supports analysis by sharing both real-time data & analysis within small-scale trust-circles so they can learn from their peer's experiences with grid security incidents and cyber breaches. Furthermore, it compares and evaluates security solutions, both from a technical as well as an operational viewpoint.

In particular, EE-ISAC Members share:

- real-time security data & analysis
- reports on security incidents and cyber breaches
- technical & operational experiences with applied security solutions
- lessons learned from past security issues
- future challenges, security outlooks & warnings

In the context of information sharing, It is important to mention also the existence of national energy sector-related ISACs. An inventory of Identified ISACs in the Energy sector is available in the Annex C of the ENISA Report on Cyber Security Information Sharing in the Energy Sector.[15]

[14] http://www.ee-isac.eu/
[15] https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

7.3 Sector Specific CSIRTs

According to the ENISA CSIRTs map and the ENISA Report on Cyber Security Information Sharing in the Energy Sector there have been identified CSIRTs existing in the Energy in Europe[16]. The countries that seem to have a sector specific CSIRT for the Energy sector are Austria, Norway and UK. Below we present a short description for each one of them.

Austrian Energy CERT (AEC)[17] is the CERT for the Austrian energy industry and plays an important role in increasing the resilience against cyberattacks in the Austrian energy industry. AEC is a Member of the CSIRTs network and its aim is the strengthening of the IT security expertise for the energy sector.[18]

Main energy operators in Italy have a CERT. In particular, Enel CERT[19], has the mission to support and protect Enel, from intentional and malicious attacks that would hamper its constituency. Enel CERT's activities cover prevention, detection, response and recovery.[20]

KraftCERT (Norwegian energy sector CERT)[21] was created after an initiative from NorCERT and Norwegian Water Resources and Energy Directorate (NVE) as a tool to create support for the entire power industry in preventing and handling security incidents.

For further information on other CSIRTs in the Energy sector there is a list presented in the Annex C of the ENISA Report on Cyber Security Information Sharing in the Energy Sector.[22]

7.4 Electricity Coordination Group

The Electricity Coordination Group (ECG) was established by the Commission in 2012. Its tasks are to serve as a platform for the exchange of information and coordination of electricity policy measures having a cross-border impact and for the exchange of experiences, best practices and expertise and also to assist the Commission in designing its policy initiatives. It should also facilitate the exchange of information and cooperation regarding security of supply in electricity, including generation adequacy and cross-border grid stability.

[16] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#constituency=Energy
[17] http://www.energy-cert.at
[18] This includes Security Incident Management, conducting trainings, attending international cyber exercises or helping in the creation of security concepts for the Austrian energy industry.
[19] https://cert.enel.com/en.html
[20] The Enel CERT profile is defined in the RFC 2350 document.
[21] https://www.kraftcert.no
[22] https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

7.5 Gas Coordination Group

In 2004, the Gas Coordination Group was created to facilitate the coordination of measures concerning the security of gas supply. The Group is composed of representatives of MS as well as of consumers and industry (e.g. infrastructure operators, gas and electricity suppliers). Among the tasks of the Gas Coordination Group, it shall assist the Commission in a number of issues, such as with all information relevant to the security of gas supply at national, regional and Union level and best practices and possible guidelines to all the parties concerned.

7.6 Oil Coordination Group

The Coordination Group for oil and petroleum products (in short, Oil Coordination Group) was set up as a standing consultative group in 2009[23]. This Group took over the activities of the "Oil Supply Group", which was created as a crisis *ad hoc* group in 1973[24] and had been meeting on a regular basis since 2003. The Group analyses the security of oil supply and facilitates the coordination of actions among Member States and with the Commission, in particular in case of a major oil disruption, by assessing the situation and coordinating the release of stocks or other relevant measures (e.g. demand restraint, information campaigns, etc). It is also a useful forum to discuss issues related to the implementation of the acquis and cross-cutting topics related to EU energy security.

7.7 European Union Offshore Oil and Gas Authorities Group

The European Union Offshore Oil and Gas Authorities Group (EUOAG)[25], was established by Commission Decision 18/07 of 2012. The EUOAG facilitates the exchange of knowledge, experience and information between the Commission and Member State's experts, industry associations and trade unions on all matters relating to major accident prevention and response in offshore oil and gas operations. It promotes the shaping and application of best safety practices in the EU offshore oil and gas sector, as well as improves and aligns the regulatory oversight and the cooperation between Member State authorities. The European Commission chairs the group and where relevant invites representatives from other sectors of the industry, trade unions, third countries, academia, research organisations, NGOs, or relevant Union Agencies.

[23] By Article 17 of Council Directive 2009/119/EC of 14 September 2009, imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products, OJEU L 265, p.9.
[24] Council Directive 73/228/EEC of 24 July 1973, on measures to mitigate the effects of difficulties in the supply of crude oil and petroleum products, OJEU L 228, p. 1.
[25] https://euoag.jrc.ec.europa.eu/

8 Security measures for OES in the energy sector

The European Union's prosperity and security hinges on a stable and abundant supply of energy. As energy is a vital part of Europe's economy and of modern lifestyles, European citizens expect uninterrupted flows of energy and access to energy sources. Numerous policies have been introduced to secure and create a European sustainable energy network, like the NIS Directive, which distinguishes the subsectors of Electricity, Oil and Gas for the Energy sector, the Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas supply or the Regulation (EU) 2019/941 on risk preparedness in the electricity sector. Additionally, the European Commission adopted in April 2019 a sector-specific guidance[26] that identifies the main actions required to preserve cybersecurity and be prepared to possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies.The table below lists international standards and good practices applicable across all the Energy subsectors of interest. It is the outcome of the conducted desktop research and it is not an all-inclusive table, as it is mainly based on bibliography.

Table 9 - International standards and good practices applicable across the Energy sector

STANDARDS	GOOD PRACTICES
• **ISO 27001** Information technology — Security techniques — Information security management systems — Requirements • **ANSI/ISA, Series "ISA-62443**: Security for industrial automation and control system" • **NIST Framework for Improving Critical Infrastructure Cybersecurity**	• Detailed Measures – Cybersecurity for Industrial Control Systems – ANSSI (France) • Good Practice Guide Process Control and SCADA Security – CPNI • AMI System Security Requirements updated – UCAIUG: AMI-SEC-ASAP • BDEW whitepaper – Requirements for secure controls and telecommunications systems – Bundesverband der Energie- und Wasserwirtschaft • Information security baseline requirements for process control, safety and support ICT systems – OLF • Twenty Critical Controls for Effective Cyber Defence: Consensus Audit Guidelines • Catalog of Control Systems Security: Recommendations for Standards Developers – USA DHS • 21 Steps to Improve Cyber Security of SCADA Networks – US DOE

According to the feedback ENISA collected from Energy operators for an internal study conducted in 2017, the most frequently applicable standards for the energy sector, in its entirety, are ISO 27001 and ISA/IEC 62443. Following, electricity, oil and gas specific standards and good practices along with the mapping to the security measures are presented.

[26] Recommendation C(2019)240 final and staff working document SWD(2019)1240 final

8.1 Electricity

The table below lists international standards and good practices applicable across the Electricity subsector.

Table 10 - International standards and good practices applicable across the Electricity subsector

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Electricity	• **NIST SP800-82** Guide to Industrial Control Systems (ICS) Security • **ISO 27019** -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry • **NERC CIP Series** "Critical Infrastructure Protection Cyber Security": CIP–002 to CIP-011. • IEEE STANDARD 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security • IEC 61850 - Power Utility Automation	• Cybersecurity model electricity subsector cybersecurity capability maturity model (es-c2m2) - U.S. Department of Energy • NISTR 7628 - Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements • ENISA Appropriate security measures for Smart Grids - ENISA • Best practices for handling smart grid cyber security - California Energy Commission

The following table illustrates the mapping of security measures with the three following Electricity specific standards and the recently published EC recommendation:

- **NIST SP 800-82 Rev. 2** (Guide to Industrial Control Systems (ICS) Security) provides guidance on how to secure Industrial Control Systems (ICS) and is usually followed by EU operators as a good practice;
- **ISO 27019** is the information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry;
- **NERC CIP** (North American Electric Reliability Corporation Critical Infrastructure Protection) is a set of requirements for North America's bulk electric system. Nevertheless, it is followed as well by EU operators that extend their business in U.S.
- **COMMISION RECOMMENDATION on cybersecurity in the energy sector** of 3.4.2019 [27]

27 https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

Table 11 - Mapping of security measures with electricity subsector specific standards and EC recommendation

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
Part 1 – Governance and Ecosystem						
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	3. ICS Risk Management and Assessment 4.5 Implement an ICS Security Risk Management Framework 6.1 Executing the Risk Management Framework Tasks for Industrial Control Systems 6.2.14 Risk Assessment	14.1.4 Business continuity planning framework 6.2.1 Identification of risks related to external parties	CIP-002-3 Critical Cyber Asset Identification CIP-002-5 BES Cyber System Categorization CIP-010-2Table R3 –Vulnerability Assessments	**Cascading effects** 8(a)(b)(c) **Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(c)
		Information system security policy	3.3.1 Policy and Procedure Vulnerabilities	5. Security policy	CIP-003-6 Cyber Security - Security Management Controls CIP-011-2Table R1 –Information Protection	**Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(c)
		Information system security accreditation	6.1.1 Security Assessment and Authorization	–	–	**Cascading effects** 8(a) **Real-time requirements** 4(b)
		Information system security indicators	3.3 Potential ICS Vulnerabilities	–	–	**Real-time requirements** 4(c) **Legacy systems** 12(a)(d)
		Information system security audit	6.2.3 Audit and Accountability	12.4 Logging and Monitoring 15.3 Information	CIP-003-6— Cyber Security —Security Management Controls, Compliance	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d)

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
				systems audit considerations	Monitoring Process	**Real-time requirements** 4(a)(c)
		Human resource security	6.2.1 Personnel Security	8. Human resource security	CIP-004 Cyber Security - Personnel & Training CIP-004-6 Table R1 –Security Awareness Program CIP-004-6Table R3–Personnel Risk Assessment Program	
		Asset Management				**Real-time requirements** 4(c) **Legacy systems** 12(d)
1.2	**Ecosystem Management**	Ecosystem mapping	–	6.2 External parties	–	**Cascading effects** 8(c) **Legacy systems** 12(f)(g)
		Ecosystem relations	–	6.2.2 Addressing security when dealing with customers 6.2.3 Addressing security in third-party agreements	–	**Real-time requirements** 4(b) **Cascading effects** 8(c) **Legacy systems** 12(f)(g)
Part 2 – Protection						
2.1	**IT Security Architecture**	Systems configuration	6.2.5 Configuration Management	11.4.4 Remote diagnostic and configuration port protection	CIP-007-6Table R1–Ports and Services CIP-010-2Table R1 – Configuration Change Management	**Legacy systems** 12(e) **Real-time requirements** 4(c)(d)(e)

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
		System segregation	5.1 Network Segmentation and Segregation 5.5 Network Segregation	10.6 Network security management 11.4.5 Segregation in networks	CIP-005-5 Table R1 – Electronic Security Perimeter	**Legacy systems** 12(e) **Real-time requirements** 4(e)
		Traffic filtering	6.3.3 Audit and Accountability 6.1.1 Security Assessment and Authorization	10.10.2 Monitoring system use	–	**Legacy systems** 12(b)(c) **Cascading effects** 8(c) **Real-time requirements** 5(b)
		Cryptography	6.3.4.1 Encryption	12.3 Cryptographic controls 15.1.6 Regulation of cryptographic controls	CIP-011-2 Cyber Security - Information Protection	**Real-time requirements** 4(b), 5(a)(b)
2.2	**IT Security Administration**	Administration accounts	6.3.1 Identification and Authentication	11.5 Operating system access control	CIP-007-6Table R5 –System Access Control CIP-004-6Table R4–Access Management Program	**Legacy systems** 12(a)(c) **Real-time requirements** 5(b)
		Administration information systems	–	10.10.4 Administrator and operator logs	CIP-007-6Table R5 –System Access Control CIP-004-6Table R4–Access Management Program	**Cascading effects** 8(c) **Legacy systems** 12(c) **Real-time requirements** 5(b)
2.3	**Identity and access management**	Authentication and identification	6.3.2 Access Control 6.3.1 Identification and Authentication	11. Access control	CIP-007-6Table R5 –System Access Control CIP-004-6Table R4–Access Management Program	**Cascading effects** 8(c) **Legacy systems** 12(c) **Real-time requirements** 4(a)(b)(e), 5(a)(b)
		Access rights	6.3.2 Access Control	11. Access control	CIP-007-6Table R5 –System Access Control CIP-004-6Table R4–Access Management Program	**Cascading effects** 8(c) **Legacy systems** 12(c)

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
					CIP-004-6Table R5–Access Revocation	**Real-time requirements** 4(b),5(a)(b)
2.4	**IT security maintenance**	IT security maintenance procedure	6.2.9 Maintenance	9.2.4 Equipment maintenance 12 Information systems acquisition, development and maintenance	CIP-007-6Table R2 –Security Patch Management	**Legacy systems** 12(a)(d)(e)(f) **Real-time requirements** 4(a)(c)
		Remote access	6.3.2 Access Control 6.3.1 Identification and Authentication	11.4 Network access control 11.4.4 Remote diagnostic and configuration port protection	CIP-005-5 Table R2 – Interactive Remote Access Management	**Cascading effects** 8(c) **Legacy systems** 12(e)(f) **Real-time requirements** 4(b),5(a)(b)
2.5	**Physical and environmental security**	Physical and environmental security	6.2.2 Physical and Environmental Protection 6.2.7 Media Protection	9. Physical and environmental security 9.2 Equipment security	CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems CIP-014-1 Physical Security	**Cascading effects** 8(c) **Real-time requirements** 4(a)(c)
Part 3 - Defence						
3.1	**Detection**	Detection	3.3 Potential ICS Vulnerabilities	–	CIP-007-6 Table R4 –Security Event Monitoring CIP-007-6 Table R3 –Malicious Code Prevention	**Legacy systems** 12(a)(b)(c)(f) **Real-time requirements** 4(e) **Cascading effects** 8(c)
		Logging	5.16 Monitoring, Logging,and Auditing	11.5.1 Secure log-on procedures	CIP-007-6 Table R4 –Security Event Monitoring	**Legacy systems** 12(b)(c)(f) **Real-time requirements** 4(c)(e) **Cascading effects** 8(c)

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
		Logs correlation and analysis	5.16 Monitoring, Logging, and Auditing	10.2.2 Monitoring and review of third party services 10.10.2 Monitoring system use	CIP-007-6 Table R4 –Security Event Monitoring	**Legacy systems** 12(a)(b)(c)(f) **Real-time requirements** 4(c)(e)
3.2	**Computer security incident management**	Information system security incident response	5.17 Incident Detection, Response, and System Recovery	13 Information security incident management	CIP-008-5 Table R1 –Cyber Security Incident Response Plan Specifications CIP-008-5 Table R2 –Cyber Security Incident Response Plan Implementation and Testing	**Cascading effects** 8(b) **Legacy systems** 12(b)(c)(f)
		Incident report	6.2.8 Incident Response	13.1 Reporting information security events and weaknesses	CIP-008 Cyber Security - Incident Reporting and Response Planning CIP-001 Sabotage Reporting	**Cascading effects** 8(b) **Legacy systems** 12(c)
		Communication with competent authorities	–	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups	CIP-008-5 Table R3 –Cyber Security Incident Response Plan Review, Update, and Communication	**Cascading effects** 8(c)
Part 4 - Resilience						
4.1	**Continuity of Operations**	Business continuity management	6.1.2 Planning 6.1.3 Risk Assessment 6.1.5 Program Management	14. Business continuity management	CIP-013-1 Cyber Security - Supply Chain Risk Management	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d)(f) **Real-time requirements** 4(a)(b)(c)(d)
		Disaster recovery management	6.2.3 Contingency Planning	14.1 Information security aspects of business continuity management	CIP-009-1 Cyber Security - Recovery Plans for Critical Cyber Assets CIP-009-5 Cyber Security - Recovery Plans	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(b)(d)

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP	EC RECOMMENDATIONS
					for BES Cyber Systems	**Real-time requirements** 4(a)(b)(c)(d)(e)
4.2	**Crisis Management**	Crisis management organization	6.2.6 Contingency Planning	14.2 Essential emergency services	CIP-009-6Table R1 –Recovery Plan Specifications CIP-009-6Table R2 –Recovery Plan Implementation and Testing	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d)(f) **Real-time requirements** 4(a)(b)(c)(d)(e)
		Crisis management process	6.2.6 Contingency Planning	14.2.1 Emergency communication	CIP-009-6Table R3 –Recovery Plan Review, Update and Communication	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(b)(c)(d)(e)

8.2 Oil & Gas

Protection of the Oil and Gas subsector within EU, but also globally, is considered of highly strategic and economic importance in the light of emerging hybrid threats targeting energy utilities.

The table below lists international standards and good practices applicable across the Oil and Gas sectors of interest.

Table 12 - International standards and good practices applicable across the Oil and Gas subsectors

SUB-SECTORS	STANDARDS	GOOD PRACTICES
Oil & Gas	• Chemical Facility Anti-Terrorism Standards (CFATS)	• API STD 1164 - Pipeline SCADA Security • Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2) • Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA)

The most known security framework related to the Oil and Gas subsector is the Chemical Facility Anti-Terrorism Standards (CFATS) program, which is a risk-based performance program that sets the standards for security at the United States highest risk chemical facilities. The CFATS program covers equally both subsectors, while it identifies and regulates ensuring that high-risk chemical facilities have in place security measures to reduce the risks

posed against these chemicals. However, the CFATS program does not consider cybersecurity, but safety.

The table below illustrates the mapping of security measures with Oil and Gas specific good practices and the EC recommendation[27]:

- **API STD 1164** - Pipeline SCADA Security good practice provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security.
- **ONG-C2M2** good practice assist oil and natural gas organizations of all types to evaluate and make improvements to their cybersecurity programs.
- **COMMISION RECOMMENDATION on cybersecurity in the energy sector** of 3.4.2019

Table 13 - Mapping of security measures with Oil and Gas subsector specific standards and EC recommendation

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
Part 1 – Governance and Ecosystem					
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	3.4 Risk and Vulnerability Assessment 3.8 Asset Inventory/Categorizing/ Tracking	Risk Management Threat and Vulnerability Management	**Cascading effects** 8(a)(b)(c) **Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(c)
		Information system security policy	1.3 Roles and Responsibilities 3.1 Security Plan 3.3 Security Policies	Cybersecurity Program Management	**Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(c)
		Information system security accreditation	–	–	**Cascading effects** 8(a) **Real-time requirements** 4(b)
		Information system security indicators	–	–	**Real-time requirements** 4(c)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
					Legacy systems 12(a)(d)
		Information system security audit	7.2.2.6 File Audit and Control	–	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(c)
		Human resource security	3.2 Personnel 5.12 Personnel Administration	Workforce Management	
		Asset Management			**Real-time requirements** 4(c) **Legacy systems** 12(d)
1.2	**Ecosystem Management**	Ecosystem mapping	7.3.4 Connections to Third Parties for Support	Supply Chain and External Dependencies Management	**Cascading effects** 8(c) **Legacy systems** 12(f)(g)
		Ecosystem relations	3.11 Procurement 7.3.4 Connections to Third Parties for Support	Supply Chain and External Dependencies Management	**Real-time requirements** 4(b) **Cascading effects** 8(c) **Legacy systems** 12(f)(g)
Part 2 – Protection					
2.1	**IT Security Architecture**	Systems configuration	3.9 Change Management 3.10.1 System Hardening 3.10.2 Software Patching and Updates	Asset, Change, and Configuration Management	**Legacy systems** 12(e) **Real-time requirements** 4(c)(d)(e)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
			3.10.3 Proper Disposal of Equipment and Media. 5.9 Disabled Non-Required Services 5.10 Operating System Tools 7.1.6 Defense in Depth 7.2.2.4 White Listing 7.2.2.5 Host/Endpoint Security 7.2.2.6 File Audit and Control 8.2.1 Network Protocols		
		System segregation	7 Network Design/Security and Data Interchange 7.1 Network Design 7.1.1 Interconnected Business and SCADA Networks 7.1.2 Communication Demarcation Points 7.1.3 Firewalls 7.1.4 Demilitarized Zone (DMZ) 7.1.5 Dual-Homed Computers 7.1.7 Firewall Management 7.1.8 Virtualization 7.1.8.2 Hypervisor and Virtual Machine Services 7.1.8.3 Networking 7.1.8.4 Resource Allocation 7.2 Network Management 7.3.1 Connections Between the SCADA Control Center Operational Facilities, Data Center, and Telecommunications Center 7.3.2 Connections Between the SCADA	–	**Legacy systems** 12(e) **Real-time requirements** 4(e)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
			System and Business Networks 7.3.3 Connections Between the SCADA System and Business Partners SCADA Systems 7.3.5 Internet and Business Network Access 7.3.6 Voice Over IP/IP telephony (VoIP/IPT) 7.3.7 Instant Messaging (IM) 7.3.8 Wireless Networking 7.3.9 Audio/Video Conferencing 7.3.10 Video Surveillance 7.3.11 Cloud Computing 8 Field Communication 8.1 Field Device Technology		
		Traffic filtering	7.1.7 Firewall Management 7.1.8.3 Networking 7.3 Data Interchange	–	**Legacy systems** 12(b)(c) **Cascading effects** 8(c) **Real-time requirements** 5(b)
		Cryptography	7 Network Design/Security and Data Interchange 7.3 Data Interchange 8.2.2 Encryption of Data on Accessible Paths	–	**Real-time requirements** 4(b), 5(a)(b)
2.2	**IT Security Administration**	Administration accounts	5.3 User Accounts 5.4 Operating System Accounts 5.5 SCADA Accounts	Identity and Access Management	**Legacy systems** 12(a)(c) **Real-time requirements** 5(b)
		Administration information systems	5.4 Operating System Accounts 5.5 SCADA Accounts	–	**Cascading effects** 8(c)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
					Legacy systems 12(c) **Real-time requirements** 5(b)
2.3	**Identity and access management**	Authentication and identification	5.3 User Accounts 5.6 Password Controls 5.7 Multi-factor Authentication 5.8 Biometrics	Identity and Access Management	**Cascading effects** 8(c) **Legacy systems** 12(c) **Real-time requirements** 4(a)(b)(e), 5(a)(b)
		Access rights	5.1 Restricted Access 5.2 Logical Access Control to Control Systems and Control Networks 5.11 Device Access 7.1.8.1 Permissions 7.2 Network Management 8.2 System Access 8.2.3 Casual User Access to Network	Identity and Access Management	**Cascading effects** 8(c) **Legacy systems** 12(c) **Real-time requirements** 4(b),5(a)(b)
2.4	**IT security maintenance**	IT security maintenance procedure	3.5 New or Replacement System Security Design 3.10 Operating System and Application Updates 3.10.2 Software Patching and Updates 3.10.3 Proper Disposal of Equipment and Media. 9 Annual Review, Reassessment, and Update	–	**Legacy systems** 12(a)(d)(e)(f) **Real-time requirements** 4(a)(c)
		Remote access	5.1 Restricted Access 5.2 Logical Access Control to Control Systems and Control Networks 5.11 Device Access	–	**Cascading effects** 8(c) **Legacy systems** 12(e)(f)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
			7.2 Network Management 7.3.4 Connections to Third Parties for Support 8.2.4 Remote Access to SCADA Components 8.2.5 Dial-up Modem Access for Maintenance		**Real-time requirements** 4(b),5(a)(b)
2.5	**Physical and environmental security**	Physical and environmental security	4 Physical Security	–	**Cascading effects** 8(c) **Real-time requirements** 4(a)(c)
Part 3 - Defence					
3.1	**Detection**	Detection	7.2.2 Network Security 7.2.2.1 Intrusion Detection and Prevention Systems (IDPS) 7.2.2.2 Malware Detection and Avoidance	Situational Awareness	**Legacy systems** 12(a)(b)(c)(f) **Real-time requirements** 4(e) **Cascading effects** 8(c)
		Logging	7.2.1 Network Monitoring & Advanced Threat Protection 7.2.2 Network Security	Situational Awareness	**Legacy systems** 12(b)(c)(f) **Real-time requirements** 4(c)(e) **Cascading effects** 8(c)
		Logs correlation and analysis	7.2.2 Network Security 7.2.2.1 Intrusion Detection and Prevention Systems (IDPS) 7.2.2.3 Security Information and Event Management (SIEM)	–	**Legacy systems** 12(a)(b)(c)(f) **Real-time requirements** 4(c)(e)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
3.2	**Computer security incident management**	Information system security incident response	3.7 Incident Response Plan (IRP)	Event and Incident Response, Continuity of Operations	**Cascading effects** 8(b) **Legacy systems** 12(b)(c)(f)
		Incident report	–	Event and Incident Response, Continuity of Operations	**Cascading effects** 8(b) **Legacy systems** 12(c)
		Communication with competent authorities	6 Information Distribution 6.1 Confidential 6.2 Restricted 6.3 Internal Use Only 6.4 Public	Information Sharing and Communications	**Cascading effects** 8(c)
Part 4 - Resilience					
4.1	**Continuity of Operations**	Business continuity management	3.6 Business Continuity Plan (BCP)	Event and Incident Response, Continuity of Operations	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d)(f) **Real-time requirements** 4(a)(b)(c)(d)
		Disaster recovery management	–	–	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(b)(d) **Real-time requirements** 4(a)(b)(c)(d)(e)
4.2	**Crisis Management**	Crisis management organization	–	–	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d)(f) **Real-time requirements** 4(a)(b)(c)(d)(e)

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2	EC RECOMMENDATIONS
		Crisis management process	–	–	**Cascading effects** 8(b)(c) **Legacy systems** 12(a)(d) **Real-time requirements** 4(a)(b)(c)(d)(e)

Finally, according to the input gathered by Oil and Gas operators in EU for an internal study of ENISA[28], the most applicable information security standards are ISO 27001, NIST Cybersecurity Framework and ISA/IEC 62443.

[28] Feedback was collected through interviews with operators.

9 Incident reporting for OES in the energy sector

9.1 Electricity

9.1.1 Description sectorial initiatives

The Risk Preparedness Regulation (Regulation (EU) 2019/941[29]) provides risk preparedness and more resilient electricity systems in Europe through:

a) The identification of possible electricity crisis scenarios at national and regional levels, using a common methodology to assess at least the risks of rare and extreme natural hazards (e.g. extreme weather conditions), accidental hazards (e.g. outages beyond the N-1 security criterion) and consequential hazards, including consequences of malicious attacks, like cyber-attacks,
b) On the basis of the electricity crisis scenarios identified, Member States have to prepare and publish "risk-preparedness plans", which contain the national and regional measures to be taken in case of a crisis;
c) The Regulation ensures that markets can work as long as possible. The intervention in the market with measures such as electricity export bans or forced interruption of electricity supply to customers, could be taken only as "last resort";
d) The Regulation sets a framework to ensure that Member States prevent and manage crisis situations in cooperation with each other in a spirit of solidarity. Member States need to agree in advance on bilateral and regional measures to assist each other during an electricity crisis. The assistance shall be subject to fair compensation. Further, this Regulation requires MS (the competent Authority) to inform other MS and the Commission when it declares an emergency.

In case of an electricity crisis, the competent authority[30] of the Member State affected, after consulting with the TSO concerned, declares an electricity crisis and informs the competent authorities of the Member States within its region[31] and, where they are not in the same region, the competent authorities of directly connected Member States as well as the Commission. The Member State declaring the crisis has to inform the others on the causes of the deterioration of the electricity supply, the reasons for declaring the crisis, the measures planned or taken to mitigate it and the need for any assistance from other Member States.

In the area of transmission system operators (TSOs), the ENTSO-E is responsible for the development of two new methodologies[32] related to the Risk Preparedness Regulation and the adoption of a common incident classification scale (point 3.a, Article 8, Regulation EC

[29] Regulation (EU) 2019/941 of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC; OJ L158 14.6.2019, p.1-21
[30] National governmental or regulatory authority designated by each Member State for carrying out the tasks contained in the Risk Preparedness Regulation.
[31] As defined in Articles 2 and 22 of the Risk Preparedness Regulation.
[32] Methodology for identifying regional electricity crisis scenarios and Short-term and Seasonal Adequacy Assessment Methodology

714/2009[33]). Furthermore, ENTSO-E defines such scale in its *Incidents Classification Scale (ICS) Methodology*[34], which concerns with the following points:

- The Incidents Classification Scale has to be used by each TSO of the ENTSO-E area.
- Each TSO will have to report grid and system incidents on a four degrees' scale (0 to 3) corresponding to incidents of increasing seriousness up to a general Europe-wide incident.
- Each TSO has to define its own internal organization to use the Incidents Classification Scale.
- Depending on the type of incident, TSO will exchange data to enable each TSO to investigate.
- Generally, reporting will have to be done by the TSO in whose system the incident has occurred and all other TSO affected by the original incident – if the consequences in their own systems reach at least Scale 0.

The ICS methodology is concerned with ***incidents that are reported only if the effects or initiating events occur in the Transmission Network with an operating voltage at or above 220 kV***. ENTSO-E provides a full list of outcomes that are considered disturbances within the electricity transmission networks. The causes that might produce the outcomes are not referred to within the document, leaving room for any kind of root causes (cyber security included also) to be considered. All incidents above certain thresholds (as described in the document) are reported to ENTSO-E for further analysis.

Note that the current incident reporting scheme focuses only on TSO, not also to suppliers and distribution operators. As distribution operators have a fairly limited geographical area of operation, there was no need for an EU level approach. Policies in this area might reside at the MS level. Nothing was identified in the area of suppliers.

9.1.2 Parameters and thresholds

According to the ICS Methodology, the Incidents Classification Scale[35] consists of four levels (from 0 to 3) of gravity corresponding to incidents of growing seriousness up to a general Europe wide incident:

- **Scale 0** for anomalies, local incidents; the system remains in normal state;
- **Scale 1** for noteworthy incidents, probability of wide area incidents; the system is in alert state;
- **Scale 2** for extensive incidents; the system is in emergency state;
- **Scale 3** for wide area incidents or major incidents in the control area of one TSO; the system is in blackout state.

For each level, the assessment of different types of consequences or criteria (e.g. incidents leading to frequency degradation, incident on load, loss of tools and facilities, black out, etc.) determines the severity of the occurred incident. The following figure (extracted from the Incidents Classification Scale Methodology) shows the different levels and the corresponding

[33] Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003, OJ L 211, 14.8.2009, p. 15–35. http://data.europa.eu/eli/reg/2009/714/oj

[34] European Network of Transmission System Operators for Electricity (ENTSO-E), Incidents Classification Scale Methodology, May 2014. See: https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf

[35] Incident Classification Scale Methodology, ENTSO-E.

severity impact in terms of types of affected services or systems (e.g. Incidents on Loans, Incidents on Transmission Network elements, Loss of tools and facilities, etc.).

Based on the description of each type of incident and the corresponding severity criteria, the incident classification takes into account the parameters reported in the table that follows.

Figure 11- Incident Classification Scale General Overview

Scale 0 Anomaly		Scale 1 Noteworthy incident		Scale 2 Extensive incidents		Scale 3 Wide area incident or major incident / 1 TSO	
Priority / Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Priority - Short definition (Criterion short code)	
#20	Incidents leading to frequency degradation (F0)	#11	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Blackout (OB3)
#21	Incidents on transmission network elements (T0)	#12	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
#22	Incidents on power generating facilities (G0)	#13	Incidents on transmission network elements (T1)	#4	Incidents on transmission network elements (T2)		
#23	Violation of standards on voltage (OV0)	#14	Incidents on power generating facilities (G1)	#5	Incidents on power generating facilities (G2)		
#24	Reduction of reserve capacity (RRC0)	#15	N-1 violation (ON1)	#6	N violation (ON2)		
#25	Loss of tools and facilities (LT0)	#16	Separation from the grid (RS1)	#7	Separation from the grid (RS2)		
		#17	Violation of standards on voltage (OV1)	#8	Violation of standards on voltage (OV2)		
		#18	Reduction of reserve capacity (RRC1)	#9	Reduction of reserve capacity (RRC2)		
		#19	Loss of tools and facilities (LT1)	#10	Loss of tools and facilities (LT2)		

Figure 12 - Incident reporting parameters and thresholds

Parameters	Unit of measure	Threshold (examples if any)	Observations
Number of users			This information is captured by the criticality of the transmission network
Duration	minutes	15mins-20mins	It depends on the country
Alert State Trigger Time	minutes	5mins-10mins	It depends on the country
Time to Restore Frequency	minutes	15mins-20mins	It depends on the country
Geographical spread			Scale 0 – Scale 3 implies different spread from Local to Wide Area Incident or major incident affecting one TSO

Parameters	Unit of measure	Threshold (examples if any)	Observations
Standard Frequency Range	mHz	50% of Maximum Steady State Frequency Deviation	The threshold is expressed in percentage of Maximum Steady State Frequency Deviation; Different levels are specified for each country

9.1.3 Situations where Incident Notification policies can be triggered

The following table reports descriptions of different types of incidents drawn from the Incidents Classification Scale methodology. The different types of incidents highlight how incidents affecting similar services or systems may have different impact level, hence resulting in a different classification.

Subsector	Safety related incidents/occurrences	Incident types related to the disruption of the service	Observations
Incidents on load (L1)	• All Synchronous Areas: Energy Not Supplied (MWh) after disconnection of load representing from 1 to 10% of estimated load of TSO just prior to the time of the incident (MW) where the incident lasted longer than three minutes. A disconnection of load less than 200 MW need not be reported. • Isolated systems: load shedding from 5% to 15% of load at the time of the incident. There is no minimal time duration of disconnection.	Scale 1 Noteworthy Incident	ENTSO-E methodology does not introduce "cyber" as a cause however any of those incidents (and not only), may be due to cyber causes. Although these types of incidents will be reported to the relevant authorities, understanding whether they have a cyber nature requires specific investigations.
Incident on Transmission Network Elements (T1)	Final tripping or manual emergency disconnection of grid equipment from Contingency List [1], other Exceptional Contingencies and Out-of-Range Contingencies (to be indicated in the report) with consequences on Responsibility Area or/and the available cross border transmission capacity. (e.g. final tripping of cross border Tie-Lines or "internal" equipment of one TSO limiting cross border transmission capacity).	Scale 1 Noteworthy Incident	
Degradation in operational conditions – Loss of tools	The TSO has a loss of one or more real time tools and facilities for more than 30 minutes. If all the tools and facilities are lost, this incident must be reported in Scale	Scale 1 Noteworthy Incident	

Subsector	Safety related incidents/occurrences	Incident types related to the disruption of the service	Observations
and facilities (LT1)	2 criteria 7 (paragraph 3.5.8). The referred tools and facilities are: • Facilities and tools for monitoring the system State of the Transmission System, including • State Estimation applications, EAS. • Means for controlling isolators and circuit breakers. • Means of communication with control centres of other TSOs. • Tools for Operational Security Analysis.		
Degradation in Operational Conditions – N Violation (ON2)	There is at least one Wide Area deviation from Operational Security Limits after effects of Remedial Actions.	Scale 2 Extensive Incidents	
Reliability Degradation – Separation from the Grid (RS2)	System incident leading to separation of a significant part from the grid representing at least one TSO Responsibility Area.	Scale 2 Extensive Incidents	
Loss of Tools and Facilities (LT2)	The TSO has a complete loss of all real time tools and facilities for more than 30 minutes. The referred tools and facilities are: • Facilities and tools for monitoring the system State of the Transmission System, including • State Estimation applications, EAS. • Means for controlling isolators and circuit breakers. • Means of communication with control centres of other TSOs. • Tools for Operational Security Analysis.	Scale 2 Extensive Incidents	
Black out	• At least one TSO declares a Blackout State [1]. OR • For all Synchronous Areas: loss of more than 50% of the estimated load in the Responsibility Area just prior to the time of the incident (MW) or • A total absence of voltage in the system lasting for more than 3 minutes and the initiation of restoration plans. • For isolated systems: 70% of load (load-shedding) at the time of the incident or total shut down.	Scale 3	

It was not identified a common incident reporting scheme for cybersecurity in the electricity sector. For TSOs there is a reporting scheme in place, but not with a direct link to cyber security. Having in mind, that Europe has around 2400 DSOs and that smart meter, electric vehicles, renewables and smart devices are directly linked to electricity distribution, there is a need for a common incident reporting scheme.

MS where asked if there are any obligations other obligations than the NIS Directive imposing cyber security and/or incident reporting requirements on energy undertakings. Some MS state that, they had mandatory incident reporting mechanism prior the NIS directive and adopted these regarding the NIS Directive. EE provides, that OES shall inform the competent authority not only if an incident did occur, but also even if an incident can be reasonably presumed. Even if the NIS Directive has not yet been implemented, OES are under a frame of legal report obligations to the Energy sector authorities (PT).

The **Electricity Coordination Group** (ECG) was established by the Commission in 2012. Its tasks are to serve as a platform for the exchange of information and coordination of electricity policy measures having a cross-border impact and for the exchange of experiences, best practices and expertise and also to assist the Commission in designing its policy initiatives. It should also facilitate the exchange of information and cooperation regarding security of supply in electricity, including generation adequacy and cross-border grid stability.

The members of the ECG are MS' authorities, in particular Ministries competent for energy, the National Regulatory Authorities for energy, the ACER and the ENTSO-E.

The ECG meets regularly and in recent meetings it has addressed cybersecurity concerns in the energy sector as well as risks and opportunities of digitalisation.

9.2 Oil & Gas

9.2.1 Description sectorial initiatives

Directive 2013/30/EU[36] (the Offshore Safety Directive) puts in place requirements that enhance safety and environmental protection in relation to offshore oil and gas activities in EU. The main focus of the Directive is to reduce the likelihood of a major accident and increase the effectiveness of response measures in case such accident occurs. Art. 2(1) of the Directive defines: *'major accident' means, in relation to an installation or connected infrastructure:*

a. *an incident involving an explosion, fire, loss of well control, or release of oil, gas or dangerous substances involving, or with a significant potential to cause, fatalities or serious personal injury;*
b. *an incident leading to serious damage to the installation or connected infrastructure involving, or with a significant potential to cause, fatalities or serious personal injury;*
c. *any other incident leading to fatalities or serious injury to five or more persons who are on the offshore installation where the source of danger occurs or who are engaged in an offshore oil and gas operation in connection with the installation or connected infrastructure; or*
d. *any major environmental incident resulting from incidents referred to in points (a), (b) and (c).*

The European Commission has also established through Commission Decision 18/07 of 2012 the European Union Offshore Oil and Gas Authorities Group (EUOAG). The EUOAG facilitates the exchange of knowledge, experience and information between Member State's experts and the Commission, as well as the industry and trade associations where relevant, and helps the shaping and application of best safety practices in the EU offshore oil and gas sector. The EUOAG shall discuss, assist and give its opinions to the Commission on issues such as: *"the occurrence and causes of and responses to major incidents, and events which could have led to major accidents as well as, operational intelligence concerning drilling installations that intend to move between Member States"* (point 3(c), Article 2 of the Commission Decision 18/07 of 2012).

In order to support the implementation of Directive 2013/30/EU, the European Commission has also issued specific regulations to better facilitate the reporting of information related to safety of offshore oil and gas activities. This includes notifications on accidents, incidents and near misses, as well as other relevant information. There are no clauses eliminating the need to report on incidents for which the root cause is a cyber-incident.

The European Commission implementing regulation EU 1112/2014[37] is concerned with determining a common reporting format for sharing and publishing information on major hazard indicators. It identifies specific information that operators and owners of offshore oil and gas installations have to report to the competent authorities of the MS they operate. It also

[36] Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC, OJ L 178, 28.6.2013, p. 66–106. http://data.europa.eu/eli/dir/2013/30/oj

[37] Commission Implementing Regulation (EU) No 1112/2014 of 13 October 2014 determining a common format for sharing of information on major hazard indicators by the operators and owners of offshore oil and gas installations and a common format for the publication of the information on major hazard indicators by the Member States, OJ L 302, 22.10.2014. http://data.europa.eu/eli/reg_impl/2014/1112/oj

identifies specific information that MS will publish and report to the European Commission. Based on the information received from Member States, the Commission then publishes an annual report on the overall levels of safety and environmental protection of the EU offshore oil and gas sector. Operators and owners of offshore oil and gas installations shall submit specific information on any major accident (in accordance with Article 23 of Directive 2013/30/EU) within 10 working days of the event. The European Commission has also created specialized software applications, which can be used by operators and Member States in order to better facilitate the reporting of the above information, namely SyRIO[38] and SIROS[39].

In the area of TSOs, Regulation (EC) No 715/2009[40] defines the ENTSO-G, an organisation having tasks in the area of *"common network operation tools to ensure coordination of network operation in normal and emergency conditions, including a common incidents classification scale, and research plans"* (paragraph 3(a) of Article 8 Tasks of the ENTSO for Gas of Regulation EC 715/2009).

Regulation (EU) 2017/1938 establishes a set of obligations imposed on MS and natural gas undertakings aiming at safeguarding the security of gas supply. Article 11 defines up to three crisis levels to be declared by MS:

(a) early warning level ('early warning'): where there is concrete, serious and reliable information that an event which is likely to result in significant deterioration of the gas supply situation may occur and is likely to lead to the alert or the emergency level being triggered; the early warning level may be activated by an early warning mechanism;

(b) alert level ('alert'): where a disruption of gas supply or exceptionally high gas demand which results in significant deterioration of the gas supply situation occurs but the market is still able to manage that disruption or demand without the need to resort to non-market-based measures;

(c) emergency level ('emergency'): where there is exceptionally high gas demand, significant disruption of gas supply or other significant deterioration of the gas supply situation and all relevant market-based measures have been implemented but the gas supply is insufficient to meet the remaining gas demand so that non-market-based measures have to be additionally introduced with a view, in particular, to safeguarding gas supplies to protected customers ….

The Regulation does not contain a definition of "event" as such so as to cover all possible incidents[41], including safety issues or incidents resulting from geopolitical tensions, extremely high gas demand or cyber attacks, among others. In this regard, Annex IV includes some

[38] https://euoag.jrc.ec.europa.eu/reporting-tools/syrio
[39] https://euoag.jrc.ec.europa.eu/spiros/index.php
[40] Regulation (EC) No 715/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the natural gas transmission networks and repealing Regulation (EC) No 1775/2005, OJ L 211, 14.8.2009, p. 36–54. http://data.europa.eu/eli/reg/2009/715/oj
[41] The first legislative act in the field of security of gas supply contained a threshold for the declaration of emergencies. However, and based on the experience with gas crisis in the EU (e.g. the disruption of gas supplies through Ukraine in 2009), it was decided that such threshold was not suitable to properly reflect diverse types of emergencies.

references to the type of risks that MS have to consider in their Risk Assessments for the gas sector and that include in this new Regulation cyber attacks.

The declaration of any of the above mentioned crisis levels requires its notification to the Commission and to other MS to which the MS in question is directly connected, including the measures that will be put in place. Moreover, MS have to describe in their Emergency Plans (to be developed and updated every 4 years) the mechanisms for the cooperation and sharing of information with other MS in the case of a crisis. The Regulation also envisages the declaration by the Commission of a regional or Union emergency, in which case the Commission shall coordinate the action of the competent authorities and, among others, shall ensure the exchange of information.

In 2004, the **Gas Coordination Group** was created to facilitate the coordination of measures concerning the security of gas supply. The Group is composed of representatives of MS as well as of consumers and industry (e.g. infrastructure operators, gas and electricity suppliers). Among the tasks of the Gas Coordination Group, it assists the Commission in a number of issues, such as with all information relevant to the security of gas supply at national, regional and Union level and best practices and possible guidelines to all the parties concerned.

In case of the declaration of an emergency, natural gas undertakings have to report to the competent authorities on a daily basis, information related to gas supplies and capacities. The new Regulation also provides a legal basis for MS and, indirectly, for the Commission to request information to natural gas undertakings in duly justified situations even before the declaration of an emergency.

It was not identified a common European or International approach for reporting cyber incidents in the Oil and Gas sectors.

9.2.2 Parameters and thresholds

The Directive 2013/30/EU identifies the Information to be included in documents submitted to the competent authority in different situations, in particular:

- Information to be submitted in a report on major hazards for operation of a production installation
- Information to be submitted in a report on major hazards for a non-production installation
- Information to be submitted in respect of a corporate major accident prevention policy
- Information to be provided in an internal emergency response plan.

The Directive 2013/30/EU (Art. 23 completed by Annex IX) also establishes conditions regarding the sharing of information and transparency. More specifically, annex IX provides some types of occurrences that may also cause disturbances in the services offered. The information to be shared by the competent authority and operators and owners shall include information relating to:

a) unintended release of oil, gas or other hazardous substances, whether or not ignited
b) loss of well control requiring actuation of well control equipment, or failure of a well barrier requiring its replacement or repair
c) failure of a safety and environmental critical element
d) significant loss of structural integrity, or loss of protection against the effects of fire or explosion, or loss of station keeping in relation to a mobile installation
e) vessels on collision course and actual vessel collisions with an offshore installation

f) helicopter accidents, on or near offshore installations
g) any fatal accident
h) any serious injuries to 5 or more persons in the same accident
i) any evacuation of personnel
j) a major environmental incident.

No specific parameters or thresholds were identified.

Regulation (EU) 2017/1938 identifies the information that natural gas undertakings have to notify to the MS' Competent Authorities in case of an emergency (Article 13):

> *(a) the daily gas demand and gas supply forecasts for the following three days, in million cubic metres per day (mcm/d);*
> *(b) the daily flow of gas at all cross-border entry and exit points as well as at all points connecting a production facility, a storage facility or an LNG terminal to the network, in million cubic metres per day (mcm/d);*
> *(c) the period, expressed in days, for which it is expected that supply of gas to protected customers can be ensured.*

After an emergency, MS shall notify the Commission within a period of maximum 6 weeks a detailed assessment of the emergency and the effectiveness of the measures implemented, including an assessment of the economic impact of the emergency, the impact on the electricity sector and the assistance provided to or received from, the Union and its MS.

9.2.3 Situations where Incident Notification policies can be triggered

The following table describes some types of incidents that may involve oil and gas services.

Table 14 - Types of incidents in Oil and Gas

Subsector	Safety related incidents/occurrences	Incident types related to the disruption of the service	Observations
Operators of offshore oil and gas installations (fixed or mobile / production or other)	Any major accident, incident or environmental incident, as defined by the Offshore Safety Directive, which could be initiated from a cyber threat.		Major Hazard Reports, Emergency Plans and Corporate Major Accident Prevention Policy could include cyber incidents. The above documents are all drafted in advance of the operations.
Operators of oil transmission pipelines	Unintended release of oil, gas or other hazardous substances, whether or not ignited; a major environmental incident; significant loss of structural integrity, or loss of protection against the effects of fire or explosion,	Inability to properly deliver and transmit oil.	Any of those incidents (and not only), to be reported only if due to cyber causes.
Operators of oil production, refining and treatment facilities, storage and transmission		Disturbances/impairments in the production, refining and treatment facilities, storage and transmission of oil.	

Subsector	Safety related incidents/occurrences	Incident types related to the disruption of the service	Observations
	or loss of station keeping in relation to a mobile installation; failure of a safety and environmental critical element;		
Gas Supply undertakings	Unintended release of oil, gas or other hazardous Substances, whether or not ignited; a major environmental incident; significant loss of structural integrity, or loss of protection against the effects of fire or explosion, or loss of station keeping in relation to a mobile installation; failure of a safety and environmental critical element;	Inability to properly deliver/transmit oil.	Any of those incidents (and not only), to be reported only if due to cyber causes.
Gas DSOs		Disturbances/impairments in the production, liquefaction, refining and treatment facilities, storage, transmission and distribution of gas.	
Gas TSOs			
Gas Storage system operators			
LNG system operators			
Natural gas undertakings			
Operators of natural gas refining and treatment facilities			

10 Outlook and conclusions

The energy sector is undoubtedly one of the most critical sectors since society and various sectors of industry are dependent on energy supply. At the same time, it is a complex sector undergoing continuous major changes (e.g. renewable energy sources, decentralisation of generation, smart grids) and which requires particular attention to specificities like real-time requirements, cascading effects and the combination of legacy and state-of-the-art technologies. In that respect, the document provides support to MS on addressing these specificities when implementing the NIS Directive. It presents an overview of the status of implementation of Article 5 for the energy sector, analyses key findings, challenges and sectorial specificities.

The document provides good practices and examples of implementation of the main NIS Directive requirements, namely OES identification criteria and methodologies, security measures, incident notification requirements. Moreover, the document provides information on governance models, cybersecurity capabilities of EU associations, organisations and bodies with a role in the energy sector and collaboration schemes.

Since numerous policies besides the NIS Directive have been introduced to secure and create a European sustainable energy network, the document establishes relations between these policies and the NIS Directive to allow for synergies and consistent implementation. To pick up an example, the Commission's recommendation on cybersecurity in the energy sector was mapped with a table of international standards and good practices applicable across all the Energy subsectors of interest, thereby building upon and adding up to the work of WS 2. With respect to security requirements, Union legislation requiring risk assessments in the energy sector were included too.

Regarding the OES identification process, the key findings derived from work carried out in WS 8 revealed that:

- Many MS included power generation in the electricity subsector despite the NIS Directive does not directly refer to the function "generation" in Annex II (while indicating in Recital 28 NIS Directive that power generation could be included).

- Several MS identified essential services covering the entire value chain, thereby including types of entities beyond the scope of Annex II of the NIS Directive.

- Concerning the oil subsector, MS identified the looser regulation compared to the electricity and gas subsectors.

- While Annex II of the NIS Directive usually refers to Union legislation when it comes to the types of entities that come into questions as OES, Annex II does not do so for the sub-sector oil, despite the existence e.g. of a Council Directive imposing an obligation on MS to maintain minimum stocks of crude oil. Nevertheless, some MS identified emergency stockholding as essential service.

- Although the interconnection of the grid systems play a key role in all the subsectors of the energy sector, it is difficult to assess the cross-border dependencies in detail.

- There is a common incident classification scale for electricity TSOs in place while one for gas TSOs is under development (see subchapter about incident notification). Although Europe has around 2400 DSOs and smart meters, electric vehicles, renewables and smart devices are directly linked to electricity distribution, no common incident-reporting scheme for DSOs exists. Various relevant Union policies where identified.

- The WS will continue its work having special consideration to the latest policy developments in the energy sector. The Cooperation Group might update this document when necessary.

List of abbreviations

ACER	Agency for the Cooperation of Energy Regulators
AEC	Austrian Energy CERT
ANSSI	National Agency for the Security of Information Systems
BEIS	Business, Energy & Industrial Strategy
C3	Cyber Security Competence Center
CA	Competent Authority
CERT	Computer Emergency Response Teams
CEER	Council of European Energy Regulators
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CPNI	Centre for the Protection of National Infrastructure
CSIRT	Computer Security Incident Response Team
CSP	Cyber Security Platform
DG	Directorate General
DOCSG	Downstream Oil Cyber Security Group
DSO	Distribution System Operators
E3CC	Energy Emergency Executive Cyber Committee
EC	European Commission
ECG	Electricity Coordination Group
ECI	European Critical Infrastructure
EE-ISAC	European Energy ISAC
ENISA	European Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators - Electricity
ENTSO-G	European Network of Transmission System Operators – Gas
EU	European Union
EUOAG	European Union Offshore Oil and Gas Authorities Group
FETSA	Federation of European Tank Storage associations
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GIE	Gas Infrastructure Europe

GWh	Gigawatt hours
HSE	Health and safety executive
IADC	International Association of Drilling Contractors
ICS	Industrial Control Systems/Incidents Classification Scale
ICT	information and communication technology
ILR	Institut Luxembourgeois de Régulation
ISAC	Information Sharing and Analysis Centre
ISO	International Standard Organisation
kV	kilovolt
LNG	Liquefied natural gas
LPG	Liquefied petroleum gas
MS	Member State(s)
MW	Megawatt
NERC	North American Electric Reliability Corporation
NCA	National Competent Authority
NCIPC	National Center for Infrastructure Protection and Cybersecurity
NCSC	National Cyber Security Centre
NCSC-FI	National Cyber Security Centre Finland
NCTV	National Coordinator for Security and Counterterrorism
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
Ofgem	Office of Gas and Electricity Markets
ONR	Office for Nuclear Regulation
OGISF	Oil and Gas Information Sharing Forum
PPD	Private-Public Dialogue
PPD-RM	Private-Public Dialogue Risk Management
REA	Research Executive Agency
TF	Task Force
TWh	Terawatt hours
TSO	Transmission System Operator
WS	Work Stream

Annex I

Annex II of the NIS Directive points to several types of entities included in the sectors and subsectors and those types of entities point to definitions included in other specific Directives. The table below maps these definitions to Annex II to facilitate MS understand what is described as an essential service for the energy sector in the NIS Directive.

TYPE OF ENTITY	DESCRIPTION
ELECTRICITY	
Electricity undertaking	• Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council(1), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive • Art 2 Nr 35 Directive 2009/72/EC: 'Electricity undertaking' means any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity, which is responsible for the commercial, technical or maintenance tasks related to those functions, but does not include final customers. • Art 2 Nr 19 Directive 2009/72/EC: 'supply' means the sale, including resale, of electricity to customers. • Art 2 Nr 1 Directive 2009/72/EC: 'generation' means the production of electricity; • Art 2 Nr 2 Directive 2009/72/EC: 'producer' means a natural or legal person generating electricity. • Art 2 Nr 7 Directive 2009/72/EC: 'customer' means a wholesale or final customer of electricity.
Distribution system operators	• Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC • Art 2 Nr 6 Directive 2009/72/EC: 'Distribution system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity. • Art 2 Nr 5 Directive 2009/72/EC: 'distribution' means the transport of electricity on high-voltage, medium-voltage and low-voltage distribution systems with a view to its delivery to customers, but does not include supply.
Transmission system operators	• Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC • Art 2 Nr 4 Directive 2009/72/EC: 'Transmission system operator' means a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity.

	• Art 2 Nr 3 Directive 2009/72/EC: 'transmission' means the transport of electricity on the extra high-voltage and high-voltage interconnected system with a view to its delivery to final customers or to distributors, but does not include supply
OIL	
Operators of oil transmission pipelines	• N/A
Operators of oil production, refining and treatment facilities, storage and transmission	• N/A
GAS	
Supply undertakings	• Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council • Art 2 Nr 8 Directive 2009/73/EC: 'supply undertaking' means any natural or legal person who carries out the function of supply. • Art 2 Nr 7 Directive 2009/73/EC: 'supply' means the sale, including resale, of natural gas, including LNG, to customers; • Art 2 Nr 24 Directive 2009/73/EC: 'customer' means a wholesale or final customer of natural gas or a natural gas undertaking which purchases natural gas
Distribution system operators	• Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC • Art 2 Nr 6 Directive 2009/73/EC: 'distribution system operator' means a natural or legal person who carries out the function of distribution and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of gas. • Art 2 Nr 5 Directive 2009/73/EC: 'distribution' means the transport of natural gas through local or regional pipeline networks with a view to its delivery to customers, but not including supply.
Transmission system operators	• Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC • Art 2 Nr 4 Directive 2009/73/EC: 'transmission system operator' means a natural or legal person who carries out the function of transmission and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transport of gas. • Art 2 Nr 3 Directive 2009/73/EC: 'transmission' means the transport of natural gas through a network, which mainly contains high-pressure pipelines, other than an upstream pipeline network and other than the part of high-pressure pipelines primarily used in the context of local distribution of natural gas, with a view to its delivery to customers, but not including supply.

Storage system operators	• Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC • Art 2 Nr 10 Directive 2009/73/EC: 'storage system operator' means a natural or legal person who carries out the function of storage and is responsible for operating a storage facility. • Art 2 Nr 9 Directive 2009/73/EC: 'storage facility' means a facility used for the stocking of natural gas and owned and/or operated by a natural gas undertaking, including the part of LNG facilities used for storage but excluding the portion used for production operations, and excluding facilities reserved exclusively for transmission system operators in carrying out their functions.
LNG system operators	• LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC • Art 2 Nr 12 Directive 2009/73/EC: 'LNG system operator' means a natural or legal person who carries out the function of liquefaction of natural gas, or the importation, offloading, and re-gasification of LNG and is responsible for operating a LNG facility. • Art 2 Nr 11 Directive 2009/73/EC: 'LNG facility' means a terminal which is used for the liquefaction of natural gas or the importation, offloading, and re-gasification of LNG, and includes ancillary services and temporary storage necessary for the re-gasification process and subsequent delivery to the transmission system, but does not include any part of LNG terminals used for storage.
Natural gas undertakings	• Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC • Art 2 Nr 11 Directive 2009/73/EC: 'natural gas undertaking' means a natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers.
Operators of natural gas refining and treatment facilities	• N/A

Annex II

Indication in national legislations – transposing the Directive[42] – where the energy sector is addressed as regards the roles, responsibilities and collaboration mechanisms of the competent authorities

Country	*Transposition Law – answers to survey by Member States*
Austria	In Austria, the energy sector is determined in § 2 NIS Law together with the other sectors. The roles, responsibilities and collaboration mechanisms of the competent authorities do not differ depending on the sector. The Federal Chancellor is the "strategic" competent authority according to § 4 NIS Law and is responsible for determining the essential services of all sectors [§ 4(2)(2) in conjunction with § 16(2) NIS Law] and for identifying the OES of all sectors [§ 4(1)(6) in conjunction with § 16(1) NIS Law]. The Federal Minister of the Interior is the "operational" competent authority according to § 5 NIS Law and is responsible for receiving incident notifications [§ 5(1)(3) NIS Law] and for assessing the compliance of OES of all sectors with incident notifications obligations [§ 5(1)(5) NIS Law] and security requirements [§ 5(1)(3) in conjunction with § 17(4)&(5) NIS Law]. The Federal Chancellery and the Federal Ministry of the Interior (together with other Ministries) cooperate together in the legally based "Inner Circle of the Operational Coordination Structure" and will jointly process incident data.
Belgium	The Belgian transposition of the NIS-Directive is still debated in Parliament; it is envisaged that the sectoral authority (in this case on Energy) will be responsible for identifying OES (but in consultation with the Centre for Cyber security Belgium and National Crisis Centre) and for organising oversight.
Czech Republic	Act No 181/2014 Coll.: e.g. section 2 , see here: https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf Criteria for determination of OES are laid down in decree 437/2014 Coll., see here: https://www.govcert.cz/download/kii-vis/preklady/Decree_437_2017_EN_v1.0_final.pdf Obligations are laid down in the decree 82/2018 Coll. (No english translation yet, soon on our web)
Germany	The NIS Directive is transposed into German law by the German NIS Directive Implementation Act. German competent authority is the BSI. The role, responsibilities and collaboration mechanisms of the BSI are laid down in the Federal Office for Information Security ("FOIS Act") / Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), specifically in Section 8b of the FOIS Act. The FOIS operates under the authority of the German Federal Ministry of the Interior.
Denmark	Electricity and naturalgas legislation: Bekendtgørelse nr. 425 af 1. maj 2018 om it-beredskab for el- og naturgassektorerne □□https://www.retsinformation.dk/Forms/R0710.aspx?id=200882

[42] Relevant information can be found on EC' website: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive and ENISA's website: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

	Oil legislation: Bekendtgørelse nr. 424 af 25. april 2018 om beredskab for oliesektoren □□https://www.retsinformation.dk/Forms/R0710.aspx?id=200881
Estonia	The NIS Directive is transposed into Estonian law by the Cybersecurity Act □□https://www.riigiteataja.ee/en/eli/523052018003/consolide
Finland	Electricity Market Act (588/2013) 29 a §: Roles and responsibilities of OES:s and NCA Natural Gas Market Act (587/2017) 34 a §: Roles and responsibilities of OES and NCA Act on the Control of the Electricity and Natural Gas Market (590/2013) 26-28 §: Collaboration mechanisms of NCAs
France	Loi n°2018-133 du 26 février 2018 transposing the NIS directive into French law https://www.legifrance.gouv.fr/eli/loi/2018/2/26/INTX1728622L/jo/texte/ Décret n° 2018-384 du 23 mai 2018 about network and information security of OES and DSP https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036939971&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000036939966 Arrêté du 13 juin 2018 about the terms of the mandatory declarations stated in the Decree n° 2018-384 about network and information security of OES and DSP https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8E12CB0B6525D7BB3567CD18C72B863F.tplgfr40s_1?cidTexte=JORFTEXT000037102068&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037102045 Arrêté du 1er août 2018 relating to the cost of the control made by ANSSI https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037277276&dateTexte=&categorieLien=id Arrêté du 14 septembre 2018 setting the security rules and deadlines mentioned in the Decree n° 2018-384 about network and information security of OES and DSP https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037444012&dateTexte=&categorieLien=id
Italy	The Legislative Decree n. 65 of May 18th, 2018, transposes the NIS Directive in the Italian legislation. Art. 4, 7, 13, 17, 19 and 20 address the roles and responsibilities of the single NIS competent authority in the energy sector. Moreover, art. 12 and 13 define the roles and responsibilities of OES.
Latvia	National legislation (transposing the Directive) where the energy sector is addressed as regards the roles, responsibilities and collaboration mechanisms of the competent authorities: Law On the Security of Information Technologies (https://likumi.lv/doc.php?id=220962) and on the basis of which the following Cabinet of Ministers regulations have been issued: - Regulation No. 442 of 28 July 2015 „Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements“ (https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam) - Regulation No. 43 of 15 January 2019 „ Regulations on the conditions for determining the significantly interfering effects of a security incident and the procedures for granting, reviewing and terminating the status of the operators of essential

	services and the status of an essential service“ (https://likumi.lv/ta/id/304327-noteikumi-par-nosacijumiem-drosibas-incidenta-butiski-traucejosas-ietekmes-noteiksanai-un-kartibu-kada-pieskir-parskata-un-izbe...) - Regulation No. 15 of 15 January 2019 „ Regulations on the significance criteria of a security incident, information procedures and the content of the report “ (https://likumi.lv/ta/id/304284-noteikumi-par-drosibas-incidenta-butiskuma-kriterijiem-informesanas-kartibu-un-zinojuma-saturu)
Luxembourg	The draft legislation foresees that the ILR will be the competent authority for the energy sector and will designate the OES of this sector and will be the national single point of contact. The ILR is also the authority responsible of market regulation of the electricity and gas sectors. In Luxembourg.there is no designated cyber authority. Given that the cybersecurity topic covers a wide range of areas and falls within the assignment of several state entities, the Government decided to bring together key players to set up an interministerial committee in charge of cybersecurity coordination at national level. The committee coordinates, alongside the Cybersecurity Board – which plays a rather strategic role –, pragmatic initiatives as part of cyber security. As a market regulator and as a NIS authority the ILR acts in close consultation with the stakeholders and operators of the private sector.
The Netherlands	The NIS Directive is being implemented in the Netherlands as the ‘Wet bescherming network en informatiesystemen’ (Wbni). The Wbni is a relatively straightforward implementation of the NIS Directive. OES are identified in the accompanying decree, which contains definitions of OES of various sectors. The role of the Telecommunications Authority follows from the Wbni and the decree. It’s regulation will be based on open norms evolving from the present best practices in the sector. Thresholds for incidents which have to be reported have been set in consultation with the sector and have been communicated to the sector by confidential letter. Collaboration within the energy sector was already established in working groups within sector organisations and the national cybersecurity center. No additional collaborative mechanisms have been set up as a result of the NIS.
Poland	The energy sector and respective subsectors are enlisted in annex 1 to the law on the national cybersecurity system. The role of the Minister of Energy as a competent authority is defined in the chapter 8 of the law, chapter 11 relates to the supervision and control which may be performed by the Minister and the chapter 14 define the sanctions towards OES’s. There are also separated articles within chapter 3 related to OES’w where the procedure of identification, audits and the role of competent authortity is given.
Portugal	Law 48/2018, of August 13 transposes the NIS Directive to the internal legal order and determines in article 7 (1) that the National Cybersecurity Centre is the National Cybersecurity Authority. According to article 7 (4) of Law 46/2018 the National Cybersecurity Centre exercises the functions of regulation, governance, supervision, inspection and sanctioning in accordance with its

	competences, and also has the power to issue instructions and define the national level of alert in cybersecurity, as in established in article 7 (5). The Energy sector, subsectors and types of entities under the authority of the National Cybersecurity Centre correspond entirely to the established in Annex 2 of the NIS Directive without further inclusions. The identification of OES is revised on an annual basis according to article 29 (2) of Law 46/2018. Articles 16 and 17 of Law 46/2018, define obligations on requirements for security measures and for the notification of incidents on OES.
Spain	The NIS Directive is fully transposed into the Spanish internal order by the Royal Decree-Law 12/2018 https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf
Sweden	***Law:*** https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174 ***Ordinance***: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet_sfs-2018-1175
United Kingdom	NIS Regulations (https://www.legislation.gov.uk/uksi/2018/506/contents/made), Schedule 1, sets out the different Competent Authorities. The BEIS NIS policy document at Gov.uk NIS Policy Document Energy Sector GB.pdf sets out the different roles and responsibilities of the authorities. This is an extract: 3.16. The BEIS regulatory policy team will be responsible for: Responsibilities of BEIS Competent Authority Function • Setting thresholds for OES and incident reporting; • Designation and revocation of OES; • Raising industry awareness of NIS compliance requirements; • Ensuring alignment of approach across the energy sector; • Setting policy on any incremental increase of initial compliance requirements over time; • Reviewing frameworks with HSE and Ofgem; and • Monitoring the overall cyber security 'health' of the energy sector. Security of Network and Information Systems Regulations – Implementation in the Energy Sector in Great Britain 3.17. Ofgem and HSE will be responsible for:

	Responsibilities of Ofgem and HSE • Monitoring the application of the NIS Regulations in their sector; • Preparing and publishing guidance on security practices and systems management approaches to assist OES in meeting the requirements of the NIS Regulations; • Assessing compliance of OES against the requirements of the NIS Regulations, including using inspections and third-party assessments; • Cooperating with other Competent Authorities to provide consistent advice and oversight to OES; • Receipt of incident reports; • Ensuring processes are in place by an OES for incident response for non-cyber incidents; • Incident investigation; and • Enforcement of the requirements of the NIS Regulations including how penalties will be issued

Annex III

The table below shows which MS have chosen different definitions of 'essential service', including for each subsector (oil, gas, electricity) in the energy sector, and describes the challenges faced when defining them.

Country	*Definitions*
Austria	Essential service is generally defined in § 3 No 9 NIS Law as a service, which is provided in one of the sectors referred to in § 2 and which is of essential importance in particular for the maintenance of the public health service, the public supply of water, **energy** and essential goods, public transport or the operability of public information and communication technology and the availability of which depends on network and information systems. Thus, there is a uniform definition. However, the general definition is differentiated and specified in a subset of essential services as the Federal Minister responsible in the Federal Chancellery has - in agreement with the Federal Minister of the Interior - determined more detailed provisions concerning the sectors referred to in § 2 NIS Law by ordinance. This ordinance ("NIS Ordinance") covers in particular sub-sectors, areas, individual essential services and types of entities eligible as OES. In the ordinance, the sector energy is divided in the sub-sectors electricity, gas and oil. The sub-sector electricity covers the field generation, distribution and transmission. The sub-sector gas covers the field extraction, storage, distribution, transmission, market area management and distribution area management. The sub-sector oil covers the field production, storage, transmission and refining.
Belgium	The same as the NIS Directive definitions.
Czech Republic	Czech Republic has the same definition of OES, but different definition of critical information infrastructure. Critical information infrastructure and essential service may, in some cases, concern a same subject. Such cases, take place especially in network sectors (e.g. distribution of electricity and gas) and the sectors with the possibility to provide services on different levels and with different importance for the customers. Therefore, sometimes it is challenging to decide, if a provider should be identified as a provider of system of critical infrastructure or essential service.
Germany	Same definitions but different thresholds for each asset category: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/bsi-kritis-ordianceposter.pdf?__blob=publicationFile&v=4
Denmark	***Essential services in the electricitysector*** are: Electricity TSO's, DSO's, Power production companies with licenses to establish power productioncapacity for 25Mwh or more and companies responsible for balancing the powergrid. ***Essential services in the natural gas sector are:*** Gas TSO, Gas DSO's and Gasstorage companies. ***Essential services in the oil sector are***:

	Oil companies with a positive stockholding obligations towards the Danish State.
Estonia	Definitions are in specific sectoral law: ***Oil*** – A fuel vendor who owns ten or more petrol stations and whose petrol stations are located in at least three counties is a vital service provider. ***Gas*** – The vital service provider is: 1) an undertaking which provides a transmission service in the gas network; 2) an undertaking with more than 10.000 consumers connected to its distribution network. ***Electricity*** - Vital service provider is: 1) a producer whose net power exceeds 200 MW; 2) a line owner with a transmission line capacity exceeding 100 MW crossing the state border; 3) the TSO; 4) a network operator with more than 10.000 consumers connected to its distribution network.
Finland	***Electricity***: DSOs and TSO. ***Gas***: TSO
France	The definitions of essentials service are defined according to the "type of entity" of the ANNEX II of the DIRECTIVE (EU) 2016/1148.
Italy	The essential services have been defined on the basis of the NIS Directive
Latvia	Essential service provider is a state or local government institution or a legal person governed by private law who performs economic activity in the Republic of Latvia and provides: 1) financial services within the meaning of the Credit Institution Law and financial market infrastructure services, supply or distribution services of drinking water, internet exchange point services, domain name system services, services of the top-level domain name register or services in the energy, transport or health sector in one of the European Union Member States; 2) services that depends on network and information systems; - services on the provision of which incident would have significant disruptive effects
Luxembourg	As work is still in progress, there are no final essential service definitions at this point. The final service definitions will probably closely match with "Type of entity" of the annex II of the directive
The Netherlands	The Act (Wbni, article 5) refers to (1) OES, as mentioned in the NIS directive and (2) other critical services. The underlying Decree[43] (Besluit beveiliging netwerk- en informatiesystemen) lists in more detail who these operators are. For electricity, the TSO and DSO's are all commissioned as OES. In the near future, this scope may be extended to electricity producers (likely based on a generation capacity threshold) For gas, the TSO and DSO's are all commissioned as OES. In addition, also the (only) company responsible for the exploration and extraction of Groningen gas is commissioned as an OES.

[43] Gas: the Decree refers to "exploration and extraction" (ïn Dutch: "opsporen en winnen").
Oil: the current Decree refers only to the 'strategic oil storage', i.e. in relation to the IEA 90 days storage obligation.

	For oil: the Dutch Stockpiling Agency is commissioned as an OES. In the near future, this scope may be extended to private storage companies (above a certain threshold, e.g. the threshold of 100.000 tonnes of output used in the Stockpiling Act).
Poland	The definitions have almost the same descriptions of the processes within the value chain (ex. generation, distribution, trading, processing or storage), except for the source of the energy (subsector). The energy sector as whole is mainly regulated in Act of 10 April 1997 – Energy law, so the challenges was low.
Portugal	The essential services identified correspond to the types of entities identified in Annex II of the NIS Directive for the Energy sector.
Spain	The essential services identified correspond to the types of entities identified in Annex II of the NIS Directive for the Energy sector. Moreover, essential services dependent on networks and information systems within the strategic sectors defined in the annex to Law 8 /2011 for the protection of critical infrastructures shall be taken into account.
Sweden	**Sector*** — **Name/Title of the Essential Service*** — **Description** Energy Electricity - TSO — All operators are OES Energy Electricity - DSO — DSO with high voltage new or DSO with identified supply to essential Energy Electricity - Production — All power stations connected to high voltage network Energy Electricity - Wholesale — Operator with imbalance agreement with TSO Energy - Gas — TSO — All operators are OES Energy - Gas — DSO — All operators are OES Energy - Gas — Wholesale — All operators are OES Energy - Gas — Operators of natural gas refining and treatment facilities — Operators handling >20GWh /yr Energy - Oil — Operators of oil production, refining and treatment facilities — Operators handling >0,5Mton/yr (fossil) or > 0,05 Mton/yr (bio) Energy - Oil — Operators of oil storage — Operators with storage capacity >100 000m3 (fossil), >50.000m3 (bio)

	Energy - Oil	Operators of oil transmission	Operators handling 0,5 Mton/yr (fossil) or 0,25 Mton/yr (jet)
United Kingdom	Thresholds for OESopera are set out in Schedule 2 of the NIS Regulations and in Annex E of the BEIS NIS policy document. Thresholds for the designation of OES were consulted widely with the energy sector. A set of thresholds were defined for each sub-sector. BEIS keeps the thresholds under review and reserves the right to amend these if necessary. NIS Policy Document Energy Sector GB.pdf		

Annex IV

Country	*Identified essential energy services beyond the NIS Directive*
Austria	Power Generation was included as it has a key role in the electricity supply chain. In the gas subsector, certain tasks of the market area manager and of the distribution area manager were considered essential.
Belgium	-
Czech Republic	Thermal industry (Heating power) – From historical point of view, there is plently of heating plants in the teritorry of the Czech Republic. This is the reason why thermal industry was also identified.
Germany	The assets and installations for supplying the general public that are of sufficient importance from the federal perspective are deemed to be Critical infrastructures in Germany.
Denmark	**-**
Estonia	District heating – often combined heat and power plants are used to provide both electricity and heat. During cold winter, lack of district heating can cause widespread problems within days.
Finland	**-**
France	For the Oil subsector: operators of logistics data transfer platforms, which operate logistics data transfer service between oil operators, and between oil operators and public authorities
Italy	Since the failure of the main power energy facilities may impact the transmission and distribution services, the power generation service is considered as an essential service according to the criteria laid down in the NIS Directive. Essentials services are defined according to ANNEX II of the DIRECTIVE (EU) 2016/1148.
Latvia	-
Luxembourg	**-**
The Netherlands	In the Netherlands there are a few identified essential energy services which go beyond the NIS Directive: Electricity: in the near future, the scope may be extended from TSO/DSO to electricity producers, likely based on a generation capacity threshold. Gas: not applicable Oil: currently the Dutch Stockpiling Agency is commissioned as an OES. In the near future, this scope may be extended to private storage companies (above a certain threshold, e.g. the threshold of 100.000 tonnes of output used in the Stockpiling Act).
Poland	The following sectors and services within these fields beyond the scope of the NIS Directive were identified in Poland: mining, heat supply, services for the energy sector, services provided by the supervised and subordinate units. The reason was to enlist all the energy sectors that provide essential services in Poland, to include the whole value chain

	in the energy sector and related sectors. What is important, all the sectors are supervised by the same authority – Minister of Energy.
Portugal	The Energy sector, subsectors and types of entities under the authority of the National Cybersecurity Centre correspond entirely to the established in Annex 2 of the NIS Directive without further inclusions. Other energy services were considered such as energy producers but were not included as types of entities under the application of Law 46/2018, of August 13 which transposes the NIS Directive. The identification of OES is periodically revised on an annual basis according to article 29 (2) of Law 46/2018.
Sweden	The Swedish NIS law refers to appendix 2 in the NIS Directive, There is thus no mandate to add national specific OES. District heating and district cooling are though examples of critical infrastructure's I Sweden.
United Kingdom	The UK has transposed the NIS Directive for energy sub-sectors referenced by the Directive only. We will consider other relevant services e.g. Smart Energy in future NIS review.

Annex V

Questionnaire

COUNTRY	
DATE AND TIME	

Introduction

The energy infrastructure is arguably one of the most complex and, at the same time, critical infrastructures that other business sectors depend upon to deliver essential services. Because of this dependency, a potential disruption for a long period of time can trigger a cascade of effects in other sectors of society.

With the growing use of digital devices and more advanced communications, the overall cyber risk is increasing for the energy sector.

It is, therefore, indispensable to look at the particularities of the energy sector that create challenges in terms of cyber security, such as real-time requirements, cascading effects, and legacy systems in combination with new technologies. A focus has to be put on:

- Systemic Impact
  - EU Energy reliability depends on Pan-European connectivity
  - Many market players in different sizes (small RES, distributed generators etc.)
- Greater system complexity and reliance on ICT due to increasing use of (I)IoT – Industrial IoT- and smart meters.
- Different priorities depending on the nature of the energy stakeholder - CIA (Confidentiality, Integrity and Availability) vs. AIC (Availability, Integrity, Confidentiality)
- Changing threat landscape increases the trans-national impact in the case of successful attacks on the electrical infrastructure.
- Structural changes in the energy market lead to the need for more dynamic trans-national energy control requirements.
- Structural changes in infrastructure make more intense the need for technological solutions which support more flexible demand and response models for energy.
- Shift in value and supply chain make traditional development and security funding models not accessible anymore.

In such a complex ecosystem, an operator has to focus on the operational environment, to protect information systems, detect potential attacks, as well as respond and recover on respective incidents. The National Competent Authorities (NCA) should, in the first place, focus

on those operators who are considered most critical – energy Operators of Essential Services (OES).

With evolving threats, the capabilities to respond and recover are getting more important. That is why the OES need the support from the national authorities or CSIRTs to better respond to cyber-attacks.

In this light, the objective of this questionnaire is to collect information from the NCA on how they identify the energy sector OES. This will allow for a more consistent approach to energy cybersecurity at EU level as well as the identification of cascading effects which might have a serious impact on many business sectors of society and even in other Member States´ economy.

I. General

1. Which are the authorities involved for the identification of OES in the energy sector.

Please name the authorities

Electricity: Gas: Oil: Other subsector:

2. Please indicate in which way the responsible authorities collaborate with each other.
Please describe issues such as: the relationship between the energy authority the cyber authority; the procedures in place; consultations with the private sector, etc.

3. Please indicate in your national legislation - transposing the Directive – where the energy sector is addressed as regards the roles, responsibilities and collaboration mechanisms of the competent authorities.

II. Essential services

4. Does your country have different definitions of 'essential service' for each subsector (oil, gas, electricity) in the energy sector? What are the challenges that you face when defining them?

If “Yes”, please name the definition(s) and the challenges

5. **Please describe if you identified other energy relevant services (i.e heating, power generation) beyond the scope of the NIS Directive that your country considers critical /vital /essential.** *(An explanation of the reasoning why other services are considered essential. An indication of factors used would be appreciated).*

III. Operators of Essential Services (OES) in the Energy Sector

6. **Is there any obligation other than the NIS Directive, which imposes cyber security and/or incident reporting requirements on energy undertakings? If yes, then please describe other incident reporting requirements.**

7. **What methodology did you follow to identify the OES in the energy sector?**

National risk assessment: ☐
Identification of Critical Infrastructures: ☐
Identification of OES: ☐
National exercises: ☐

Other:

Please describe the methodology:

Electricity:

Gas:

Oil:

Other:

8. **Can you please provide a summary of the main challenges/overlaps faced when you try to switch from ECI Directive to the NIS Directive method for the identification of OES?**

9. **Did you follow a state-driven or operator driven approach to identify OES in the energy sector?**

- State driven (the state is responsible to identify the OES according to certain criteria and thresholds) ☐
- Operator driven (the state publishes the criteria and thresholds and the operators identify themselves and register as OES) ☐

10. **How do you engage with the private energy sector operators?**

11. **Please describe the approach that you follow for the identification of OES for the energy sector with cross-border impact. How do you assess these dependencies?** *(please share your practice)*

12. **Please indicate which criteria or factors you are using, or planning to use for the identification of OES in the energy sector regarding the electricity subsector. If applicable, please name thresholds.**
Article 5 and 6

Criteria or factor		**Thresholds (if applicable)**
▪ Providing a service depending on network and information systems	☐	
▪ Number of essential services provided	☐	
▪ Quantity of service or goods produced, carried or handled in some other way	☐	
▪ Size of the entity (e.g. by market share)	☐	
▪ Number of people relying on the service provided	☐	
▪ Importance for societal activities	☐	
▪ Importance for economy	☐	
▪ Importance for public safety and/or order	☐	
▪ Importance for public confidence and/or trust	☐	
▪ Importance for environment	☐	
▪ Time of reconstruction in case of incident	☐	
▪ Uniqueness of service or underlying physical infrastructure	☐	
▪ Geographic spread with regard to the area that could be affected by an incident	☐	
▪ 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	☐	

▪ Inter-sector operators' dependencies: Dependencies on other operators within the same sector	☐	
▪ Cross-sector operators' dependencies: Dependencies on other operators in other sectors	☐	
▪ Cross-border dependencies within EU: Dependencies on operators in other EU MS	☐	
▪ Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	☐	
▪ Other:	☐	

13. Please indicate which criteria or factors you are using, or planning to use for the identification of OES in the energy sector regarding the oil subsector. If applicable, please name thresholds.
Article 5 and 6

Criteria or factor		**Thresholds (if applicable)**
▪ Providing a service depending on network and information systems	☐	
▪ Number of essential services provided	☐	
▪ Quantity of service or goods produced, carried or handled in some other way	☐	
▪ Size of the entity (e.g. by market share)	☐	
▪ Number of people relying on the service provided	☐	
▪ Importance for societal activities	☐	
▪ Importance for economy	☐	
▪ Importance for public safety and/or order	☐	
▪ Importance for public confidence and/or trust	☐	
▪ Importance for environment	☐	
▪ Time of reconstruction in case of incident	☐	
▪ Uniqueness of service or underlying physical infrastructure	☐	
▪ Geographic spread with regard to the area that could be affected by an incident	☐	
▪ 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	☐	
▪ Inter-sector operators' dependencies: Dependencies on other operators within the same sector	☐	
▪ Cross-sector operators' dependencies: Dependencies on other operators in other sectors	☐	
▪ Cross-border dependencies within EU: Dependencies on operators in other EU MS	☐	
▪ Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	☐	
▪ Other:	☐	

14. Please indicate which criteria or factors you are using, or planning to use for the identification of OES in the energy sector regarding the gas subsector. If applicable, please name thresholds.

Article 5 and 6

Criteria or factor		Thresholds (if applicable)
▪ Providing a service depending on network and information systems	☐	
▪ Number of essential services provided	☐	
▪ Quantity of service or goods produced, carried or handled in some other way	☐	
▪ Size of the entity (e.g. by market share)	☐	
▪ Number of people relying on the service provided	☐	
▪ Importance for societal activities	☐	
▪ Importance for economy	☐	
▪ Importance for public safety and/or order	☐	
▪ Importance for public confidence and/or trust	☐	
▪ Importance for environment	☐	
▪ Time of reconstruction in case of incident	☐	
▪ Uniqueness of service or underlying physical infrastructure	☐	
▪ Geographic spread with regard to the area that could be affected by an incident	☐	
▪ 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	☐	
▪ Inter-sector operators' dependencies: Dependencies on other operators within the same sector	☐	
▪ Cross-sector operators' dependencies: Dependencies on other operators in other sectors	☐	
▪ Cross-border dependencies within EU: Dependencies on operators in other EU MS	☐	
▪ Cross-border dependencies internationally: Dependencies on operators in countries outside the EU	☐	
▪ Other:	☐	

15. Please name other sub-sector specific factors that you are taking into account, when identifying OES in the energy subsectors (electricity, gas, oil).

Example: In the oil subsector, the essential service may be identified according to the volume of oil supply per day.

Sub- Sector	Sub-sector-specific criteria or factor	Thresholds (if applicable)

16. Which are the sectoral specificities that influence the identification of energy operators and make it more/less complex than in other sectors? *(i.e. An operator offering a billing service might be considered OES only under specific circumstances, or high level interlinked dependencies with other sectors).*

17. What kind of sources did your country consider to determine the criteria mentioned in the previous question?

- National statistics ☐
- Expert discussions ☐
- Third party assessments ☐
- *Eurobarometer* by the European Commission ☐
- Data from each sector via public-private partnerships ☐
- Public data from a sector ☐
- Other ☐

Please describe in detail

18. Does or will your country provide incentives to encourage operators of essential services in the energy sector to enhance their cyber security?

- Yes ☐
- No ☐
- Maybe ☐

IV. Challenges

19. Please indicate the challenges that you are facing or have been facing in the identification of OES in the energy sector.

- Cooperation with the private sector ☐

- Availability of information regarding OES in the energy sector ☐
- Specifying threshold to determine the relevant supply level ☐
- Adopting or changing existing methodologies to the requirements of the NIS Directive ☐
- Initiating an identification process for OES ☐
- Confusion with regard to the various terms used for each subsector ☐
- Difficulty with assessing dependencies with other MS ☐
- Difficulty with assessing dependencies with other sectors ☐
- Other (please describe) ☐

20. Which are the sectoral specificities that influence the identification of energy operators and make it more/less complex than in other sectors?