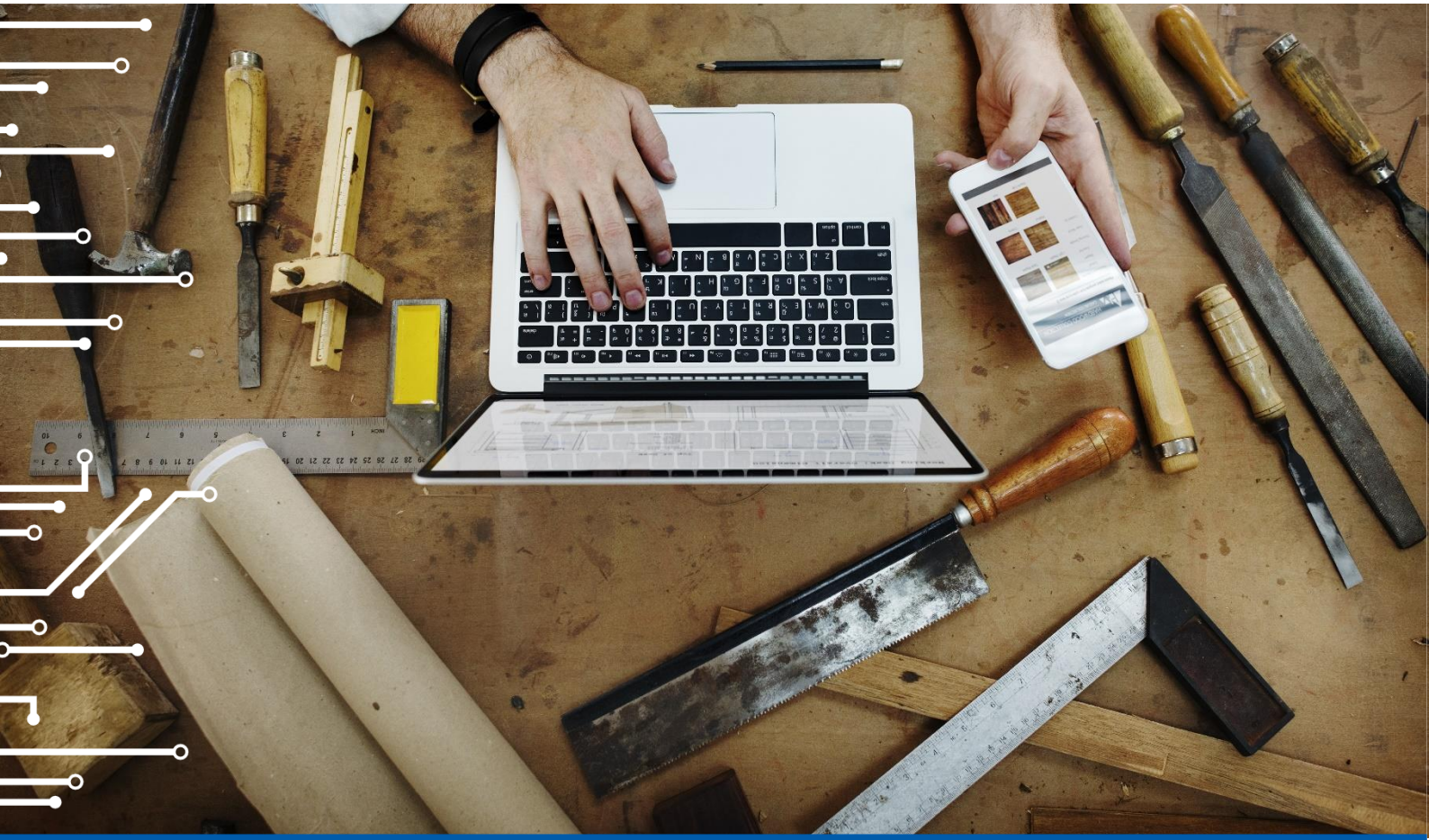
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



EU MS INCIDENT RESPONSE DEVELOPMENT STATUS REPORT

NOVEMBER 2019

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use: csirt-relations@enisa.europa.eu.

PGP Key ID: 31E777EC 66B6052A PGP

PGP Key Fingerprint: AAE2 1577 19C4 B3BE EDF7 0669 31E7 77EC 66B6 052A for media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Edgars Taurins, ENISA

ACKNOWLEDGEMENTS

ENISA performed this study with the help of contractor CEIS and with the input from Informal Expert Group on EU Member States Incident Response Development.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-310-0, DOI 10.2824/74233

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Following the recent transposition of the NIS Directive[1] (NISD) into European Member States (MS) legislation, this study aims to analyse the current operational Incident Response set-up within NISD sectors[2] and identify the recent changes. The study provides a deeper insight into NISD sectoral Incident Response capabilities, procedures, processes and tools to identify the trends and possible gaps and overlaps.

Incident Response Capabilities (IRC) within NISD sectors is a growing concern to tackle potential incidents which could have a major impact on European societies and citizens. To assess IRC, the analysis framework for the research included the following aspects:

- Impact of the NIS Directive on national CSIRT/IR layout and operational set-up in the NISD sectors;
- IR cooperation and operational models within the NISD sectors
- IRC development in the NISD sectors
- Lessons learned and recommendations.

A series of seven findings were identified while conducting the research activities.

Key Finding #1 – Member States' organisational culture and resources tend to shape the overall IR layout and set-up

Depending on whether a Member State's organisational culture is centralised or decentralised, the Incident Response layout and set-up is often structured in a similar manner, i.e. with a central authority or instead with shared responsibilities between different actors. The main entities in charge of Incident Response at national level, tend to be the national CSIRT and the Operator of essential Services (OES)[3]. However, the mandate and the resources of the National CSIRT or national cybersecurity authority is another important element influencing a centralised or distributed incident response model.

Key Finding #2 – The Directive's main positive impact was to clarify actors' roles and responsibilities within the IR organisation

The main positive impact of the Directive was to improve the IR organisation and governance by clarifying actors' roles and responsibilities. The data collected also suggest that the NISD had an unequal effect from one country to another. Indeed, this positive impact is less visible in Member States with a more mature layout and pre-existing national regulations to govern incident response in NISD sectors. However, the Directive has led/is leading to the formal identification of OES in countries who had not previously done so.

Key Finding #3 – The implementation of the NISD raises operational and regulatory challenges for the MS regulators and competent authorities

The implementation of the Directive raises operational and regulatory challenges, in particular for the definition of OES and competent authorities and the legal balance between sharing

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN#d1e1386-1-1
[2] Definition in Chapter 1
[3] Definition in Chapter 1

information and respecting privacy regulations. The operational implementation of the Directive in the Member States also highlights MS willingness to move forward since most of them extended the number of sectors targeted and their scope.

Key Finding #4 – The success of demand or regulatory drivers for the creation of sectoral IR entities and capabilities depends on IR layout maturity

The creation of sectoral IR entities and capabilities is driven by both operational demand and policy regulation. A blend of bottom-up and top-down incentives could be the most efficient driver to enhance capabilities, however an important element to take into account is the MS IR layout maturity. In countries with a very mature or centralised IR layout, there is less need for sectoral IRC. For all NISD sectors and/or sub-sectors, the main entities in charge of IR for 51% of the respondents are the national CSIRT and the OES

Key Finding #5 – Sectoral CSIRTs rely on similar notification and reporting tools as National CSIRTs but provide sector-specific knowledge and expertise to their constituents

Both national CSIRTs and sectoral CSIRTs have developed mature reporting processes and notification tools. The main added value of sectoral CSIRTs is to provide services specific to their sectors' needs, in particular a more in-depth knowledge of the threat and actor landscape, better adapted tools and solutions and operational expertise. Sector-specific regulations which include guidelines and requirements for reporting and management of incidents are crucial to enhance capabilities at the sectoral level. However, there is a lack of skilled staff, making it difficult for sectoral CSIRTs to reach full capacity.

Key Finding #6 – There is a growing number of sectoral cooperation and information-exchange initiatives, yet they often lack visibility or resources to sustain their efficiency

There is a multiplication of information exchange tools and initiatives to facilitate cooperation at sectoral, national, regional and EU level. These initiatives can take various forms and be more or less formalised. This quantitative evolution is an encouraging sign but does not provide information on the quality and outcomes of the exchanges. The long-term benefits of these initiatives will depend on the presence of both organisational and structural elements to sustain the efficiency of the initiatives.

Key Finding #7 – Training at sectoral level is key to foster and enhance preparedness

Training is an area of constantly growing interest for sectoral CSIRTs and for other operational entities and it is considered as a crucial pillar of the cybersecurity value chain and IR actors' preparedness and expertise. Interesting good practices to organise training have been gathered by national CSIRTs, which could provide an answer to the need for skilled personnel training opportunities.

Recommendations to ENISA

- Knowledge: Collect deeper insights on both national and sectoral CSIRT maturity when the NISD will have been fully practically implemented;
- Cooperation: Bolster cross sectoral knowledge between the stakeholders;
- Information sharing: Continue to collect available resources to enhance IRC & enhance information-sharing and build a repository;

- Training: Evaluate a possibility to develop a continuum for training activities which include assessing sectors trainings needs, promoting the “train-the-trainers» approach and developing basic sectoral trainings.

Recommendations to the IRC community (National and sectoral CSIRTs)

- Transparency: Publish a clear list of the sectors covered within NISD at national level (same as the NISD or extended);
- Information sharing: Encourage the use of secure communication tools, common taxonomy and sharing of lessons learned after incident with peers and everywhere; The responsible disclosure of vulnerabilities should be fostered by setting incentives;
- Cooperation: Build trust within communities and engage with OES and DSP;
- Resources: the IR community should have adequate resources to conduct their missions.

1. OVERVIEW AND SCOPE OF THE STUDY

1.1 CONTEXT

In 2019, ENISA is assisting European Member States (EU MS) with their Incident Response Capabilities (IRC) by providing a state-of-the-art overview of the CSIRT landscape and development in Europe. This work aims to further develop and apply ENISA recommendations for CSIRT capability development.

ENISA's public website features both a European CSIRT inventory[4] with an interactive map, which gives an overview of the actual situation of publicly listed CSIRT teams in Europe and a published Study on CSIRT landscape and IR capabilities in Europe 2025[5]. These two elements support an overall picture of current CSIRTs' incident handling and response capabilities (IRC), with initial facts on sectoral CSIRTs.

OES in the seven sectors identified in the NISD are accelerating their efforts to build or upgrade their IRC.

Following the adoption of the NIS Directive, EU Member States (MS) transposed the different measures and guidelines into national legislation, including those focusing on OES and critical infrastructure. For example, the NIS Directive requests MS to appoint at least one Computer Security Incident Response Team to monitor incidents at national level and facilitate collaboration at European level. Beyond national and/or governmental CSIRTs, operators of essential services (OES) in the seven sectors identified in the NISD are accelerating their efforts to build or upgrade their IRC. This effort includes the set-up of specific capabilities within the NISD sectors and the development of sector-specific IR collaboration mechanisms and fora at sectoral, national, EU and international level.

1.2 OBJECTIVE OF THE STUDY

The objective of this study is to help ENISA gain a better understanding of and draw conclusions about the recent and current changes in the European Incident Response landscape based on NISD requirements. This study aims to dive deeper into IRC in NISD sectors and to study the procedures, processes and tools used either by designated CSIRTs in particular sectors or by an entity responsible for IR in these sectors in all EU MS and collect existing good practices from neighbouring countries.

The specific objectives of this study are:

- To collect and aggregate comprehensive data on current IRC of NISD sectors;
- To analyse and evaluate the recent changes since the implementation of the NIS Directive;
- To identify potential gaps, overlaps and challenges in national IR procedures, processes and tools.

To achieve these objectives a series of three research activities have been conducted in parallel, namely desktop research of open sources, a survey of EU national and sectoral CSIRTs (response received from 17 Member States and Norway) and complementary interviews with sectoral IRC experts and national CSIRTs.

[4] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
[5] https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025

Norway has also been included in the scope of the study because it provides interesting case studies within its financial sector. The country is highly digitalised and faced important cyber-attacks targeting their operator of essential services in the past which led them to develop sectoral IRC before the publication of the NISD.

An overview of the methodology, an assessment and presentation of the data collection are presented in chapter 3 and 4.

1.3 SCOPE OF THE WORK AND DEFINITIONS

This study provides data and analysis on the recent changes and evolutions of IR capabilities (IRC) within NISD sectors in Member States (and Norway).

The study focuses on:

- The impact of the NISD on the organisation and conduct (layout) of IR and on CSIRT operational set-up in all EU MS;
- The cooperation models and the capabilities (including processes, procedures and tools) developed by MS for each NISD sector;
- The way sectoral CSIRTs and other IR actors (private sector, OES) function in conjunction with the national CSIRT in crisis/large incident situations from communication processes to escalation procedures and incident management;
- Good practices, lessons learned and key challenges in this area.

It was therefore important to agree on the definition of the key structuring concepts and elements of the study.

The following definitions have been used in this document and shared to define the scope and key concepts of the research:

Incident response (IR): The protection of an organisation's information by developing and implementing an IR process (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.[6]

Incident response capabilities (IRC): Incident response capabilities are the processes (e.g. plans, defined roles, training, communications, management oversight), procedures and tools (log analysis, Intrusion Detection Systems, Vulnerability scanners, Data Capture & Incident Response Forensics Tools, Patch management systems, etc.) used to respond to identify, respond and mitigate an attack, to restore continuity of service.[7]

Incident response models: Within the survey, a typology of four Incident Response models have been defined:

- **Centralised:** the national CSIRT is in charge of handling incidents across the different sectors; it provides a centralised point for incident reporting and analysis, decision making, response coordination, and information dissemination.
- **Distributed:** the national CSIRT has core responsibilities to handle incidents and works with a competent authority for each sector (e.g. national ministries or public agencies); the role of these actors may be to facilitate incident notification and information dissemination.

[6] Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, August 2016.
[7] Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, August 2016.

- **Hybrid:** a national CSIRT and the sectoral CSIRTs share the IR responsibilities and operations, which may depend for example on the sector(s) impacted or the scale of the incident.
- **Decentralised:** a sectoral CSIRT is in charge of handling incidents in a given sector from incident detection to response coordination and decision making, including coordinating with other stakeholders.

National/Government (N/g) CSIRTs: Teams that serve a country's government by helping to protect its critical information infrastructure. N/g CSIRTs play a key role in coordinating incident management with the relevant stakeholders at national level. They also bear responsibility for cooperation with other countries' national and governmental teams.[8]

Sectoral CSIRTs: Entities that respond to computer security or cybersecurity incidents affecting a specific sector. Sectoral CSIRTs are usually established in NISD sectors such as Healthcare, Public Utilities, and the Financial Sector. Unlike the National/Government CSIRTs who serve the public sector, sectoral CSIRTs provide services to constituents from a single sector only[9] (in the context of this study, the Sectoral CSIRTs and sectors mentioned are mainly NISD sectors).

NIS Directive: The Directive on Security of Network and Information Systems (NISD) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The NISD provides legal measures to boost the overall level of cybersecurity in the EU.[10]

NISD sectors: Sectors vital for the European Union's society and economy and heavily dependent on ICT. Seven sectors are listed in the NIS Directive (NISD sectors), for which Member States have been requested to identify operators of essential services (OES). The seven sectors – and related sub-sectors - listed in the Directive[11] are:

- Energy (electricity, oil, gas);
- Transport (air, rail, water, road);
- Banking;
- Financial market infrastructures;
- Health sector;
- Drinking water supply and distribution;
- Digital Infrastructure.

Operator of Essential Services (OES): Operators of essential services are private or public sector entities who play an important role in providing security in healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply. According to the NIS Directive, the Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services[12].

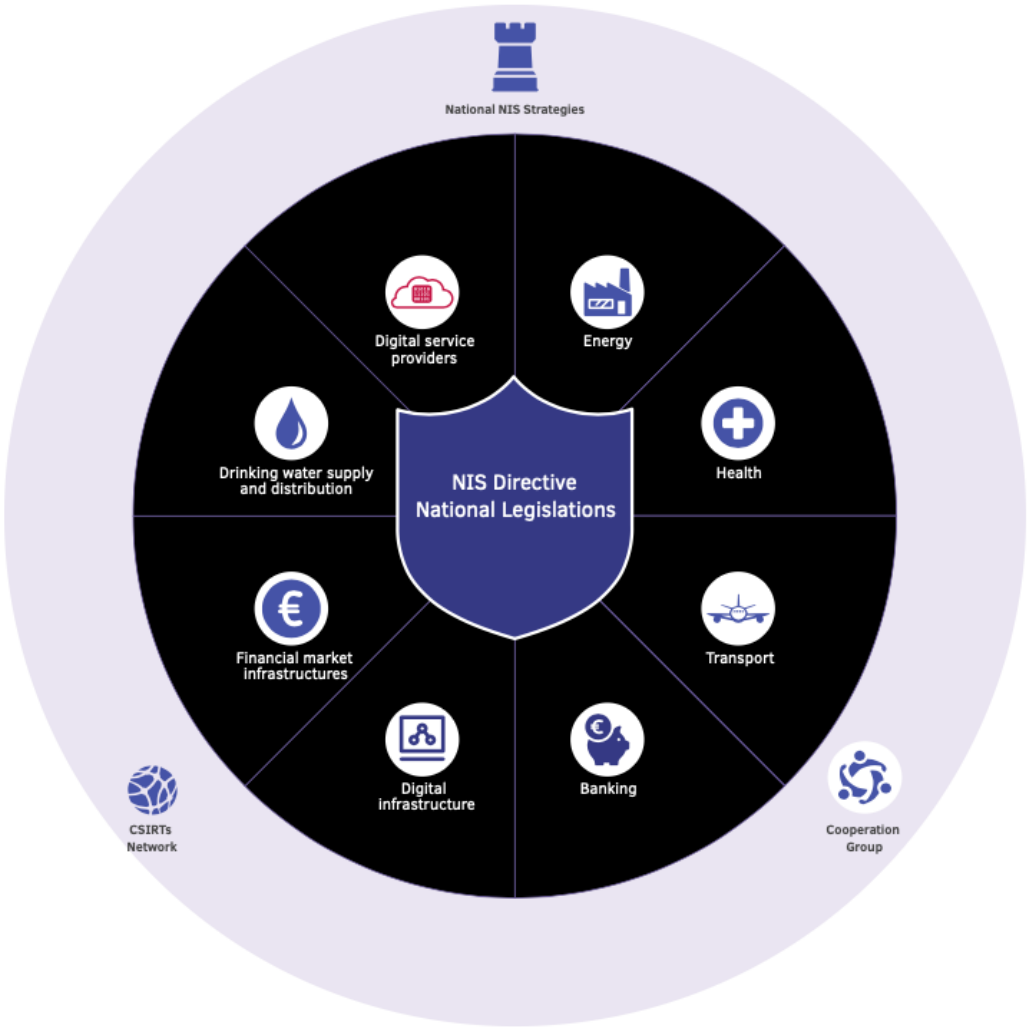
Digital Service Provider (DSP): A digital service provider is an entity who provides one or more of the three types of digital service:

- **Cloud computing services:** digital services that enable access to a scalable and elastic pool of shareable computing resources.

[8] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities
[9] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv3_documents/GCI%20V3%20Reference%20model.pdf
[10] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

- **Online marketplaces:** digital services that allow consumers to conclude online sales or service contracts with traders online using computing services provided by the online marketplace.
- **Online search engines:** digital services that allow users to perform searches of, in principle, all websites or websites.

Figure 1: NISD sectors (Source ENISA)



2. METHODOLOGY AND DATA COLLECTION

2.1 OVERVIEW OF THE METHODOLOGY

The methodology to identify, collect and analyse data on Incident Response set-up and capabilities within the NISD sector is illustrated in the graphic below. It aggregates a succession of steps which are presented in this chapter.

Figure 2: Overview of the methodology

2.2 A SEVEN-STEP APPROACH

2.2.1 Step 1 – Definition of the research focus for the data collection

The research focus of the study was defined by building an analysis grid to be used to classify the information collected on Sectoral IRC, by defining a set of analysis criteria and theme.

The list of criteria was defined according to elements of interest for ENISA and additional criteria pertaining to the specific data sought in the context of this study (e.g. cooperation aspects, recently created entities, etc.).

The list of criteria defined are presented in Annex 1.

2.2.2 Step 2 – Desktop research in open source on NISD Sectors IRC

This step consisted in conducting a literature review and open source research to collect data on sectoral IRC and recent trends in the field of IRC.

During this step, the research team used the pre-defined classification criteria to build an analysis grid. The purpose of this analysis grid was to facilitate the data collection by focusing the research work on the key topics of interest for ENISA and to present the raw data in a structured way.

During a preliminary data collection phase, the relevant data was gathered in the data classification grid by a first team of analysts. The preliminary data was then validated and further enriched by a second team of analysts.

2.2.3 Step 3 – Designing and validating the survey

Publicly available information on Sectoral IRC procedures and tools was, as anticipated, not detailed enough to provide insightful input (see part 3.1.2). It was therefore planned early on to conduct a survey to collect comprehensive data from relevant parties.

Once the objective of the survey was defined, two categories of organisations were identified to participate to the survey:

- 28 Member States' national CSIRTs and Norway;
- Additional sectoral CSIRTs from the 28MS and Norway.

Norway has also been included in the scope of the study because it provides interesting case studies within its financial sector including FinCERT, an entity involved in the IR for Financial sector also in other Nordic countries. The country is highly digitalised and faced important cyber-attacks targeting their operator of essential services in the past leading to the early creation of sectoral IRC, before the publication of the NISD.

The Project Team then drafted the survey which could be sent to both audiences considering aspects such as data protection, privacy and legal aspects, language, size and format, and structure.

2.2.4 Step 4 – Conducting the survey and complementary interviews

The survey was sent by ENISA to the 28 national CSIRTs and additional sectoral CSIRTs CSIRTs that were recommended by CNW members. To maximise participation the survey included a presentation of the study and its context.

Targeted emails were sent to relevant contacts and followed-up on, to ensure answers from a maximum of Member States and sectors.

Following the survey, additional interviews were conducted to complement and further enrich the data collected with the survey and desktop research with both:

- National and sectoral CSIRTs who replied to the survey;
- National and sectoral CSIRTs who did not reply to the survey.

A list of entities was drafted for each with a rationale for the interview which was validated by ENISA.

Once an organisation agreed to participate in the interview, a timeslot was scheduled and a list of 6 to 7 questions was sent to the interviewees ahead of the interview based on the answers provided in the short questionnaire or additional element to fill in information gaps.

2.2.5 Step 5 – Collation of raw data

The raw data collected from the desktop research, the survey and the interviews, was gathered in structured tables in a collaborative tool.

The collaborative tool allowed the aggregation of all raw data, the generation of statistics and the identification of key input.

2.2.6 Step 6 – Analysis and identification of trends

The methodology used in this step was a qualitative use of the Delphi Method, which ensures that the data collection team and the data analysis team benefit from and build on each other's expertise, and that the final analysis addresses all aspects of the request presented in a concise, coherent and comprehensive way.

A first analysis of the raw data was made by the data collection team and the data analysis team to develop a draft set of key findings. Once analysis methods were applied, a first version of the key findings of the study was drafted and subjected to validation and further discussion.

At a second stage, a virtual workshop held via videoconference was organised with members of the ENISA Informal Expert Group on Sectoral Incident Response Capabilities[13].

Once the virtual workshop was held and all final comments received, a second version of the key findings of the study was drafted and subjected to validation and further discussion.

2.2.7 Step 7 – Final report

This final step consisted in further developing findings of specific interest to ENISA and in drafting the final report of the study in collaboration with the member of the IEG.

2.3 OVERALL ASSESSMENT OF THE DATA & INFORMATION AVAILABILITY

The identification of reliable and qualitative data was crucial throughout the study. For each of the three activities conducted during the study, namely the desktop research phase, the survey and the complementary interviews, an overall assessment the data and information availability was conducted, and several assumptions are noteworthy.

2.3.1 Desktop research – Data collection assessment

During the open-source desktop research phase, information on IR layout and set-up were collected for 17 out 28 Member States.

- The clarity and level of information available on the national IR approach in NISD sectors was very different from one Member States to another and not all of them had information publicly available;
- **Information on procedures, processes and tools used by Sectoral IR teams were rarely, if ever, detailed in publicly available documents**;
- Publicly available information about cooperation models or cross-border procedures was not detailed;

[13] https://www.enisa.europa.eu/topics/csirt-cert-services/reactive-services/informal-expert-group-on-eu-ms-incident-response-development/

- Qualitative information on information exchange communities and fora were rarely, if ever, detailed in publicly available documents.

2.3.2 Survey – data collection assessment

The survey collected answers from 24 respondents: 18 National CSIRTs and 6 Sectoral CSIRTs from 17 Member States and Norway (knowing that the minimum planned requirement was responses from 15 MS).

- Efforts were made to cover all Member States, but the survey was conducted between June and August, a challenging moment to find available yet relevant respondents;
- A majority of respondents were National CSIRTs, resulting in the **collection of input more focused on national approaches towards IR in NISD sectors rather than sectoral approaches and capabilities**;
- 18 out of 24 respondents provided one or several qualitative comments through the survey.

2.3.3 Interviews – data collection assessment

In total, 8 complementary interviews were conducted: Two with national CSIRTs representatives and one with a Sectoral CSIRT representative who had replied to the survey. One with a sectoral expert who did not participate to the survey and four with experts from the Informal expert group.

- Efforts were made to collect additional inputs from sectoral stakeholders. It allowed to draft interesting case studies but not to develop an analysis at sectoral level;
- The interviews allowed to get deeper insights on procedures, processes and tools used within the interviewees' organisation.

3. KEY FINDINGS

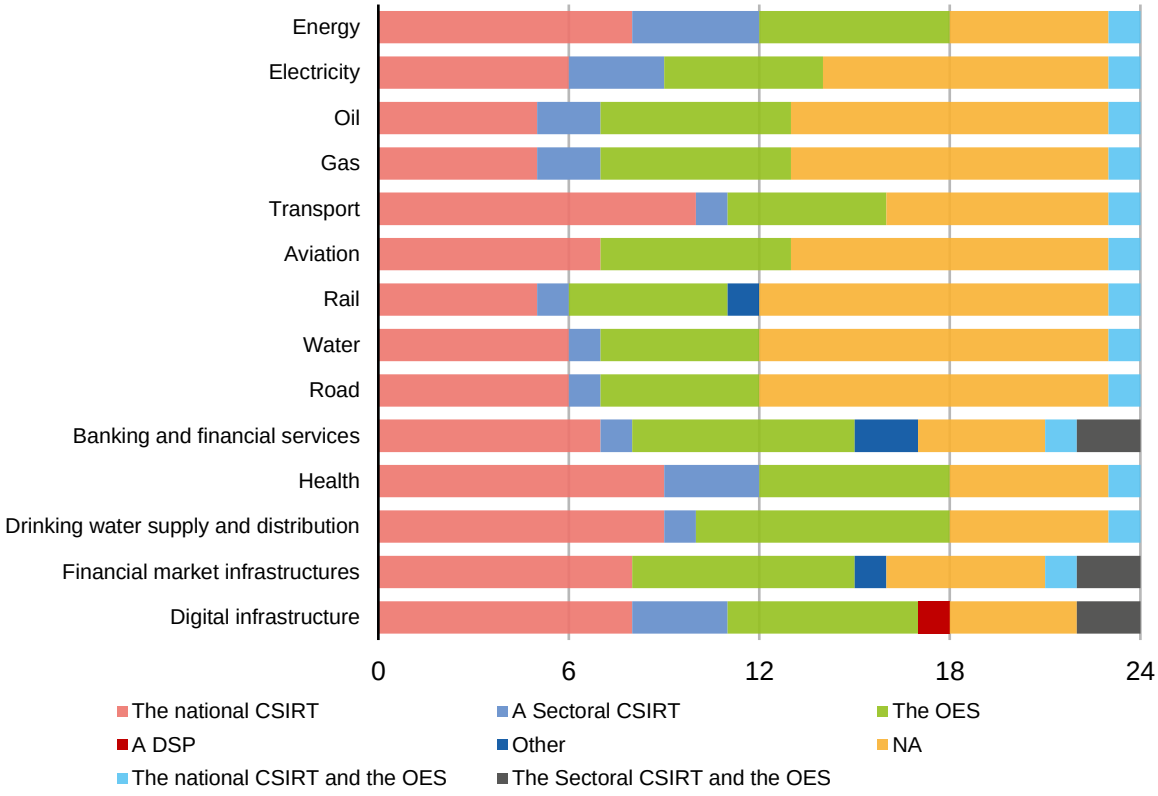
3.1 KEY FINDING #1

3.1.1 Member States' organisational culture and resources tend to shape IR layout and set-up

The sectoral Incident Response layout and set-up at national level across the EU is strongly impacted by the national organisational culture of each Member State. Countries with a very centralised state culture tend to have a centralised Incident Response model under the supervision of the national CSIRT, whereas decentralised countries tend to have more hybrid or decentralised models with sectoral CSIRTS in charge of Incident Response.

According to the survey and as illustrated in the graph below, the IR model is centralised or hybrid for 90% of the respondents and 100% of countries with centralised organisational culture have a centralised IR model.

Figure 3: Entity in charge of Incident Response by Sector



NB: The respondents to the survey could select the competent entity in charge of Incident Response within each sector and sub sectors. NA is the number of respondents who did not provide an answer for the sector or sub-sector. As an example, for the energy sector:

- The national CSIRT is the entity in charge or IR for the Energy sector for 8 respondents;
- A Sectoral CSIRT is the entity in charge or IR for the Energy sector for 4 respondents;
- The OES are the entities in charge or IR for the Energy sector for 6 respondents;
- 5 respondents did not provide answer to for this sector;
- Both the national CSIRT and the OES are the entities in charge or IR for the Energy sector for 1 respondent.

Based on Figure 1, all NISD sectors and/or sub-sector, the **main entities in charge of incident response for 51% of the respondent are the national CSIRT in cooperation with the OES.**

National CSIRTs and OES are the entity in charge of IR for 51% of the respondents

Table 1: Case study - Sectoral IR layout and set-up: France vs The Netherlands

Sectoral IR layout and set-up: centralised vs Hybrid models	
France	**The Netherlands**
Organisational Culture	
French governance and society have been shaped by a centuries-old trend towards centralization, beginning under the French monarchs and culminating in the French Revolution and the First Napoleonic Empire[14]. At the end of the 20th century, two major decentralisation Acts were adopted but these progressive measures are likely to take time to change this profoundly anchored governance culture.	Since 1848, the Netherlands has been a decentralised unitary state. The central government has trust in abilities of local and regional governments. The Minister of Interior affairs encourages decentralisation, especially with regard to local government, and is bound to that by the Municipalities Act (art. 117) but the central government guarantees the unity of state. [15]
Incident Response Model	
Centralised: the national CSIRT is in charge of handling incidents across the different sectors; it provides a centralised point for incident reporting and analysis, decision making, response coordination, and information dissemination.	**Hybrid:** a national CSIRT and the sectoral CSIRTs share the IR responsibilities and operations, which may depend for example on the sector(s) impacted or the scale of the incident.
National approach towards IR in NISD sectors	
In 2013, a dedicated CIIP regulatory framework was established: the “CIIP law”. The law is destined to apply to more than 200 public and private operators from 12 sectors already identified as critical in France. Security requirements will apply only to the operators’ most “critical information systems”. ANSSI[16] sets technical and organisational rules, mostly basic cyber hygiene measures common to all sectors. ANSSI can impose measures in case of a major crisis, declared by the Prime Minister. It lays down legal basis for action in the framework of crisis management plans[17].	The Dutch envision that every sector should set-up their own CSIRT. One of the new ambitions of their National Cyber Security Agenda is to create a network of cybersecurity partnerships, including sectoral and regional CSIRTs. NCSC-NL is the CSIRT for the central government and critical infrastructure providers / Operators of Essential Services (“Rijksoverheid”). Other governmental bodies like provinces and municipalities are responsible for their own information security.

[14] Centralization and Decentralization in French History, John Loughlin
[15] https://www.oecd.org/regional/regional-policy/Netherlands-experience.pdf
[16] The French national Cyber and Information security Agency
[17] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

	Some sectors do not (yet) have a CSIRT but there are Information Sharing and Analysis Centre (ISACs) for more sectors than defined in the NISD.
Incident Response layout and operational set-up	
Competent authorities in charge of Incident Response	
The Agence Nationale de la Sécurité des Systèmes d'Information or ANSSI (and more precisely CERT-FR, the national CSIRT) is in charge of IR for the 12 NISD sectors identified.	OES are in charge of Incident Response for the Energy, Transport, Banking and financial services, the Drinking water supply and distribution, and the Financial market infrastructure sectors. The Water, Health and Digital Infrastructure sectors have a sectoral CSIRT.
Sectoral CSIRT roles	
There are no sectoral CSIRTs in France, but mature sectors have created sectorial cyber expertise groups.	Sectoral CSIRTs roles depend on the sector and maturity of the CSIRT. NCSC-NL encourages sectoral CSIRTs to develop towards supplying all elements of the NISD-framework. All ISACs are mature and have been in operation for years.
Authority to which to report incidents	
For each sector, OES have to report incidents to the national CSIRT.	For the Energy, Transport, Banking and financial services, drinking water supply and distribution, and Financial market infrastructure sectors, incidents must be reported to the national CSIRT and the sectoral competent authority. For the Water, Health and Digital Infrastructure sectors, incidents must be reported to the Sectoral CSIRTs and the sectoral competent authority.
Main challenge identified for the implementation of the NIS Directive within sectors	
Organisational challenge: find the right governance model between national and sectoral actors.	**Organisational challenge:** find the right governance model between national and sectoral actors. **Regulatory challenge:** develop the right legal framework enabling the uptake of security requirements and the notification of incidents.

The **national CSIRT's mandates and financial resources** also strongly impact the sectoral Incident Response layout and set-up.

Within each Member State, National CSIRTs can have different mandates, among others:

- Raising awareness on threats;
- Identifying risks;
- Protecting and hardening systems;
- Deterring attacks;
- Monitoring and detecting incidents;
- Responding to incidents;
- Recovering from incidents;
- Integrating and disseminating lessons learned.

As an illustration, when building CERT-UK, the United Kingdom's national CSIRT, the UK Cabinet Office identified 47 possible functions of a national CSIRT, but ultimately prioritised only four in the creation of CERT-UK[18].

Another interesting case to mention is the Czech Republic layout. The Czech governmental CERT constituency is consists of owners of important information networks and providers of essential services (energy, etc.). The national CSIRT provides Incident handling for all other subjects within the sectors and some private subject have their own IR teams[19]. Hence, there are no sectoral CSIRTs in the Czech Republic.

Sectoral IR layout depends strongly on the national CSIRT mandate and budget

The research highlighted that several national CSIRTs' mandates do not include Incident Response, often because of a lack of resources. National CSIRTs tend to delegate functions such as identification of Operator of Essential Services (OES) and Incident Response activities to sectoral authorities and sectoral CSIRTs. Additionally, even if national CSIRTs do not include the IRC, they do include and are responsible for national Incident coordination.

Table 2: Case Study Sectoral IR layout and set-up: Portugal

Sectoral IR layout and set-up: Portugal
National CSIRT Mandate
The CERT.PT is a service integrated in the Portuguese National Cybersecurity Centre that **coordinates the response to incidents involving State entities, operators of essential services, digital service providers** and, in general, the national cyberspace, including any device belonging to a network or address block attributed to an operator of electronic communications, institution, collective or singular person based, or physically located, on Portuguese territory.
National CSIRT – Key resources
• Resources: The National Security Cabinet provides a budget to the Portuguese national CSIRT. The National Cybersecurity authority's budget was not increased after the transposition of the NISD, which led to the delegation of certain tasks and responsibilities to sectoral authorities (such as the identification of OES).
National CSIRT services
• Incident Handling Coordination • Incident Reporting • On-Site Support • CSIRT Capability Building • Security Alerts
Incident Response Model - Distributed
The Portuguese National Cybersecurity Centre The coordination of the response to incidents can be an initiative of the Portuguese National Cybersecurity Centre, for example in the case of a large-scale incident, or it may be requested through the established communication channels. In case of necessity or force majeure, the Portuguese National Cybersecurity Centre coordinates with other national authorities. **The national CSIRT** is in charge of: • Sorting incident notifications and technical forensic analysis; • Coordinating with the national and international entities involved;

[18] http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf
[19] Interview with the Czech National Cyber and Information Security Agency (NÚKIB)

• Producing recommendations for the mitigation and/or resolving of incidents. **The sectoral authorities** are in charge of: • Identifying OES within their sectors; • Mapping dependencies; • Supervising cybersecurity. **The sectoral CSIRTs** are in charge of: • Incident Management; • Artefact analysis; • Information Assurance; • Situational awareness; • Communication/outreach. **The OES** in NISD sectors are in charge of: • Taking appropriate measures to prevent incidents affecting networks and information systems; • Reporting incidents to the national CSIRT.
IR in NISD sectors – Entity in charge
• The OESs' CSIRT are in charge of IR in the Energy, Transport, Health, Drinking Water, Financial Market and Digital Infrastructure sectors (sectoral CSIRTs are planned in the Energy and transport sectors); • A sectoral CSIRT is in charge in the Banking sector.
Impact of the NIS Directive on IR layout
The NIS Directive led to the improvement of the CSIRT/IR national layout already in place but did not increase the national Cybersecurity authority's budget, which is why the identification of OES was delegated to sectoral authorities.
Sources
https://www.cncs.gov.pt/en/certpt_en/ Survey Interviews with experts

3.1.2 Lessons learned and recommendations

• The organisational culture of a country could be further taken into account when analysing the Incident response model of European countries.

• A deeper insight into MS national CSIRTs' mandates would be an interesting topic to be further studied by ENISA to better assess the overall IR layout. This could be done by using CSIRT maturity products[20].

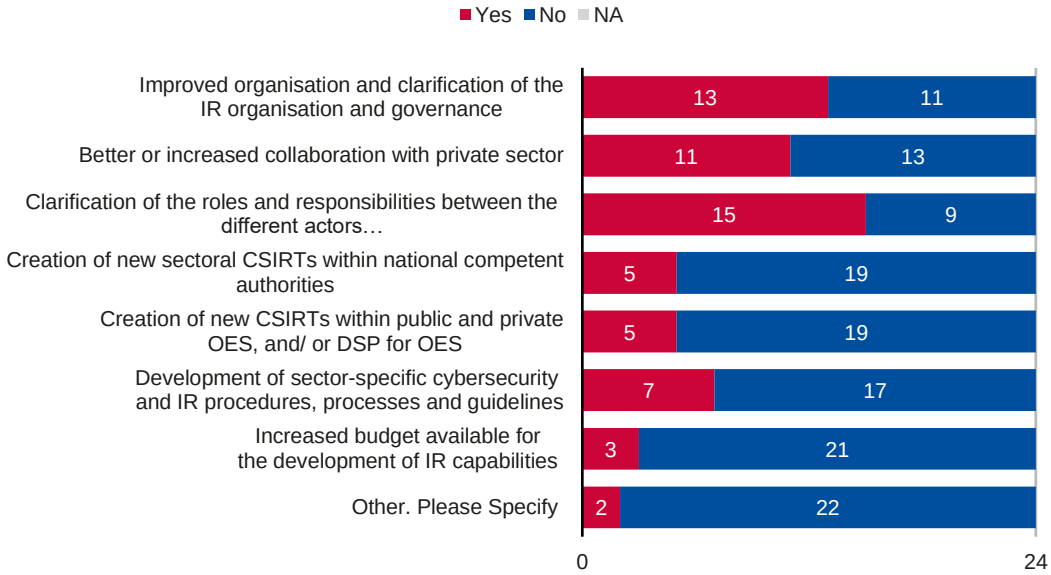
[20] http://www.enisa.europa.eu/csirt-maturity

3.2 KEY FINDING #2

3.2.1 The NIS Directive has improved the IR organisation and governance by clarifying actors' roles and responsibilities

The transposition of the NIS Directive into national legislation seems to be having a positive impact on the Incident Response (IR) landscape at national level, contributing to improved overall organisation and governance.

Figure 4: Main features of the changes following the NIS Directive



According to national CSIRTs, the Directive has led to a clarification of the roles and responsibilities of the various actors involved in IR at all levels, and the ongoing implementation is leading to significant organisational changes, including:

- The formal identification of OES;
- The creation of sectoral CSIRTs.

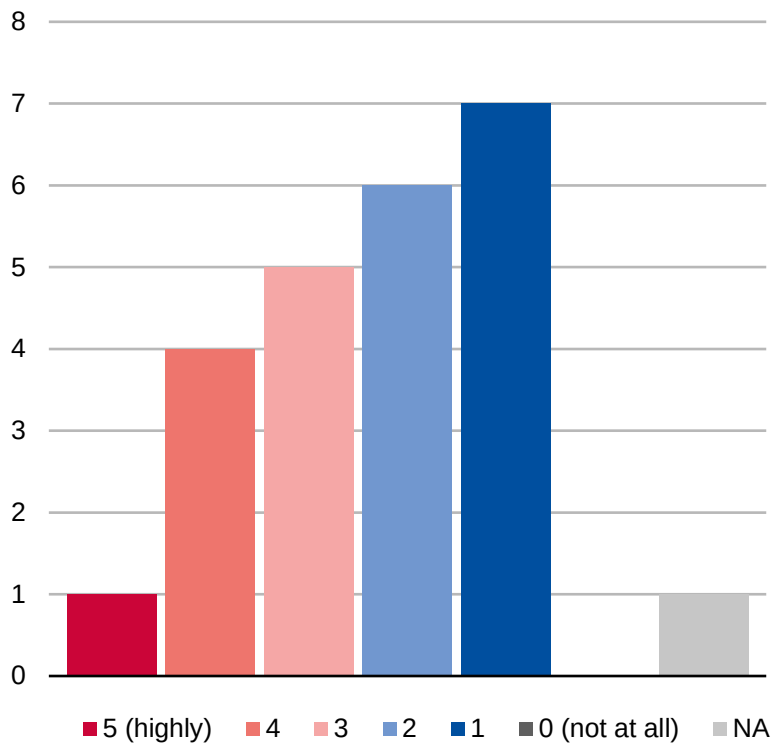
This positive impact is less visible in countries with a more mature organisational layout. **The data collected indeed suggest that the NISD had an unequal effect from one country to another.**

The NISD has had a positive impact on the clarification of the roles and responsibilities of IR stakeholders.

During the survey, respondents were asked about the impact of the NISD of the set-up of their IR capacities on a scale from 5 (high impact) to 0 (no impact). The replies show that:

- 10 out of 24 respondents thought that the NISD had an important impact (5 to 3);
- 13 out of 24 respondents thought that the NISD had a relatively small impact (2 to 0);
- 1 respondent did not provide an answer.

Figure 5: Evaluation of the changes on the CISRT/IR layout and operational set-up



"Before the transposition of the NISD we had a law and strategy that already set this way. The NISD was treated as an update to the previous law and continues the way of thinking." (National CSIRT)

"The NISD didn't change much, since we were working in the same way before." (National CSIRT)

According to the results of the survey, **the countries who tend to be less impacted by the Directive are the countries with a more mature landscape who already had a clear governance and definition of roles and responsibilities**.

The evolution of the maturity of MS IR landscape could be an interesting area to further study by using the ENISA CSIRT Maturity Toolkit[21] based on SIM3 (https://opencsirt.org/maturity/sim3/).

These mixed results highlight the fact that there are still important differences between Member States' cybersecurity landscape and IRC at large.

3.2.2 Lessons learned and recommendations

- Based on received data, it would be interesting to have another round of analysis to evaluate the mid- and long-term impacts of the NIS Directive on IR layout once the NISD has been completely implemented in all the MS.

It would be useful to conduct a maturity assessment of sectoral CSIRT landscape within NISD sectors (using ENISA CSIRT Maturity Toolkit as a basis) and to identify future changes.

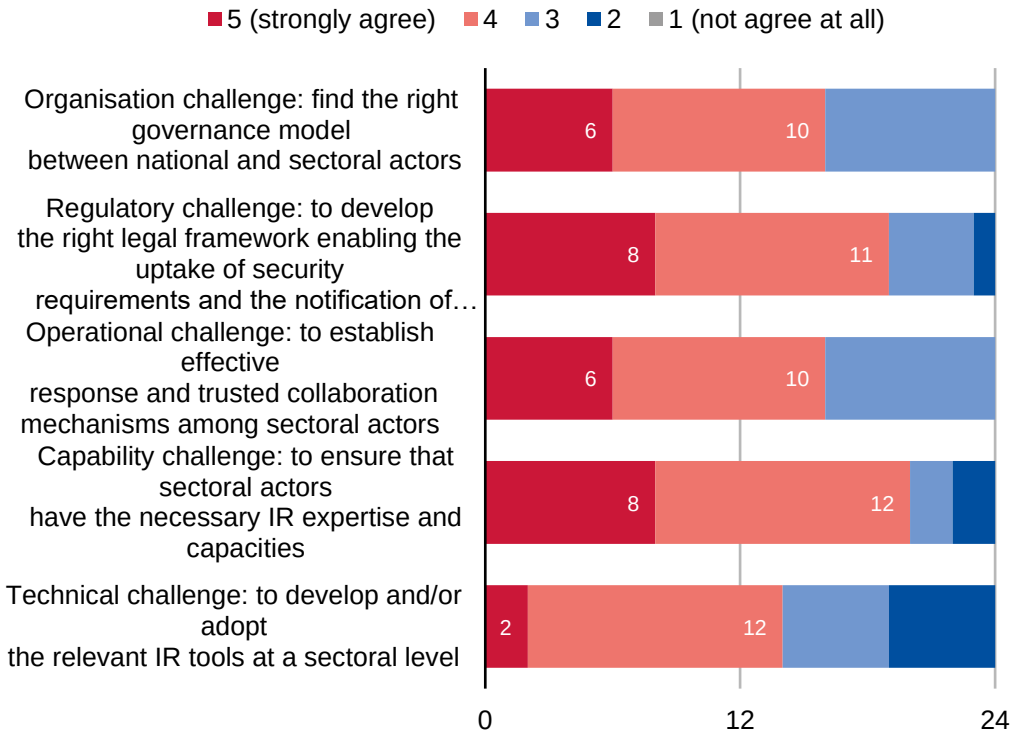
[21] http://enisa.europa.eu/sas-tool

3.3 KEY FINDING #3

3.3.1 The implementation of the Directive raises operational and regulatory challenges and highlights MS willingness to move forward by extending the scope and number of sectors targeted

Following the transposition of the Directive into national legislation, EU Member States are now in the process of implementing the regulation. The two main challenges raised by respondents and confirmed by sectoral experts are regulatory and operational.

Figure 6: Assessment of the challenges faced during the implementation of the NISD



NISD implementation poses regulatory and operational challenges

The **legal and administrative definition of what constitutes an OES** can pose a challenge for the authority in charge of defining the list of OES within the NISD Sectors. There are two issues in defining the OES:

- The legal definition and threshold/criterion of what constitutes an OES;
- The administrative identity of the OES: Name, headquarter, VAT number, etc.

The threshold and criterion to identify the OES are defined by the authority which can be the national cybersecurity authority, the sectoral authority or another competent authority. The Directive provides an initial list of entities, but each MS has to define the thresholds and criterion for the sectors which can be based on quantitative aspects (share of market, tons of freight, etc.).

Table 3: Case-study: Maritime transport OES definition & threshold (United Kingdom)

Definitions and thresholds for identification of Operators of Essential Services in the United Kingdom maritime transport sector[22]	
Essential service	**Identification Thresholds**
Shipping	A shipping company which handles (a) over 5 million tonnes of total annual freight at UK ports; and (b) over 30% of the freight at any individual UK port which fulfils at least one of the following criteria: (I) handles more than 15% of UK total roll-on roll-off traffic; (II) handles more than 15% of UK total lift-on lift-off traffic; (iii) handles more than 10% of UK total liquid bulk traffic; or (iv) handles more than 20% of UK biomass fuel traffic; or A shipping company with over 30% of the annual passenger numbers at any individual UK port which has annual passenger numbers greater than 10 million.
Provision of services by a harbour authority	A harbour authority (as defined in section 313(1) of the Merchant Shipping Act 1995) which (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) handles more than 15% of UK total roll-on roll-off traffic; (ii) handles more than 15% of UK total lift-on lift-off traffic; (iii) handles more than 10% of UK total liquid bulk traffic; or (iv) handles more than 20% of UK biomass fuel traffic.
Provision of services by an operator of a port facility	(a) An operator of a port facility which handles passengers at a port which has annual passenger numbers greater than 10 million; or (b) An operator of a port facility at a port which fulfils at least one of the following criteria: (i) handles more than 15% of UK total roll-on roll-off traffic; (ii) handles more than 15% of UK total lift-on lift-off traffic; (iii) handles more than 10% of UK total liquid bulk traffic; or (iv) handles more than 20% of UK biomass fuel traffic; and where that port facility operator handles the same type of freight for which the port fulfils one of the criteria mentioned in sub-paragraphs (i)-(iv). "Port facility" has the same meaning as in regulation 2 of the Port Security Regulations 2009.
Vessel traffic services	Operator of vessel traffic services at a port which (a) has annual passenger numbers greater than 10 million; or (b) fulfils at least one of the following criteria: (i) handles more than 15% of UK total roll-on roll-off traffic; (ii) handles more than 15% of UK total lift-on lift-off traffic; (iii) handles more than 10% of UK total liquid bulk traffic; or (iv) handles more than 20% of UK biomass fuel traffic. "Vessel traffic services" has the same meaning as in regulation 2(1) of the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 20049.

The identification of all the OES can be an **operational challenge in sectors with an extended range of suppliers and service providers.** Sectors which include various public and private actors can depend strongly on SMEs in their value chain. Should these SMEs be targeted by a cyberattack, this could impact the entire value chain. It is therefore complex for the

[22] http://www.legislation.gov.uk/uksi/2018/506/schedule/2/made

regulator and/or the entity in charge of listing OES (be it the national CSIRT, the Sectoral Authority or the sectoral CSIRT) to map the dependencies and identify all the OES within the sectors and set-up thresholds.

Finally, classifying OES can become complex in the case of large companies who have more than one activity/branch which falls under the scope of NISD (e.g. an IXP (OES) might also operate as a cloud provider (DSP)). This could result in a company reporting to several sectoral authorities in a decentralised IR model, generating overlaps and duplication between the competent authorities.

Regulatory challenge: information-sharing and incident notification

A regulatory challenge posed by the implementation of the Directive concerns information-sharing with third countries, especially when there is not an adequate legal basis under GDPR for such sharing. A national CSIRT analyst may find actionable information which could be of great help for another country, but he/she may not legally be able to share this information with that other country's authority.

As an example, in order to mitigate relevant challenges, the transposition of the NISD into Dutch law allows the NCSC-NL (CISRT for government and OES in the Netherlands) to share actionable information outside of its mandate to third countries' IR entities as long as the entity is a CSIRT and if it is believed that the entity has the capacity to use the information and will do so in a reasonable manner.

Moreover, it should be noted that in the case of a security breach involving personal data (as e.g. in the bank, finance or health sector), aside reporting to the national CSIRT, the national Data Protection Authorities (DPAs) should be notified, according to GDPR..

According to one of the interviewee, there may be **a missing link between the national CSIRT and the national Data Protection Authority**, and it would be therefore interesting to think of a communication channel between the two types of authorities covering the incidents where personal data is part of the security breach.

Extension of the scope and number of NISD sectors

NISD implementation is leading to significant differences among MS and, in some MS, to an extension of the scope and number of sectors covered

As mentioned above, the implementation of the Directive is still in progress in some Member States, but the research highlights significant differences among national operational set-ups:

While transposing the NIS Directive into national legislation, some Member States opted for using the 7 sectors listed in the NIS Directive (see Section 3.1 Definition) while others decided to extend the scope and number of sectors covered:

- **12 out of 28 MS have extended the scope of NISD sectors** and added entities not listed in the NISD as OES.

The sectors mostly added are electronic communications/telecommunication networks (for 7 out 12 MS) and chemical Industry.

Table 4: Extended scope of sectors and OES

NISD transposition into national legislation – extended scope of the sectors (examples)	
Different and/or additional sectors identified	**Different and/or additional categories of OES included**
Cyprus	
Additional sectors considered: electronic communications, wastewater, food, government and national security/ emergency services and environmental.	OES related to the additional sectors included.
Czech Republic	
Additional sector considered: chemical industry.	OES related to the additional sectors included.
Estonia	
Additional sector considered: electronic communication, public media.	Under the Estonian implementation legislation, Operators of Essential Services also include Electronic communication service providers, public broadcasting, providers of digital identification and digital signing service and district heating service providers. Within the Health sector, small-scale medical clinics are included as OES. Estonia goes further in its definition of important services and the setting the threshold for being considered OES, in addition to that provided for in the NIS Directive.
Finland	
Finland has identified 7 vital societal functions: leadership, international and EU affairs, national defence, domestic security, economy, infrastructure and security of supply, services for citizens, psychological resilience.	Under Finnish national legislation industries such as online marketplaces, search engines, cloud providers and other digital infrastructures are considered OES.
France	
France has identified 12 sectors[23]: - Energy: as in the NIS; - Transport: extended to guided transport and logistics: - Finance: extended to insurance; - Health: extended to pharmaceutical distribution network; - Food industry: new sector; - Water: extended to water treatment sector; - Military activities of the State; - Judiciary activities of the State; - Civilian activities of the State; - Electronic communication, audio visual & information; - Industry;	Industries that are considered OES under French legislation include industries involved in state civil, judicial and military activities, food, electronic, audio-visual and information communication, space and research, and finance industries.

[23] http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

- Space and research.	
Germany	
Germany's Ministry of interior proposed a Draft Bill on March 27th, 2019 to extend the list of existing critical infrastructure sectors (KRITIS) (currently energy, water, information technology/telecommunications, food, health, finance/insurance and transportation/traffic) by including waste management as an additional KRITIS sector[24].	The bill proposes to expand to two new sets of entities: (i) "infrastructures of special public interest"; and (ii) operators with "cyber-criticality". The definition of "infrastructures in the special public interest" covers companies in three different sectors: (i) defence; (ii) cultural and media sector; and (ii) "companies of considerable economic importance". The explanatory memorandum also mentions the automotive and chemical industry; However, these sectors are not included in the Draft Bill itself.[25]
Lithuania	
Additional sectors considered: industrial sector, chemical and nuclear sub-sector, state administration, civil safety, environmental, national defence and foreign and security affairs.	OES related to the additional sectors included.
Poland	
Additional sectors considered: heating and mining.	OES related to the additional sectors included.
Slovakia	
Additional sector considered: pharmaceutical/ chemical industry, public administration, electronic communication, postal service.	OES related to the additional sectors included.
Slovenia	
Additional sector considered: environmental protection industries.	OES related to the additional sectors included.
Sweden	
Additional sector considered: Telecommunications.	OES also include Telecommunication Critical operators.
The Netherlands	
Additional sector considered: nuclear energy, telecommunications networks and water regulation.	In the Netherlands, the list of OES also includes essential operators of the additional sectors: nuclear energy, telecommunications networks and water regulation.

3.3.2 Lessons learned and recommendations

- An overview of all MS NISD sectors (including additional ones) should be published by ENISA to allow MS or sectoral actors to leverage synergies between sectors;
- MS who have already defined their OES could continue sharing their lessons learned and good practices. This information should be made available to the authorities in charge of defining OES and identifying the OES if different.

[24] https://www.jdsupra.com/legalnews/germany-s-draft-bill-on-it-security-2-0-55094/
[25] Ibid

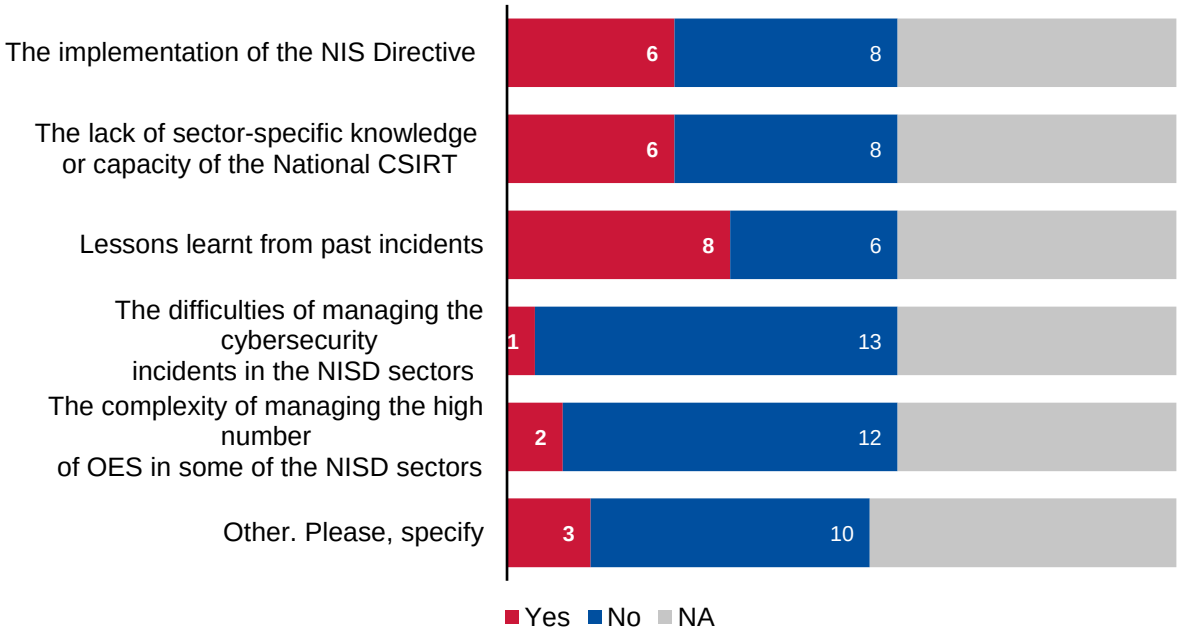
3.4 KEY FINDING #4

3.4.1 A blend of bottom up and top down incentives could be the most efficient driver for the creation of sectorial CSIRTS, depending on MS IR layout maturity.

The NIS Directive is one of the three key drivers for the creation of sectoral CSIRTs, along with lessons learned from past incidents and the lack of sector-specific knowledge of the national CSIRT, according to the respondents.

"[The creation of the sectoral CSIRT was driven by] a need to collaborate and coordinate Incident Response against ongoing cyberattacks" (Sectoral CSIRT)

Figure 7: Key drivers to create sectoral IR capabilities

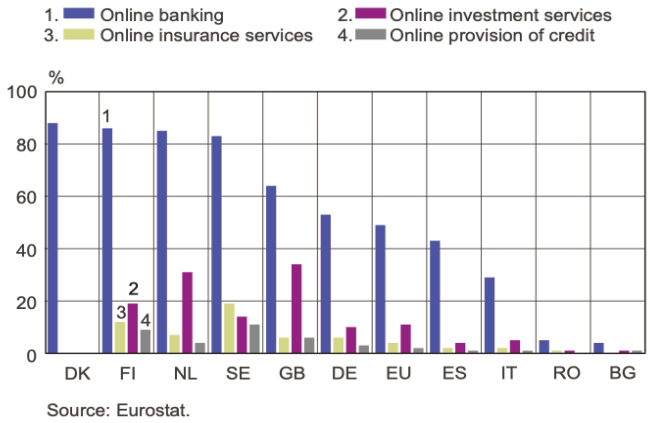


Demand-driven

For 8 out of 24 respondents, the creation of sectoral IRC was driven by lessons learned from past incidents while for 6 out of 24 respondents it was the lack of either sector-specific knowledge or national CSIRT capacities. In other words, according to the survey, a bottom-up (demand-side) incentive favoured the creation of sectoral IRC.

In some of the cases, operators of essential services (public or private entities) created a sectoral CSIRT on their own initiative. This is also the case for non-EU sectoral CSIRTs such as the NordicFin CERT which provides a good illustration of a cross-border sectoral IRC set up prior to the publication of the NISD to respond to an operational need.

Table 5: Case Study NordicFin

Financial Sector – A need for OES to collaborate at sectoral level nationally and regionally
A highly digitalised Financial sector in Nordic countries – vulnerable to cyber attacks
According to the Digital Economy and Society Index (DESI), the most digitalised countries in Europe are Denmark, Finland and Sweden[26]. They adopted digital financial services such as online banking, digital investment services or online provision of credit early, as illustrated in the chart below. **Online banking more common in Finland than in many other euro area countries**    Source: Eurostat. According to The Bank of Finland Bulletin, "*Not only have banks in the Nordic countries invested in digitalisation; the position of new FinTech actors is also better in the Nordic region than in many other countries.*" This growing digitalisation of the Nordic financial sectors opened new vulnerabilities to cyber threats.
A need to collaborate to better respond to an increasing number of cyber attacks
From 2007 to 2016, Nordic countries experienced numerous attacks on their financial sector. In 2007, Norway was targeted by their first internet banking malware attacks. Between 2008 and 2011, financial operators collaborated through both formal and informal schemes to respond to cyber incidents. In 2012, Sveriges Riksbank (central bank of Sweden) was hit by a Distributed Denial of Service (DDoS) attack which left its website offline for 5 hours. In 2014, a DDoS attack on seven large financial institutions in Norway resulted in suspended services for an entire day. In Finland, at the end of 2014, three banks (Op Pohjola, Danske Bank and Nordea) suffered DDoS attacks that rendered their online services unavailable and for one bank prevented customers from withdrawing cash and making card payments.
Lessons learned from incident called for IR cooperation at national level
In 2012, in Norway, while the National Cyber Security Strategy was in the process of being created, the country experienced a peak of attacks and decided to set up a national platform, FinansCERT, dedicated to responding to cyber threats targeting the financial sector. FinansCERT was created to formalise collaboration between relevant actors, and actively cooperates with the national CSIRT and with the law enforcement computer crime unit. FinansCERT Norway, based in Oslo, was operational from 2013 to 2017.
A demand from operators to create a cross-border capability to collaborate to fight cybercrime
In 2017, the largest banks operating in the Nordic countries, namely Nordea, Danske Bank and DNB worked on a project to set-up a single payment clearance system which would be operated by one company for all the Nordic countries. To secure this project and face a

growing number of attacks, Danske Bank, Nordea, DNB, Sparebank 1 and Eika Group, among other Nordic banks, decided to expand FinansCERT, to develop a collaboration platform to the entire Nordic region: Nordic Financial CERT (NordicFin CERT).
Nordic-Fin CERT mandate
The Nordic Financial CERT aims at fortifying the Nordic community in the face of cyber risks to customer assets and at providing a safety net for all financial institutions, big and small. It envisions a Nordic community in which the financial sector actively and responsively identifies, defends against and combats cyber risks. The collaboration will enable the banks to gather the best knowledge available about fighting cybercrime in the Nordic financial sector, and it will lead to synergies that will improve both the customers' and the banks' security.
Sources
https://www.bofbulletin.fi/en/2018/2/nordic-banks-go-digital/ Cyber Risk for the Financial Sector – IMF, A. Bouveret, 2018 https://www.nordea.com/en/press-and-news/news-and-press-releases/press-releases/2017/04-10-08h00-nordic-banks-collaborate-on-fighting-cybercrime.html

Regulation-driven

For other Member States, the NIS Directive was the main reason for initiating such capacities. As a result, their sectoral capabilities are recent or still work in progress. In those cases, the NIS Directive and the GDPR were an opportunity to justify the need for additional resources to increase capabilities and create sectoral CSIRTs. However a major increase of financial resources was rarely noted according to the data collected.

- It was the implementation of the NIS Directive for 6 out of 24 respondents, which was the main driver for the creation of Sectoral capabilities.

As an illustration, Bulgaria is in the process of creating seven sectoral CSIRTs as a consequence of the transposition of the NISD in the national legislation.

In some cases, the creation of sectoral capacities is driven by both national authorities and operators. This is the case in The Netherlands, which features many sectoral CSIRTs although the national CSIRT (and cybersecurity agency) also play a proactive role.

The support of national CSIRTs to the development of sectoral CSIRTs and capabilities tends to be of great added value because it capitalises on existing expertise.

The support of national CSIRT to develop and enhance Sectoral IRC is key to capitalise on existing expertise

A noteworthy initiative, pre-dating the NIS Directive, is that of the Dutch NCSC, which provided incentives and guidelines to support the creation of CSIRTs:

- Guidelines to start a collective CSIRT[27];
- Guidelines to operationalise a CSIRT: NCSC' CSIRT Maturity Toolkit[28].

NCSC-NL also appointed a liaison officer whose mission was to follow the creation of sectoral CSIRTs. The liaison officer came to the sectoral CSIRT's premises 2 days a week to support the newly created team.

[27] Guidelines to start a collective CSIRT
[28] https://english.ncsc.nl/get-to-work/cooperation/i-would-like-to-strengthen-my-collaboration/csirt-maturity-toolkit

It also worth mentioning that countries with a centralised Incident Response model tend not to have, nor to plan to develop specific sectoral CSIRT capabilities since the national CSIRT tend to have sectoral IR teams within its structure. In these countries, IR is directly managed by the OES and reported straight to the National CSIRT or governmental CSIRT such as in Czech Republic (see Key Finding 1).

6 out of 24 respondents confirmed that there are no sectoral CSIRTs in their country.

"Currently we do not provide sectoral CSIRTs and there is no plan to create any" (National CSIRT)

100% of respondents with no sectoral CSIRT have a centralised IR model with national CSIRT as the competent authority for NISD sectors.

"We don't tend to use sectoral CSIRTs but [the national CSIRT] 's Engagements Team do maintain close contact with all NISD sectors." (National CSIRT)

3.4.2 Lessons learned and recommendations

- Sectoral actors could benefit from the experience and knowledge of national and other sectoral CSIRTs, for instance through the appointment of a liaison officer, sharing of know-how, expert advice or tailored training.
- ENISA should continue to collect available resources (guidelines and toolkits), for example by enabling a GitHub repository.

3.5 KEY FINDING #5

3.5.1 National CSIRTs have developed mature reporting processes and notification tools, as have sectoral CSIRTs who provide solutions specific to their sectors' needs

The nature of the capabilities developed and used by sectoral CSIRTs in contrast with national CSIRTs strongly depends on the range of services that both can provide to their constituents.

According to FIRST "CSIRT Services Framework[29]", CSIRTs can provides various cyber security services and functions:

Table 6: FIRST'CSIRT Services Framework V2.0

Services Areas	Services	Functions
Information Security Event Management	Monitoring and detection	Log and sensor management, Detection use case management, Contextual data management
	Analysing	Correlation
Information Security Incident Management	Accepting information security incident reports	Information security incident report receipt, Information security incident report triage and processing,
	Analysing information security incidents	Information security incident triage (prioritization and categorization), Information collection, Coordinate any more detailed analysis, Information security incident root cause analysis, Cross-incident correlation.
	Analysing artefacts and forensic evidence	Media or surface analysis, Reverse engineering, Run time and/or dynamic analysis, Comparative analysis
	Mitigation and recovery	Establishing a response plan, Applying ad-hoc measures and containment, Returning all systems back to normal operation, Supporting other information security entities,
	Information Security Incident Coordination	Communication, Sending notifications, Distributing relevant information, Coordinating activities, Reporting, Communicating with the media.
	Supporting crisis management	Distributing information to constituents, Reporting on cyber security status, Communicating strategic decisions
Vulnerability Management	Vulnerability discovery / research	Vulnerability discovery based on information security incident management, Vulnerability discovery via public sources, Vulnerability research, Vulnerability report intake, Vulnerability report receipt, Vulnerability report triage and processing
	Vulnerability analysis	Vulnerability triage (prioritization and categorization), Vulnerability root cause analysis, Vulnerability remediation development
	Vulnerability coordination	Vulnerability notification/reporting, Vulnerability stakeholder coordination

[29] https://www.first.org/education/csirt_services_framework_v2.0

	Vulnerability disclosure	Vulnerability announcement/communication/dissemination, Post vulnerability disclosure feedback
	Vulnerability response	Vulnerability detection, Vulnerability remediation
Situational Awareness	Data acquisition	Policy aggregation, distillation, and guidance, Mappings of assets to functions, roles, actions and key risks, Collection, Data processing and preparation
	Analyse and interpret	Projection and inference, Event detection (through alerting or hunting), Situational impact
	Communication	Communication, Reporting and recommendations, Implementation, Dissemination / integration / information sharing, Managing the sharing of information, Feedback
Knowledge Transfer	Awareness building	Research and information aggregation, Development of reports and awareness materials, Outreach
	Training and education	Knowledge, skill, and ability requirements gathering, Development of educational and training materials, Delivery of content, Mentoring, CSIRT staff professional development
	Exercises	Requirements Analysis, Format and environment development, Scenario development, Executing exercises, Exercise outcome review
	Technical and policy advisory	Risk Management Support, Business Continuity and Disaster Recovery Planning Support, Policy Support, Technical Advice

One of the most common services provided by both National CSIRT and Sectoral CSIRT according to the survey is **information security incident reporting**. To provide this specific service, **both National CSIRTs and Sectoral CSIRT have developed and/or use mature reporting processes and notification tools** to allow citizens, OES and other private or public-sector organisations to report incidents.

Notification and reporting tools of national CSIRTs and sectoral CSIRTs

According to the survey, 83% of respondents use incident notification templates and 100% have specific information-exchange tools to enable the notification of incidents.

The **reporting tools** used by both national CSIRT and sectoral CSIRT identified through the survey and the desktop research are:

- Email-based reporting tools (secured and/or encrypted), Secured networks/chats, Web forms, notification portals, collaboration portal, in-house developed tools (in-house notification portal, customized tool based on RTIR[30]).

REPORTING TOOLS
Email-based reporting tools (secured and/or encrypted), Secured networks/chats, Web forms, notification portals, collaboration portal, in-house developed tools (in-house notification portal).

OTHER TOOLS
Early detection systems, monitoring systems, Industrial control systems, Threat intels systems, Malware Information Sharing Platform (MISP), IntelIMQ, information sharing platforms and tools.

[30] RTIR - Request Tracker for Incident Response (RTIR) is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker.

The **other tools** identified are:

- Early detection systems, monitoring systems, Industrial control systems, Threat Intel systems, Malware Information Sharing Platform (MISP)[31], IntelMQ[32], information sharing platforms and tools.

Table 7: Case study: CERT-BE, Belgium

National CSIRT, dedicated notification tools for OES (Belgium)	
Context	
According to Belgian law, OES have to notify 3 or 4 different authorities: • The national CSIRT (CERT-BE); • The Centre for Cyber Security Belgium (CCB); • The Sectoral Authority; • *GDPR Authority (in case of data leak)*. A Belgian regulation states that Belgian citizens should only have to report to one authority and not duplicate the notification to other administrative entities, which resulted in the creation of a dedicated portal for OES to centralise notifications and systematically transfer the incident notification to the other 3 authorities.	
Notification tool for OES	**Description**
Online dedicated portal for OES	The form is accessible online on the CSIRT-DSP website and the notification is sent directly to both the CSIRT and the competent Authority;
Notification tool for all[33]	**Description**
Notification by email / encrypted email	A central email address is available on the CERT-BE website. The national CSIRT also offers to send a secure message by using an encrypted message with PGP encryption.
Exchange of information on incidents based on Traffic Light Protocol (TLP)[34]	CERT.BE uses the "Traffic Light Protocol" to facilitate and encourage the exchange of information in a safe manner. The protocol requires that the person sending information assigns it a colour code. This colour indicates if and in what ways this information may be further disseminated. Someone who receives information and believes that it should be further disseminated must first ask for permission from the sender.
Online notification form	The form is accessible online on the CERT-BE website and includes mandatory information to fill in.

[31] The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.
[32] IntelMQ is a solution for IT security teams for collecting and processing security feeds using a message queuing protocol (Github definition).
[33] https://www.cert.be/en/report-incident
[34] https://www.cert.be/en/traffic-light-protocol-tlp

Depending on their mandate, **sectoral CSIRTs tend to offer the same range of incident reporting and notification services as the national CSIRT**, including similar notification tools and reporting processes which rely mostly on web forms and email.

Table 8: Case study: DSP-CSIRT, The Netherlands

CSIRT for Digital Service Provider, notification tools (The Netherlands)	
Context	
In November 2018, the NIS Directive was transposed into Dutch legislation under the Dutch law on the protection of networks and information systems. According to this national regulation, Digital Service providers are required to report incidents on their networks and information systems (duty to report), and to take security measures on their networks and information systems (duty of care)[35].	
As a direct effect of the Directive, a CSIRT dedicated to DSP was created (CSIRT-DSP). In case of incident, according to the Dutch law, DSPs have to report to the CSIRT-DSP and to the Competent Authority, which, for the DSPs, is the Radio communications Agency. In order to do so, Digital Service Providers can use three different notification tools:	
Notification tools	**Description**
An online incident report form	The form is accessible online on the CSIRT-DSP website and the notification is directly sent to both the CSIRT and the competent Authority;
A telephone number	A standard number is available on the CSIRT-DSP website. However, the report over the phone will not be shared with the competent Authority;
An e-mail	An e-mail is available on the CSIRT-DSP website. However, the report by email will not be shared with the competent Authority;

However, if sectoral CSIRTs appear to use reporting and notification tools and capabilities similar to the national CSIRTs', **they also provide services more adapted to the sector's specificities and needs.**

Sectoral CSIRT specific capabilities and services

When asked about the main added value of sectoral CSIRT, respondents to the survey and sectoral experts raised the following:

- **Better knowledge of specific sectors' threat landscape;**

By working on a more focused perimeter, sectoral CSIRTs gain robust knowledge of the specific risks and threats targeting their sectors. As an illustration, the Dutch Health sector CSIRT, Z-CERT[36], offers specialized services to healthcare institutions by publishing regular white papers[37] on the specific threats targeting hospitals.

[35] https//csirtdsp.nl/en/node/1
[36] https://www.z-cert.nl/
[37] https://www.z-cert.nl/nieuws

- **Better knowledge of the entire sector value-chain and better relationship with vendors;**

Sectoral CSIRTs tend to have more direct contact with sectoral operators. Operators can often register as participants to sectoral CSIRTs to better benefit from said CSIRT services. Hospitals (ranging from academic "UMCs", top clinical "STZ" to "general" hospitals) as well as mental healthcare institutions ("GGZ") can register with Z-CERT as participants (constituency)[38].

- **More qualitative and operational information sharing, better sharing of good practices.**

Sectoral CSIRTs provide or are used as information-exchange entities either to share identified vulnerabilities, incidents or lessons learned. Z-CERT, for instance, informs its constituency of any vulnerabilities detected in medical devices, medical networks and medical applications. To those participants affected by a vulnerability, Z-CERT provides advice on how best to deal with the situation. Z-CERT also sends out alerts regarding possible threats and current attacks. Z-CERT shares its knowledge (through the release of whitepapers, for example) with its participants, facilitates meetings for its participants, and hosts networking events and theme sessions[39].

Sectoral capabilities maturity assessment

When assessing the maturity of the tools and processes used by national and sectoral CSIRT, two specific factors must be taken into consideration.

First, the maturity of the CSIRT itself: a more mature (see ENISA Maturity Evaluation Methodology for CSIRTs)[40] CSIRT will tend to have better developed tools and processes than others.

In The Netherlands, the national CSIRT appointed a liaison officer to follow the creation of the sectoral CSIRT and support their development and maturity. According to the liaison officer:

"*They [Sectoral CSIRT] are **growing in staff** but it is **challenging to find people with cyber security skills.** Besides, we have also seen **growth in services, number of staff and expertise**. Our CSIRT for Municipalities and the Health-CERT have been around a couple years now, grow in more mature CERTs every day, and **expand their services from the traditional incident response activities to activities focused on tackling more long-term cybersecurity problems** by writing advisory products and developing threat landscapes for their constituency."*

There is a shortage of skilled staff to conduct IR tasks within both national and sectoral CSIRTs

The **shortage of skilled staff for both national and sectoral CSIRT** has been identified has a recurrent issue by IR experts.

Highly regulated sectors and maturity of IRC

Secondly, reporting processes and information exchange tend to be more mature in highly regulated sectors. As stated in the NIS Directive, requirements for notification of incidents can be part of normal supervisory practice in the highly regulated sectors or sectors ruled by a supervisory mechanism.

[38] https://www.z-cert.nl/en
[39] https://www.z-cert.nl/en
[40] ENISA Maturity Evaluation Methodology for CSIRTs

For example, the financial sector has particular regulations which require the notification of incidents impacting the network and information systems and call for specific IRC and monitoring tools.

"Financial institutions are particularly exposed to cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected networks. Critical financial market infrastructures include payment and settlement systems, trading platforms, central securities depositories, and central counterparties."[41]

The Financial and banking sectors are targeted by increasingly frequent and sophisticated cyber-attacks. According to an IMF study on cyber risks (Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, WP/18/143, July 2018)[42], cyber-attacks targeting the financial sectors can have several effects:

- Business disruptions prevent firms from operating, resulting in loss revenue;
- Fraud leads to direct financial losses;
- Data breaches take more time to materialize, through reputational effects as well as litigation costs.

To tackle these risks and avoid cascading effects at European level, the European Central Bank (ECB) conducted a thematic review on cyber security risk in 2015 (prior to the NIS Directive) and targeted on-site inspection[43]. In 2016, the ECB Banking supervision has implemented a **cyber-incident reporting framework as a pilot scheme which was rolled out to the banking institutions in 2017**[44]. All significant institutions from the 19 Eurozone countries have to report significant cyber incidents as soon as they detect them. This enables supervisors to identify and monitor trends in cyber incidents affecting significant institutions and to gain a deeper knowledge of the cyber threat landscape. It also allows for a swifter reaction to a potential crisis caused by a cyberattack[45].

Table 9: Case study: TIBER-EU - threat intelligence-based ethical red-teaming framework

ECB - TIBER-EU
TIBER-EU Context and Framework
TIBER-EU is the European framework for threat intelligence-based ethical red-teaming. It is the first EU-wide guide on how authorities, entities, threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack. TIBER-EU was jointly developed by the ECB and the EU national central banks, approved by the Governing Council of the ECB and published in May 2018. It was inspired by and takes into account the lessons learned from similar initiatives in the United Kingdom (CBEST) and the Netherlands (TIBER-NL). The TIBER-EU framework is currently (being) implemented in Belgium, Denmark, Ireland and the Netherlands, as well as by the ECB in its oversight capacity. Other jurisdictions are expected to follow soon.
Functioning
TIBER-EU tests mimic the tactics, techniques and procedures of real-life attackers, based on bespoke threat intelligence. They are tailor-made to simulate an attack on the critical functions of an entity and its underlying systems, i.e. its people, processes and technologies. The outcome is not a pass or fail;

[41] Bouveret, A., Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, 2018
[42] https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx
[43] https://www.bankingsupervision.europa.eu/press/publications/newsletter/2017/html/ssm.nl170517_3.en.html
[44] Ibid.
[45] https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

instead the test is intended to reveal the strengths and weaknesses of the tested entity, enabling it to reach a higher level of cyber maturity.
Participants
The main participants in a TIBER-EU test are assigned to one of five different teams depending on their role and responsibilities: Blue team – the people in the entity that is the subject of the test and whose prevention, detection and response capabilities are being tested without their foreknowledge Threat intelligence provider – the company that looks at the range of possible threats and carries out reconnaissance on the entity Red team provider – the company that carries out the simulated attack by attempting to compromise the critical functions of the entity by mimicking a cyber attacker White team – a small team within the target entity who are the only ones there who know a test is happening and that leads and manages the test in collaboration with the TIBER cyber team TIBER cyber team – the team within the authority that is responsible for overseeing the test and making sure it meets the requirements of the TIBER-EU framework, thus enabling mutual recognition of the test by relevant authorities.
Sources
https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

3.5.2 Lessons learned and recommendations

- Sector specific regulations tend to act as a key driver to enhance IRC. ENISA and sectoral authorities should collaborate more if possible to streamline IRC-related guidelines or good practices within the future regulation.
- The mitigation of the shortage of skilled staff for IR activities at both national and sectoral level should be a priority for MS. Innovative methods to attract and retain skilled staff could be studied along with relevant incentives such as training building on existing practices within the Member States.

3.6 KEY FINDING #6

3.6.1 There is a multiplication of information-exchange tools to facilitate cooperation at sectoral, national and EU/international level, but the quality of the exchange depends on both organisational and structural criteria

The importance of sharing information is widely recognised among Member States, highlighted by a growing number of initiatives to foster cooperation through information exchange at national, European and international level.

These initiatives can take very different forms:

- Cooperation agreements;
- Cooperation and information platforms;
- Dedicated fora, communities and networks;
- ISACs and other information centres.

Sectoral initiatives at national level

There is a multiplication of initiatives such as ISACs, networks and fora at national level to foster information exchange and increase awareness among stakeholders within a sector. Certain fora and communities were created in the early 2000's but a growing number are currently being created to respond to the need of information exchange.

Table 10: Information exchange initiatives at national level within sectors

Information exchange initiatives at national level – sectoral illustrations & good practices
Luxembourg
The Luxembourg Bankers' Association (ABBL) has put in place the Trust and Cybersecurity Committee (TCS). The TCS Committee's purpose is to promote Cybersecurity and Information Risk information across the banking sector, as well as to act as a connector between the various actors on the market. The members of the TCS Committee gather for quarterly plenary sessions at the Luxembourg House of Finance in order to openly exchange on the current threat landscape, regulatory and supervisory aspects and general market practices regarding cyber risks.
Portugal
The Civil Aviation authority organise workshops to share good practices and lessons learned with its constituent. This information can also be share with the National CSIRT and at EU-level.
Spain
The Industrial Cybersecurity Centre (CCI) was created in in June 2013 to boost and improve industrial cybersecurity in Spain and Spanish-speaking Latin America, defining industrial cybersecurity as "the set of practices, processes and technologies, designed to manage cyberspace's risk associated to the management, process, storage and transmission of information used by industrial infrastructures, from the points of view of people, processes and technologies".[46] The activities of the Centre, focused on provide maximum benefits to its members and sponsors are ruled by the following strategic objectives: • Conglomerate the main experts and actors in industrial cybersecurity in order to facilitate the exchange of experience and information and be kept up to date on the last technologies and improvements on this subject.

[46] https://www.cci-es.org/en/mision

- Provide awareness on the current state of cybersecurity, paying special attention to new threats and attack techniques.
- Set communication channels with authorities and lawmakers in order to ease communication among the different actors involved in industrial cybersecurity (government, industrial associations, critical infrastructures, engineers, integrators, vendors, consulting firms, associations, standard and good practice developers and citizens).
- Improve awareness among all the actors through courses, events, seminars, publications and a presence in the media.
- Qualify professionals on industrial cybersecurity in order to facilitate hiring.
- Improve and expand the Spanish and Latin American industrial cybersecurity market.

Trans-sectoral initiatives at national level

According to the survey, 55% of respondents have a network of IR actors at a national or sectoral level to exchange good practices on cyber information exchange, capabilities, cooperation etc. to support the development of OES IRC.

National CSIRTs have developed dedicated platforms for information exchange and cooperation which are open to OES from all NISD sectors.

Table 11: Information exchange initiatives at national level cross-sectors

Information exchange initiatives at national level – trans-sectoral examples & good practices
Belgium – TIP & MiSP
The Belgian Threat Intel Platform (TIP)[47] is a transversal information-exchange platform initially created for Law enforcement and Intelligence stakeholders to share threat intelligence and was later partially opened to OES. Within the TIP, OES from all sectors will have access (Belgium is still in the process of designating OES) to the TIP to receive threat intelligence about their sector. The Belgian Malware Formation Sharing Platform (MISP) is publicly accessible, but users can set up private dedicated sectoral communities to exchange information on sectoral incidents.
Poland – N6 Project
The n6 project[48] was designed and developed entirely at CERT Polska as a platform for acquisition, processing and exchange of information regarding Internet threats. It is operational since February 2012. Within the n6 project, millions of security events are processed daily in an automated manner. The goal is efficient, reliable and fast delivery of large volumes of network incident data to interested parties: network owners, administrators and Internet Service Providers. The project disseminates information gathered from various security systems operated by security organizations, software vendors, independent researchers, etc. The core element of n6 is its engine responsible for sorting and managing flow of data. Sorting and delivering data to appropriate parties is made possible by a flexible tagging system, which defines categories of incoming data and addresses specific interest.
The Netherlands - NDN
The National Detection Network (NDN)[49] is a partnership for better and faster detection of digital dangers and risks. By sharing information about threats, parties can take appropriate measures in a timely manner under their own responsibility, to limit or to prevent possible damage.

[47] Interview with CERT-BE
[48] https://www.cert.pl/en/projekty/n6-network-secident-exchange/
[49] Interview with NCSC-NL

United Kingdom – CiSP
The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.[50]

Initiatives at European / regional level

Several initiatives were identified at both European and regional level to support the creation and/or the uptake of tools facilitating the exchange of technical information about incidents.

Table 12: Information exchange initiatives at European level

Information exchange initiatives at European level (examples)	
Initiatives	**Description**
Trans-sectoral	
CSIRT Network[51]	The CSIRT Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs Network members"). The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs' cooperation, provide the secretariat and active support for incident coordination upon request. The CSIRT Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.
European Government CERTs (EGC) group[52]	The EGC group forms an informal association of governmental CERTs in Europe. Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets. To achieve this goal, the EGC members: ▪ Jointly develop measures to deal with large-scale or regional network security incidents ▪ Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities ▪ Identify areas of specialist knowledge and expertise that could be shared within the group ▪ Identify areas of collaborative research and development on subjects of mutual interest ▪ Communicate common views with other initiatives and organizations
Transport	
EU Aviation ISAC	An EU Aviation ISAC is being created which will exist alongside two existing entities: ECCSA and the US Aviation ISAC. The need for a European-based Aviation ISAC was expressed by European industry members, OEMs and Airlines who saw a need to organise and collaborate in the realm of cyber security and in the field of intelligence and analysis sharing for the aviation sector.

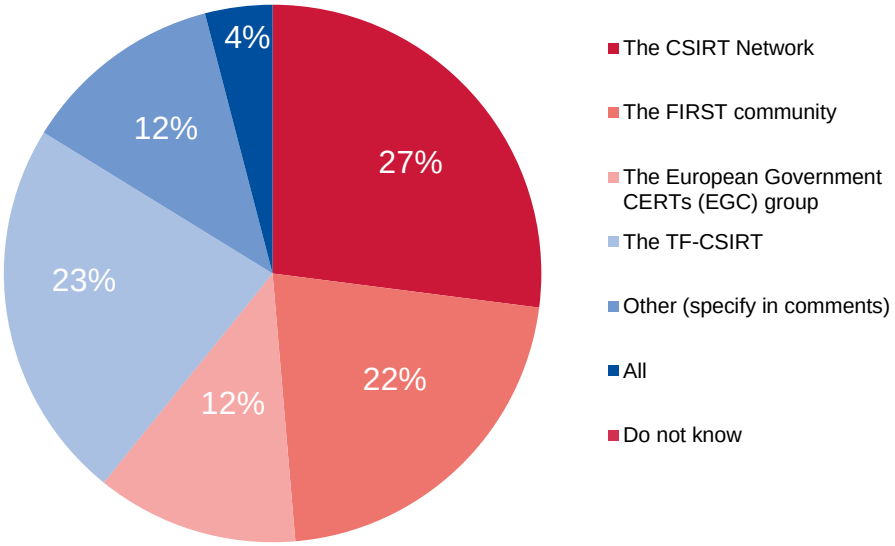
[50] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
[51] https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network
[52] http://www.egc-group.org/

Finance	
FI-ISAC[53]	The FI-ISAC exists since 2008 as an independent organisation and is well integrated with European and MS banking institutions and EU organisations such as ENISA, Europol, the European Central Bank, European Payment Council and the European Commission. ENISA provides also a secretariat support. The mission of the European FI-ISAC is information exchange on e- and m-channel, cards, central systems and all ICT related topics including: ▪ Cyber-criminal activity affecting the financial community ▪ Vulnerabilities, technology trends and threats ▪ Incidents and case-studies This information exchange helps each member and the banks in its member state, to raise awareness on potentials risks, and provides an early warning on new threats and Modus Operandi's.
Energy	
EE-ISAC[54]	The European Energy - Information Sharing & Analysis Centre (EE-ISAC) 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 to: • Set up long lasting relationships of trust with partners across the entire value chain • Share both real-time data & analysis within small scale trust-circles • Learn from their peer's experiences with grid security incidents and cyber breaches • Compare & evaluate security solutions, both from a technical and operational viewpoint • Benefit from an open dialogue with industry partners and suppliers

According to the respondents of the survey, the three most used groups to exchange with peers at European and international level are the CSIRT Network[55] (27%), the TF CSIRT[56] (23%) and the FIRST Community[57] (22%).

[53] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership
[54] https://www.ee-isac.eu
[55] https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network
[56] https://tf-csirt.org/
[57] https://www.first.org/

Figure 8: Main groups use to exchange with peers



A discrepancy was identified between the quantitative data collected through the survey and complementary interviews on the use of the European Government CERTs (EGC)[58] group. Only 12% of survey respondents (8 out the 17 National CSIRTs) use the EGC group to exchange IR good practices and experience, but the interviews with IR experts indicate that there are more frequent and qualitative exchange within this community which could be explained by the fact that not all EGC members have participated to the survey.

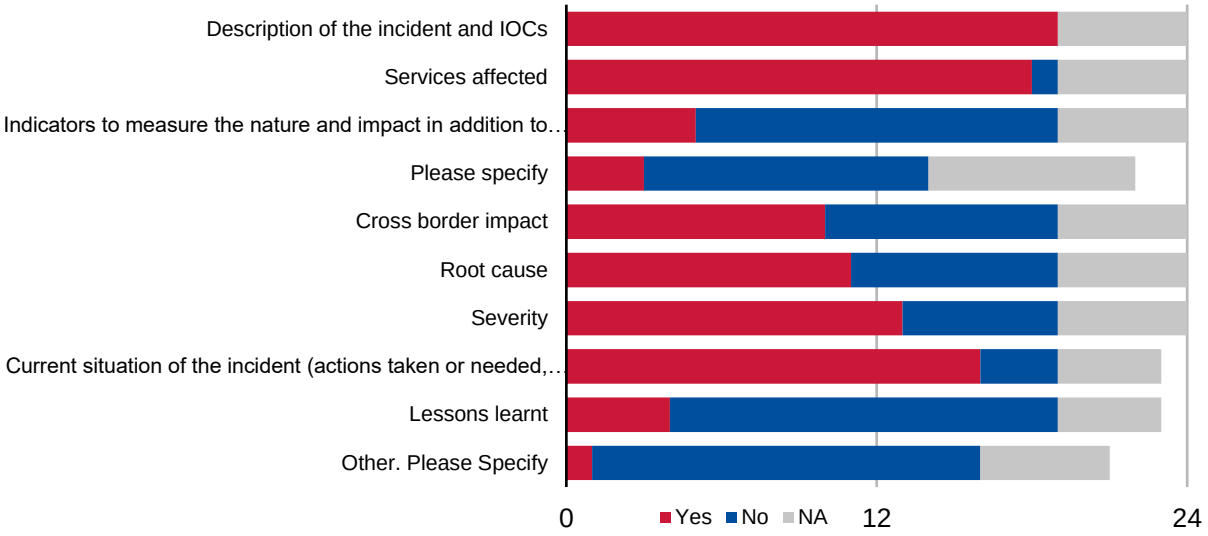
Cross-border initiatives

Cross-border cooperation relies mostly on information-sharing between MS (peer to peer exchange in regional communities) and cooperation agreements with other national CSIRTs.

- 78% of respondents to the survey have specific measures in place to inform the relevant actors (national authorities and OES) in neighbouring countries about an incident that may impact them.

[58] http://www.egc-group.org/

Figure 9: Assessment of the nature of specific measures to inform relevant actors in neighbouring countries about a cross-border incident



Quality and efficiency of information sharing in sustainable communities

The multiplication of networks and initiatives, however encouraging and a sign of rising awareness on the need to facilitate information exchange, must also be evaluated in terms of quality of the exchange within these fora.

Information-sharing communities and fora need resources to sustain the efficiency

Certain fora were created in response to legitimate sectoral needs. Yet **these fora can lack the organisational and structural means to sustain the efficiency of information-sharing**, thus undermining their *raison d'être*.

As an illustration, the European Cyber Security Organisation (ECSO) published a position paper on the creation of a European Energy ISAC[59] which the paper claims lacks visibility among most European energy operators. In ECSO's opinion, "*EE-ISAC carries out many activities but the main outcomes and benefits of the organisation are not clear. In addition, EE-ISAC involves only a few energy operators whereas they should be strongly represented to drive the ISAC activities according to the energy sector's needs.*"

Several factors are currently or could in the future jeopardise the quality and efficiency of the information-sharing initiatives such as:

- **A lack of representativity and visibility** within the sector: if there are multiple communities or platforms aiming the same objective within a given sector and if the communication and dissemination resources are not sufficient to raise awareness on the existence of the initiatives;
- **A lack of financial resources**: If there is not enough budget to sustain the initiative on a long term;
- **A lack of trust between participants**: within over-sized fora with too many stakeholders, it can be challenging to build trust to allow fruitful exchanges among participants;

[59] https://ecs-org.eu/documents/publications/5c0a6a3aac673.pdf

- A **fear of penalty for the voluntary reporting of incident caused by human error:** when reporting human errors, stakeholders should be ensured not to be blamed or penalised to encourage sharing of lessons learned.

Finally, information sharing at sectoral level can also raise operational challenges:

According to one of the interviewees, *"one of the difficulties is how **to make sure the right knowledge and information will reach all relevant organisations.** On top of that, you want to have a feedback loop where information flows from the national CSIRT to the sectoral CSIRT to the individual organisations**, it should not be a one-way-street**.*

*Other challenges involve the fact that OES have a notification requirement to their Single Point of Contact and sectoral regulator, but not always to their sectoral CSIRT, which can sometimes make the information sharing and notification duties **a complex set of responsibilities**. In addition, **there is a risk of inefficiency."***

Finally, it can sometimes be challenging for Sectoral CSIRT and OES to assess when a threat or an incident can also have impact for other sectors and should be shared. In case a major incident which could have impacts in national security the National CSIRT would be in direct contact with the OES, and the Sectoral CSIRT in hybrid or distributed IR models. This situation could raise the question to delegate national security tasks to private sectoral CSIRTs.

This is why it seems like both a continuous exchange with national CSIRT and cross-sectors communication channel could be important to set-up or maintain at national level. This would **allow to share the work and avoid that several CSIRTs (national and sectoral) analyse the same threat or event and does not share the analysis.** Therefore, there it would mitigate the risk of doing double work with the already limited cyber security resources.

3.6.2 Lessons learned and recommendations

- ENISA could further study the drivers to sustain information-sharing initiatives, develop a set of guidelines, user-friendly tools and enablers (such as "Secure Group Communications for incident response and operational communities"[60] and "Proactive detection of network security incidents - incident response tools mapping") .
- Dedicated collaboration schemes at MS level could avoid duplication of efforts and ensure that all relevant stakeholders are informed such as user-friendly cross-sectoral communication tools or channels between several authorities (NISD and GDPR authorities).
- The anonymised voluntary reporting of human errors should be encouraged and supported to ensure that lessons learned are widely disseminated.
- The promotion of responsible disclosure programs of vulnerabilities at sectoral level should be foster.

[60] https://www.enisa.europa.eu/publications/secure-group-communications

3.7 KEY FINDING #7

3.7.1 There is a growing interest in training to enhance and foster preparedness in NISD sectors at European level

The NISD encourages MS to foster their preparedness by requiring the establishment of appropriate measures such as the creation of CSIRTs. Many MS have placed increasing cyber preparedness, in particular that of NISD sectors, as a priority in their national cyber security strategy.

Although, it was difficult to measure how this priority is concretely implemented at operational level, one of the key areas identified to increase preparedness is the set-up of training.

There is a need for sector-specific training to mitigate shortage of skilled-staff

According to the FIRST CSIRTs services framework:

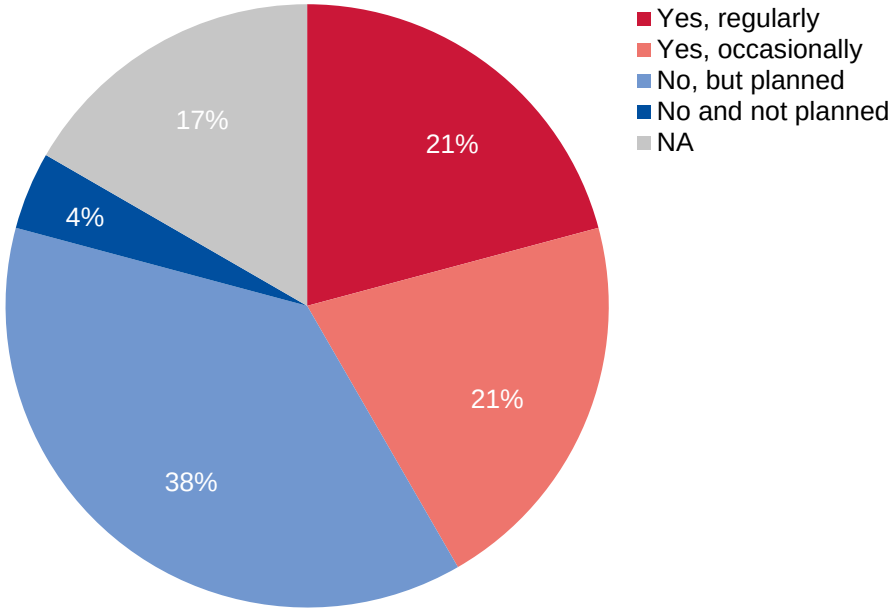
"A training and education programme can help the CSIRT to establish relationships, ***and to improve the overall cybersecurity posture of its constituency****, including the ability to prevent future incidents from happening. Such a programme can help maintain user awareness, help the constituency* ***understand the changing landscape and threats****,* ***train the constituency on tools, processes and procedures related to security and incident management.***

This can be done through various types of activities including documenting the knowledge, skills and abilities (KSAs) required, developing educational and training materials, delivering content, mentoring, and professional and skill development. Each of these activities will collectively contribute to the constituency's and the team's capabilities."

According to the survey, out of 24 respondents, sector-specific cybersecurity training activities are conducted:

- Regularly: 5 National CSIRT
- Occasionally: 2 National CSIRT and 3 Sectoral CSIRT
- No but planned in the future: 8 National CSIRT and 1 Sectoral CSIRT
- No and not planned: 1 National CSIRT
- Did not provide answer: 3 National CSIRT and 1 Sectoral CSIRT

Figure 10: Sector-specific training evaluation



These answers indicate a significant interest from the sectoral CSIRT in training. It could be a concrete way to mitigate the shortage of skills highlighted in the previous findings.

Several initiatives already exist at both national and EU level to conduct trainings on Incident response procedures and tools.

Table 13: Case study: Good practices for training

Good practices for Training at national level – Illustrations	
Initiatives	**Description**
Belgium	
CERT-BE annual training program	Every year CERT-BE organises a training programme for federal officials. They launched a call for tenders for private companies that provides cybersecurity trainings. These trainings can cover a wide range of skills. CERT-BE organises the training programme and private companies send their trainers.
Luxembourg	
CIRCL.LU trainings[61].	CIRCL.LU offers courses to its members and organisations based in Luxembourg. In their mission to improve information security, CIRCL shares its field experience through a set of training or technical courses. Due to diversity of competences within the team, CIRCL is able to provide a large diversity of information security trainings. Courses target technical experts but also non-technical staff in the topics of incident handling, malware analysis, operational security and system forensics.

[61] https://www.circl.lu/services/training/

3.7.2 Lessons learned and recommendations

- ENISA should continue its efforts in the area of trainings and promote the training programmes also within sectoral CSIRTs[62].
- To mitigate the shortage of skilled staff and enhance IRC capabilities within sectors, raising awareness in sectors about the added value of sector-specific training could be initiated.
- Dedicated training could be created for sectoral actors. This could be done by first assessing the sector-specific training needs with relevant stakeholders and identifying existing trainings (such as TRANSITS-I, TRANSITS-II, and the ones conducted by ENISA, FIRST, etc.) to build on their experience.
- Sectoral CSIRTs might want to prioritize practical areas of IR:
  - Tools;
  - Taxonomy;
  - Responsible vulnerability disclosure;
  - Trust building;
  - Information sharing and developing skills and experience.

3.8 FINAL RECOMMENDATIONS

Recommendations	
Actors	**Description**
Recommendations to ENISA	
Knowledge	Collect deeper insights on both national and sectoral CSIRT maturity when the NISD will have been fully implemented;
Cooperation	Favour cross sectoral knowledge between the stakeholders;
Information sharing	Continue to collect available resources to enhance IRC & enhance information-sharing and build a repository;
Training	Develop a continuum for training activities which range from assessing sectors trainings needs, to promote the “train-the-trainers» approach, to continue developing sectoral trainings.
Recommendations to the IR Community	
Transparency	Publish a clear list of the sectors covered within NISD at national level (same as the NISD or extended);
Information sharing	Encourage the use of secure communication tools, common taxonomy[63] and sharing of lessons learned after incident with peers and everywhere; The responsible disclosure of vulnerabilities should be fostered by setting incentives;
Cooperation	Build trust within communities and engage with OES and DSP;
Resources	The IR community should have adequate resources to conduct their missions.

[62] https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors
[63] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

4. PRESENTATION OF THE RAW DATA

4.1 DESKTOP RESEARCH – SECTORAL IR SET-UP

The objective of the desktop research was to identify Incident Response (IR) actors and bodies playing a role in NISD sectors across EU Member States.

This comprehensive analysis also focused on the distribution of responsibilities to present draft hypotheses on the emergence of new actors following the publication of the NIS Directive.

4.1.1 Data structuring and classification criteria

The raw data gathered during the study was consolidated in an Excel table. It was first classified based on the 28 Member States.

Then, for each Member State, the following information was provided, when available:

- **Summary of national approach towards IR in the NISD sectors**
- **Incident Response general Set-up**
  - NISD Sectors
    - Competent authorities;
    - Existing/newly created CSIRT or IR entities;
    - Role of OES;
    - Role of DSP.
- **Cooperation set-up & processes**
  - IR processes and procedures (IR and reporting);
  - Collaboration procedures with NISD sectors;
  - Cross-border IR aspects.
- **Development of capabilities and other initiatives**
  - Operational Preparedness and capacities;
  - Tools;
  - Initiatives, communities, etc.

4.1.2 Overview of the Sectoral IR Set-up within the 28 Member States

4.1.2.1 Desktop research – Key Figures

Table 14: Desktop research – Data Collection overview

Nature of information collected	Data Collection
Summary of national approach towards IR in the NISD sectors	Identified in 14 MS
Competent authorities for NISD sectors	All NISD Sectors competent authority/ies for 13 MS, partial data for 3 MS
Existing/newly created or planned CSIRT or IR entities	31 Existing/newly created identified 2 planned identified

Role of OES	Identified for 23 MS
Role of DSP	Identified for 19 MS
IR processes and procedures (IR and reporting)	Minimal data in 10 MS
Collaboration procedures with NISD sectors	Minimal data in 8 MS
Cross-border IR aspects	Minimal data in 9 MS
Operational Preparedness and capacities	5 identified
Tools	4 identified
Initiatives, communities, etc.	9 identified

24 respondents from 17 EU MS and Norway.

4.2 SURVEY AND INTERVIEWS – IR APPROACH AND SECTORAL CAPABILITIES

The objective of the survey and complementary interviews were to fill in the information gaps in the desktop research and gain deeper insight on IR set-up within the 28 Member States.

These activities also focused on the recent changes and evolution of Sectoral IRC and improve the knowledge on Sectoral CSIRTs processes, procedures and tools following the publication of the NIS Directive.

4.2.1 Survey - Data structuring and classification criteria

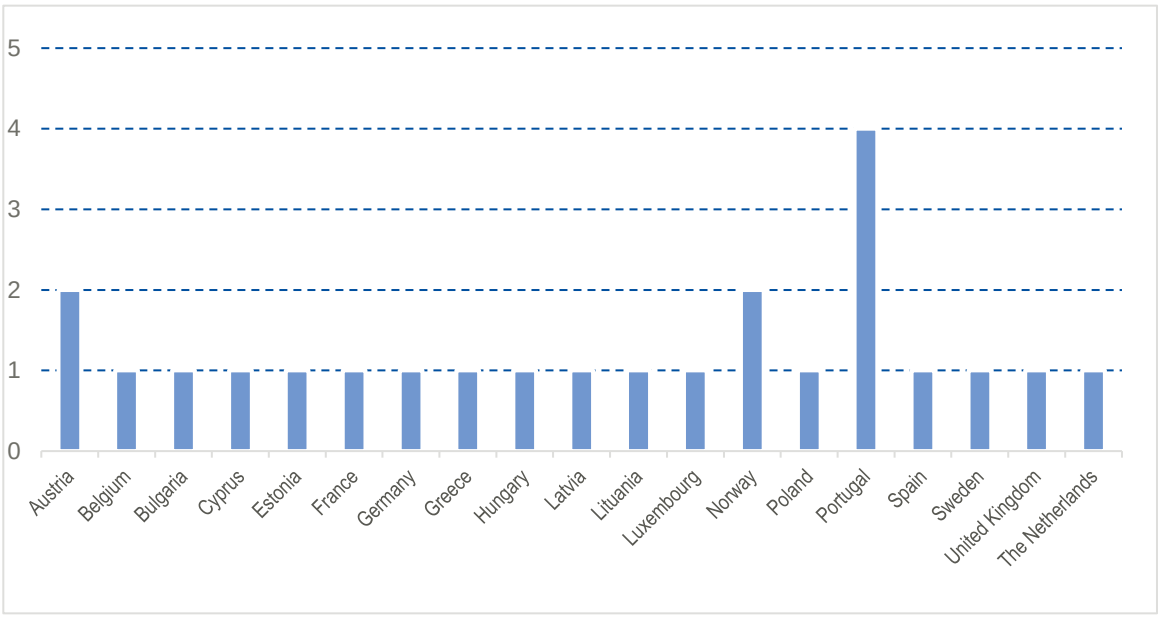
The raw data gathered from the survey was consolidated in an Excel table. It was first classified based on the 28 Member States.

Then, for each Member State, the table was structured around the answers of each respondent according to the questions of the survey. Overview of the Sectoral IR Set-up within the 28 EU Member States

4.2.1.1 Survey - Key Figures

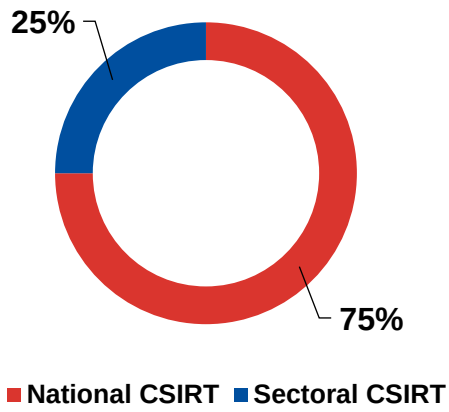
The data collection relies on **24 responses from 17 EU Member States, and Norway**. It also includes insights from another Member States who did not reply to the survey.

Figure 11: Respondents by countries



Two-thirds of respondents were **national CSIRTs** with IR teams of full-time equivalents ranging **from 4 to 90 people.**

Figure 12: Respondents by entity

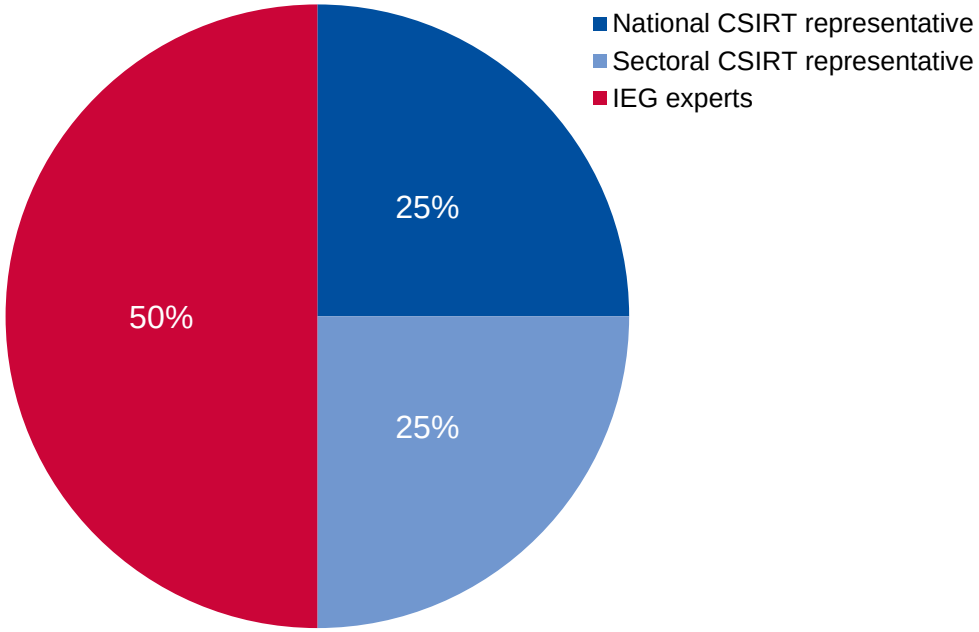


4.2.2 Complementary Interviews – Rationale and key figures

The main objective of the survey was to collect main information of the IR set-up, along with quantitative assessment of recent changes and impact of the NISD. After reviewing the first results collected, complementary interviews were schedules with two different rationales:

- Interviews with 2 national CSIRT and 1 sectoral CSIRTs who had already answered the survey to clarify some answers or collect additional and more qualitative inputs;
- Interviews with other 1 sectoral CSIRTs to obtain deeper insight from the NISD sectors;
- Interviews with 4 ENISA NIS Informal Experts Group to obtain deeper insight from their sectors.

Figure 13: Interviewees by organisation



5. BIBLIOGRAPHY

Bouveret, A., *Cyber Risk for the Financial Sector*, International Monetary Fund, 2018

ECSO, Position paper European Sector-Specific ISACs, European Cyber Security Organisation, December 2018

ENISA, *Maturity Evaluation Methodology for CSIRTs*, European Union Agency for Network and Information Security, 2019

ENISA, *Strategies for Incident Response and Cyber Crisis Cooperation*, European Union Agency for Network and Information Security, 2016

Loughlin, J., *Centralization and Decentralization in French History*, Subnational Government, 2007, pp. 25-44

NCSC, *Guide to Starting a Collective CSIRT*, National Cyber Security Centre, 2018

WEBSITES AND ONLINE PUBLICATIONS:

ANSSI, “The French CIIP Framework”, 2019. [Online].
Available: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

Bank of Finland, Bulletin “Nordic banks go digital”, 2018. [Online].
Available: https://www.bofbulletin.fi/en/2018/2/nordic-banks-go-digital/

CERT-BE, “Report an incident”, 2019. [Online].
Available: https://www.cert.be/en/report-incident

CERT-BE, “Traffic Light Protocol (TLP)”, 2019. [Online].
Available: https://www.cert.be/en/traffic-light-protocol-tlp

CIRCL, “Training and Technical Courses”, 2018. [Online].
Available: https://www.circl.lu/services/training/

CNCS, “CERT.PT”, 2019. [Online].
Available: https://www.cncs.gov.pt/en/certpt_en/

CSIRT-DSP, “Duty to report incidents for digital service providers”, 2019. [Online].
Available: https://csirtdsp.nl/en/node/1

ECS, Position Paper “European Sector-Specific ISACs”, 2018. [Online].
Available: https://ecs-org.eu/documents/publications/5c0a6a3aac673.pdf

European Central Bank, “What is TIBER-EU?”, 2019. [Online].
Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Central Bank, “What is cyber resilience?”, 2019. [Online].
Available: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

ENISA, “History”, 2019. [Online].
Available: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities

EUR-Lex, “The Directive on security of network and information systems (NIS Directive)”, 2016. [Online].
Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

FIRST, “FIRST CSIRT Framework V0.2”, 2019. [Online].
Available: https://www.first.org/education/csirt_services_framework_v2.0

GitHub, “CERT Tools”, 2019. [Online].
Available: https://github.com/certtools/

GitHub, “Digital Forensics and Incident Response (DFIR) Resources”, 2019. [Online].
Available: https://github.com/The-Art-of-Hacking/h4cker/tree/master/dfir

GPPi, New America, “National CSIRTs and Their Role in Computer Security Incident Response”, 2015. [Online].
Available:
http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf

Industrial Cybersecurity Center, “The center”, 2019. [Online].
Available: https://www.cci-es.org/en/mision

ITU/BDT, “Cyber Security Programme: Global Cybersecurity Index (GCI)”, 2018. [Online].
Available:
https://www.itu.int/en/ITUD/Cybersecurity/Documents/GCIv3_documents/GCI%20V3%20Reference%20model.pdf

JDSUPRA, “Germany’s Draft Bill on IT Security 2.0 – Extended BSI Authorities, Stricter Penalties and New Obligations on Providers”, 2019. [Online].
Available: https://www.jdsupra.com/legalnews/germany-s-draft-bill-on-it-security-2-0-55094/

MISP Threat Sharing, “Features of MISP, the open source threat sharing platform”, Date? [Online].
Available: https://www.misp-project.org/features.html

NCSC, “CiSP”. [Online].
Available: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

NCSC, “CSIRT Maturity Toolkit”, 2018. [Online].
Available:
https://english.ncsc.nl/get-to-work/cooperation/i-would-like-to-strengthen-my-collaboration/csirt-maturity-toolkit

Nordea, “Nordic banks collaborate on fighting cybercrime”, 2017. [Online].
Available:
https://www.nordea.com/en/press-and-news/news-and-press-releases/press-releases/2017/04-10-08h00-nordic-banks-collaborate-on-fighting-cybercrime.html

OECD, “The Netherland’s experience with decentralisation”. [Online].
Available: https://www.oecd.org/regional/regional-policy/Netherlands-experience.pdf

Open CSIRT Foundation, “SIM3 and references “. [Online].
Available: https://opencsirt.org

SGDSN, “La sécurité des activités d’importance vitale”, 2016. [Online].
Available: http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

Z-CERT, Expertise center for Cybersecurity in Healthcare “Home”, 2019. [Online].
Available: https://www.z-cert.nl/en

Z-CERT, Expertise center for Cybersecurity in Healthcare “News”, 2019. [Online].
Available: https://www.z-cert.nl/nieuws

A ANNEXES:

A.1 ANNEX 1 – LIST OF CRITERIA

- **Summary of national approaches towards IR in the NISD sectors**
- **Incident Response general set-up**
  - NISD sectors:
  - Competent authorities;
  - Existing/newly created CSIRT or IR entities;
  - Role of OES;
  - Role of DSP.
- **Cooperation set-up & processes**
  - IR processes and procedures (IR and reporting);
  - Collaboration procedures within NISD sectors;
  - Cross-border IR aspects.
- **Development of capabilities and other initiatives**
- **Operational preparedness and capacities;**
- **Tools;**
- **Initiatives, communities, etc.**

A.2 ANNEX 2 – LIST OF FIGURES

A.3 ANNEX 3 – LIST OF TABLES

978-92-9204-310-0

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-310-0
DOI: 10.2824/74233