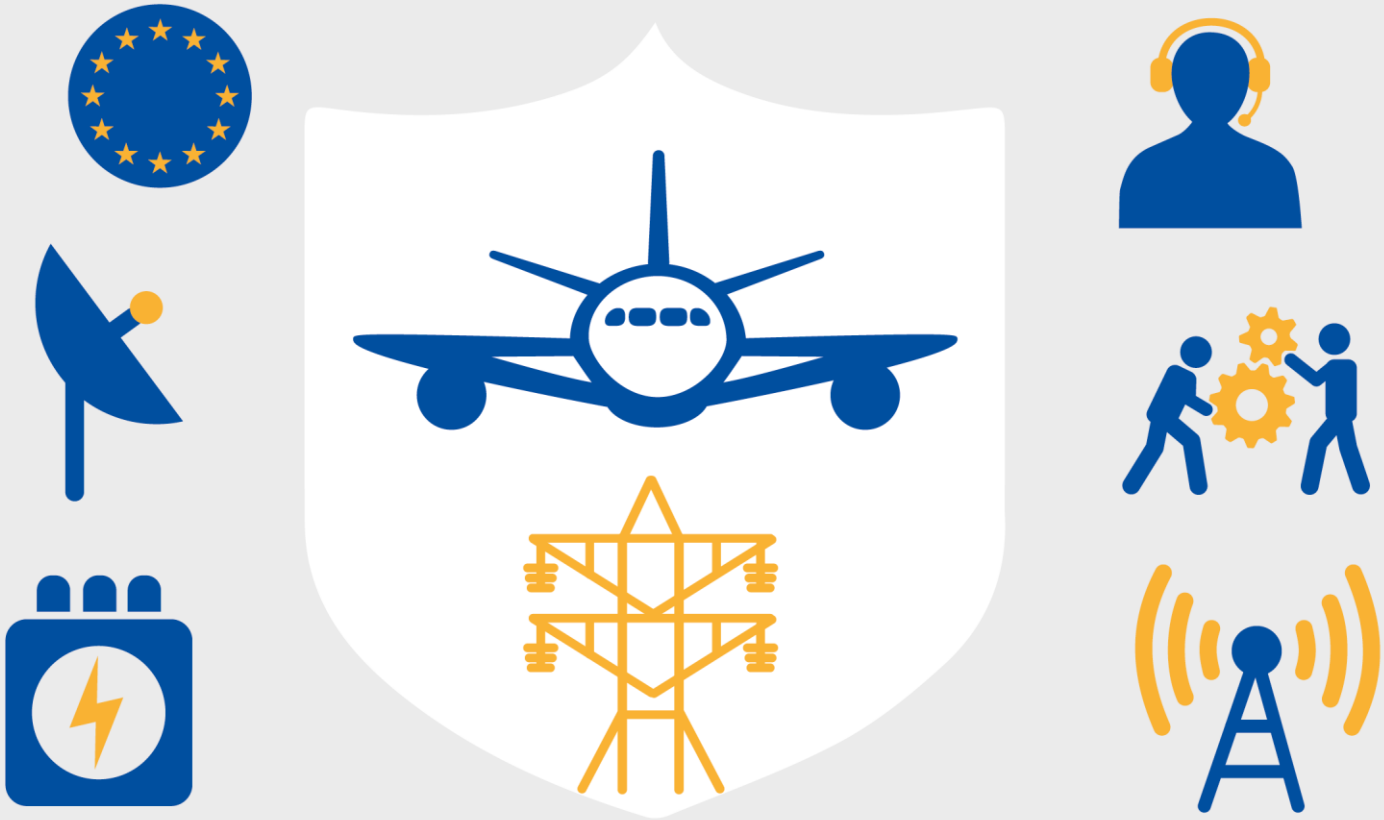
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



SECTORAL CSIRT CAPABILITIES

Status and Development in the Energy and the Air Transport sector

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use: csirt-relations@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Edgars Taurins, ENISA.
Activities supporting this study were conducted under contract with CEIS-Avisa Partners.

ACKNOWLEDGEMENTS

Study was performed with the input from Informal Expert Group on EU Member States Incident Response Development.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-444-2 - DOI 10.2824/123795

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital infrastructure, Information and Communication Technologies are critical to our societies and economies. The global Covid-19 pandemic witnessed in 2020 sent all these technologies into the limelight like never before and forced millions around the world to work from home and rely on remote connections to professional networks during the lockdown.

Cyberattacks have risen sharply since the beginning of the COVID-19 pandemic, in particular in critical sectors such as transport, health or finance.

Vital sectors had to ensure continuity of service during this lasting global crisis despite increased exposure to cyber threats over this long-lasting global crisis. The growing use of remote IT networks by a large part of the population working remotely opened new digital attack surfaces to criminals who were quick to exploit such vulnerabilities. Cyberattacks rose sharply since March 2020, as confirmed by a number of cybersecurity experts and law enforcement agencies such as Interpol. They specifically noted a rise in malware, phishing and Trojan horse attacks worldwide[1].

Both the Energy and the Air Transport sectors face considerable threats with potentially disastrous financial and societal consequences, requiring solid Incident Response Capabilities (IRC).

Both sectors come with large supply chains and a multiplicity of stakeholders (Public authorities, Regulators, Professional associations, large industries, SMEs, etc.). They have, in recent years, taken steps to structure and strengthen their ability to face cyber threats and to respond to cyber incidents. The creation of ISACs[2] to foster information-sharing at sectoral level is an excellent illustration of this evolution.

This study provides a continuation of work on Sectoral IRC at European level following the publication of the 2019 "EU Member States incident response development status report"[3]. The report focuses on trends in Energy and Air Transport Incident Response (IR) Capabilities, procedures, processes and tools. It also offers insights on current challenges and gaps facing IR communities.

The analysis aimed to focus on:

- Current IRC of Air Transport and Energy sectors,
- The recent changes in the context of the Covid-19 pandemic,
- The upcoming revision of the NIS Directive,
- To draw practical recommendations for the IR community.

[1] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[2] For example Energy ISAC https://www.ee-isac.eu/ and Aviation ISAC https://www.a-isac.com/
[3] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

KEY FINDINGS

The research highlighted the following eight key findings:

Key Finding #1 A large majority of EU countries tend to have dedicated sectoral specialists and experts within their National/governmental CSIRTs rather than one dedicated sectoral entity at national level. Sectoral CSIRTs are not yet the norm in the EU.

Key Finding #2 The EU countries which decided to create a dedicated sectoral CSIRT for the Energy or Air Transport sector were driven by organisational and functional needs rather than technical ones.

Key Finding #3 Energy and air transport sectoral CSIRTs tend to provide their constituency with sector-specific expertise in addition to the generic services provided by national CSIRTs.

Key Finding #4 The tools and processes used by sectoral CSIRTs to deliver their services are similar to those used by national CSIRTs.

Key Finding #5 Although IR stakeholders did not request specific guidance when developing their capabilities, they tended to use dedicated tools made available by EU authorities, regulators and national CSIRTs.

Key Finding #6 Sectoral CSIRTs in both air transport and energy sectors are facing similar challenges, such as legislations overlapping, or the growing time spent on compliance issues.

Key Finding #7 Sectoral CSIRTs in both the air transport and energy sectors face the common challenge of formally and rapidly sharing ex-ante information in a particularly tense context.

Key Finding #8 On-going programmes and information sharing initiatives successfully supported IRC developments in both sectors. However, a strong demand remains for more framework, guidance and know-how in relation to the impact of the Covid-19 pandemic.

1. OVERVIEW AND SCOPE OF THE STUDY

1.1 CONTEXT

Since its creation, ENISA has been actively working to assist the European Commission, European Union Member States (EU MS) and the overall cybersecurity community to enhance their capabilities and expertise. The Agency engaged in an in-depth research on Incident Response Capabilities (IRC) to that end. As a result ENISA was able to produce a state-of-the-art overview of the CSIRT landscape and of its development in Europe. This study aims to complement this work by continuing to update ENISA's recommendations for the CSIRT capability development and to disseminate the latest trends and evolutions in this domain.

Incident Response Capabilities have never been so crucial for sectoral stakeholders who rely heavily on digital tools.

ENISA's public website features a European CSIRT inventory. The interactive map it includes gives an overview of the current CSIRT teams active in Europe. A study on the CSIRT landscape and an overview of the IR capabilities in 2025 Europe are also available. These features serve the purpose to present a comprehensive picture of existing CSIRTs' incident handling and response capabilities (IRC), with initial facts and figures about sectoral CSIRTs.

2020 has been impacted by the global COVID-19 pandemic in many ways but in addition to an unprecedented financial impact, it has resulted in a massive increase in the use of digital tools and services. As a result, cybersecurity and Incident Response Capabilities in particular have become more crucial than ever. It is therefore fundamental that ENISA continues to closely monitor capability development, particularly in light of the upcoming revision of the NIS Directive.

This revision is a great opportunity to take stock of the recent evolutions of the Incident Response Landscape across the EU. The revision will be an occasion to build on the lessons learnt by the IR community across the EU Member States (MS) in addressing the challenges the implementation of the NISD has given rise to.

Following the publication of the 2019 "EU Member States incident response development status report"[4], ENISA is eager to take a closer look at the IRC development of sectoral CSIRTs, more specifically in the energy and air transport sectors.

1.2 OBJECTIVE OF THE STUDY

This study aims to further ENISA's understanding and knowledge of IRC development and draw conclusions about the development of IR capabilities particularly in the energy and air transport sectors.

It constitutes an extensive analysis of IRC in the energy and air transport sectors and presents potential gaps, overlaps and challenges in the services offered as well as in the procedures, processes and tools used by sectoral IRCs.

[4] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

The specific objectives of this study are:

- To collect and aggregate comprehensive data on the current IRC in the air transport and energy sectors;
- To analyse and measure the evolution and development in sectoral CSIRTs services, capabilities, processes, tools and cooperation mechanisms;
- To identify potential gaps, overlaps and challenges in national IR procedures, processes and tools.

To this end, research was divided into three parallel activities, namely:

- A desktop research of open sources,
- A survey of EU national and sectoral CSIRTs (responses received from 13 Member States and a European sectoral CSIRTs),
- Complementary interviews with sectoral IRC experts and national CSIRTs.

An overview of the methodology and an assessment and presentation of the data collected can be found in chapters 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 Air Transport and Energy sectors in Member States.

The study focuses on:

- Capabilities of sectoral CSIRTs;
- Operational preparedness of sectoral CSIRTs or other IR entities;
- IR services actually provided to constituency;
- IR processes and procedures;
- IR tools (used by sectoral CSIRTs or other IR entities) standalone and/or in contrast with national CSIRT(s);
- Awareness of ENISA maturity assessment and/or (Self) assessment framework for CSIRTs;
- Examples and/or lessons learnt of sectoral incidents;
- Cooperation mechanisms used nationally and internationally;
- Current levels of maturity and requirements for development.

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

The scope and key concepts of the research were defined as follows:

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.[5]

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

Incident response capabilities (IRC): 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 identify, respond to and mitigate the impact of an attack, and to restore continuity of service.[6]

Incident response models: the survey used a typology of four Incident Response models:

- **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 dissemination of information.
- **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 dissemination of information.
- **Hybrid:** a national CSIRT and the sectoral CSIRTs share the IR responsibilities and operations, which may depend on the sector(s) impacted or the scale of the incident for instance.
- **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.[7]

National Sectoral CSIRTs: Entities responding to computer security or cybersecurity incidents affecting a specific sector at national level. N/ Sectoral CSIRTs are usually established in NISD sectors such as Healthcare, Energy, and the Transport Sector. Unlike the N/G CSIRT who serves the public sector, the national Sectoral CSIRTs provides services to constituents from a single sector in one country (in the context of this study, the national Sectoral CSIRTs and sectors mentioned are mainly Air Transport and Energy sectors).

Sectoral CSIRT of international organisation: Entities or teams within an international organisation or company responding to computer security or cybersecurity incidents affecting the organisation and providing services to constituents from a single sector at regional (EU) or international level.

OES CSIRT/IRTs: Entities or teams responding to computer security or cybersecurity incidents affecting an Operator of Essential Services within a sector.

Operators of Essential Services (OES): Operators of essential services are private or public sector entities who play an important role in providing healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply. According to the NIS Directive, Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services[8].

[6] Ibid.
[7] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities
[8] 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

Digital Service Provider (DSP): A digital service provider is an entity providing one or more of the three types of digital service, such as:

- **Cloud computing services**: digital services enabling access to a scalable and elastic pool of shareable computing resources.
- **Online marketplaces**: digital services allowing consumers to conclude online sales or service contracts with traders online using computing services provided by the online marketplace.
- **Online search engines**: means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

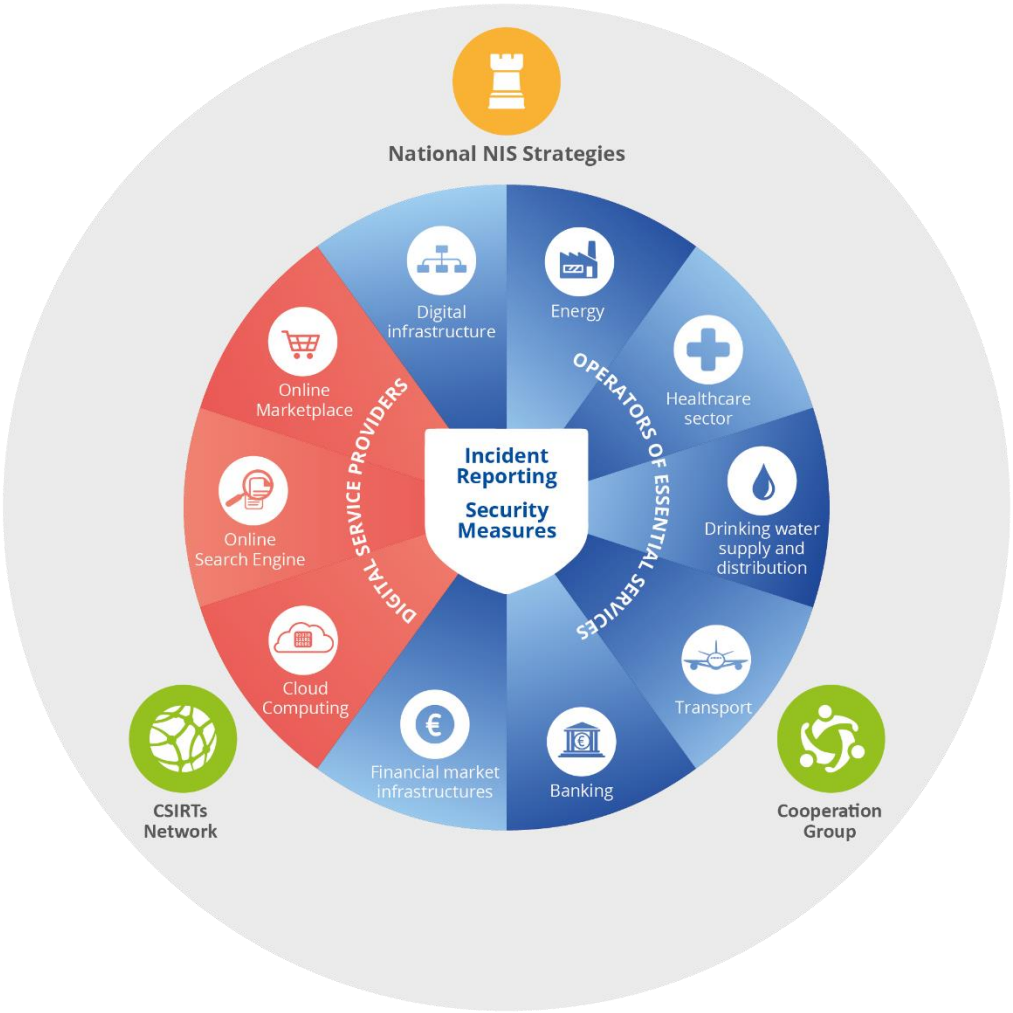
NIS Directive: The Directive on Security of Network and Information Systems (NISD) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The NISD provides legal measures to boost the overall level of cybersecurity in the EU.[9]

NISD sectors: Critical sectors for the European Union's society and economy are heavily dependent on ICT. Member States have been requested to identify operators of essential services (OES) for the seven sectors listed in the NIS Directive (NISD sectors). These seven sectors – and related subsectors – listed in the Directive[10] are:

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

[9] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[10] 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

Figure 1: NISD sectors



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 air transport and energy sector is illustrated below. The series of steps the methodology consists of is 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 in close cooperation with the ENISA team. To that purpose an analysis grid setting criteria and theme was created to classify the information collected on energy and air transport Sectoral IRC

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

2.2.2 Step 2 – Desktop research in open source on air transport and energy Sectors IRC

This step consisted in conducting a literature review and open source research in order to collect data on sectoral IRC and recent trends in the field of air transport and energy IRC. This research was performed within the 27 Member States and a selection of 13 neighbouring countries[11].

During a preliminary data collection phase, a first team of analysts gathered the relevant data in the data classification grid. A second team of analysts validated and further enriched the preliminary data. An overview of the collected data is detailed in chapter 5.1.

2.2.3 Step 3 – Designing and validating the survey

Publicly available information on air transport and energy Sectoral IRC procedures and tools was, as anticipated, not detailed enough to provide insightful input (see chapter 5.1).

[11] Albania, Bosnia-Herzegovina, Georgia, Iceland, Kosovo, Moldova, Montenegro, North Macedonia, Norway, Ukraine, the United Kingdom, Serbia and Switzerland.

Therefore, a survey to collect comprehensive data from relevant parties had been planned early on.

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

- 27 Member States' national CSIRTs;
- Additional public, private (IRC of Operator of essential services (OES)) and European sectoral CSIRTs from the 27 MS.

Further information on data collected can be found in A Annex – Presentation of the raw data (p. 44).

Together with ENISA, the project team then drafted the survey to be sent to both audiences considering aspects such as data protection, privacy and legal aspects, language, size and format, and structure.

The final version of the survey validated by ENISA is available in B Annex: Survey – questionnaire (p. 48)

2.2.4 Step 4 – Conducting the survey and complementary interviews

The survey was sent by ENISA to the 27 national CSIRTs and additional sectoral CSIRTs through the CSIRTs Network[12]. To maximise participation the survey included a presentation of the study and its context.

Targeted e-mails were sent to relevant contacts and followed up on, to ensure a high response rate from Member States and sectors.

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

- Sectoral Cybersecurity experts;
- Members of the Informal Expert Group on Incident response Capabilities;

A list of entities was drafted for each group with an interview rationale validated by ENISA. Once agreed, participants were able to fill-in the survey, using the EU survey tool, or scheduling a phone interview to provide their answers.

An overview of the raw data collected through the survey is detailed in A Annex – Presentation of the raw data (p. 44).

2.2.5 Step 5 – Collation of raw data

The raw data collected from the desktop research, the survey and the interviews, was aggregated 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. This method ensures that the data collection team and the data analysis team benefit from and build on

[12] https://csirtsnetwork.eu/

each other's expertise, and that the final analysis addresses all aspects of the request presented in a concise, coherent and comprehensive way.

The data collection team and the data analysis team performed a first analysis of the raw data to develop a draft set of key findings. With analysis methods applied, the teams drafted a first version of the key findings of the study and submitted it to ENISA for validation and further discussion.

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

After the virtual workshop and once all final comments were received, a preliminary version of the final report was drafted and submitted to ENISA for validation and further discussion.

2.2.7 Step 7 – Final report

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

Close interactions and exchanges with ENISA ensured that the final recommendations of the study were in line with the Agency's needs and expectations.

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 were made. A detailed overview of the raw data is presented in A Annex – Presentation of the raw data (p. 44).

For both the desktop research and survey data collection phases, research identified all CSIRTs relevant to the energy and transport sectors about which information was publicly available, regardless of size or maturity. As described in the key findings, whether these two sectors are covered by sectoral or by national CSIRTs varies from country to country. The information is summarised p. 16.

2.3.1 Desktop research – Data collection assessment

During the open-source desktop research phase, information on IR layout and set-up was collected for 19 out of 27 Member States and a few elements were collected for the remaining 8 MS.

- The clarity and level of information available on national IR approach in NISD sectors was very different from one Member States to another;
- 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;
- Qualitative information on information exchange communities and fora were rarely, if ever, detailed in publicly available documents.

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

2.3.2 Survey – data collection assessment

The survey collected answers from 20 respondents from 13 Member States and 1 regional air transport organisation:

- 10 National CSIRTs;
- 4 Regulatory organisation, body or Ministry;
- 2 Sectoral CSIRT (1 national and 1 European);
- 4 Energy and Air Transport OES IRT.

Further information is presented in A Annex – Presentation of the raw data (p. 44). Specific information about the breakdown of respondents by type and sector can be found p.46.

2.3.3 Interviews – data collection assessment

And additional two interviews were conducted with sectoral experts in each of the two targeted sectors (Air Transport and Energy) along with extra interviews conducted with members of the Informal Expert Group on Incident Response Capabilities.

3. KEY FINDINGS

3.1 KEY FINDING #1- IRC SET-UP AND LANDSCAPE

A large majority of EU countries tend to have dedicated sectoral specialists and experts within their National/governmental CSIRTs rather than a dedicated sectoral entity at national level. Sectoral CSIRTs are not yet the norm in the EU.

Our research, which covered the 27 EU Member States, identified National sectoral CSIRT capabilities in 19 Member States[14]:

- 65% (12 out 19 MS) have no Sectoral CSIRTs, 9 haven't planned to create one in the near future, but 3 are discussing the possibility of creating one some at national level in the future, should the need arise;
- 1 MS is currently setting up both an Energy and Air Transport CSIRT at national level;
- 4 MS have no Energy or Air transport CSIRT at national level yet but do have other Sectoral CSIRTs (Finance, Health or Water, etc.);
- 1 MS has an Energy Sectoral CSIRT at national level and 1 MS has an Air Transport Sectoral CSIRT at national level;

To this date, the general approach towards IR set-up in both the Energy and Air Transport sectors in the EU is to have the National CSIRT acting as the competent authority for IR and OES in charge of conducting incident response at operational level, with a dedicated unit or sectoral expert to that purpose.

Table 1: Overview of all MS' basic IR set-up in sectors (with available data collected)

Countries	Summary of national approach toward IR in the Energy & Air Transport sectors
Austria	The Federal Chancellery is the Strategic NIS authority and CERT.at, the national CSIRT, is the primary contact point for IT-security in a national context. CERT.at coordinates other CSIRTs operating in the area of critical or communication infrastructure provides basic IT-security information to SMEs. In case of significant online attacks against Austrian infrastructures, CERT.at will coordinate the response by the targeted operators and local security teams. The Austrian Energy CERT (AEC) is the single contact point for incidents in the Energy sector. There is no dedicated entity for the Air Transport sector.
Belgium	The Centre for Cybersecurity Belgium (CCB) acts as the national coordination authority, and acts as national CSIRT in the CSIRTs Network. In support of the national CSIRT, each sectoral authority may choose to develop a sectoral CSIRT, subject to compliance with the obligations set out in Annex I of the transposition of the NIS Directive. The CCB acts as coordinator for all sectoral CSIRT at national level. Belgium is currently discussing the creation of a sectoral CSIRT for Oil.
Bulgaria	CERT Bulgaria (English), is the National Computer Security Incident Response Team. Its mission is to provide information and assistance to its constituencies in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur. Bulgaria is currently creating sectoral CSIRTs to facilitate the implementation of the requirements of the NIS Directive.

[14] Our desktop research delivered a general overview of Incident Response Set-up in the 27 Member States. In 8 Member States (Croatia, Denmark, Hungary, Ireland, Italy, Latvia, Malta, Slovenia), no formal confirmation of the existence of sectoral CSIRTs at national level could be found at the time of the production of the present report.

Countries	Summary of national approach toward IR in the Energy & Air Transport sectors
Croatia	National CSIRT (CERT.hr) is a department within the Croatian Academic and Research Network – CARNET established in accordance with the Information Security Act of the Republic of Croatia. According to this Act, CERT.hr is a national body for the prevention of cyber threats and the protection of the security of public information systems in the Republic of Croatia. The department's main task is to handlecomputer security incidents to preserve the security of information systems in Croatia. Furthermore, according to the Act on cybersecurity of operators of essential services and digital service providers CERT.hr workswith the Information Systems Security Bureau (ISSB) of the Republic of Croatia on the coordination of prevention and response to computer threats to information systems security. The Information Systems Security Bureau (ISSB) is the central state authority responsible for technical areas of information security of the Republic of Croatia state bodies, which includes standards of information security, security accreditation of information security, managing crypto material used in the exchange of classified information, and coordination of prevention and response to computer threats to information system security. ISSB, is a CSIRT for most of NIS sectors, including energy and transport.
Cyprus	The Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) is an independent regulatory authority of the Republic of Cyprus in matters of electronic communications and postal services, with additional responsibilities in the areas of terminal equipment, network and information security and protection of critical information infrastructures. It was selected as the body responsible for coordinating the implementation of the National Cybersecurity Strategy of the Republic of Cyprus, in relation tothe pillars of network and information security (cybersecurity), cybercrime, cyber defence and related external affairs. OCECPR is responsible for the creation and coordination of a body or bodies for response to incidents related to Network and Information Security in Cyprus. It also supervises and regulates the activity of the above CSIRT entities. CSIRT-CY handles reported cyber incidents, proactively identifying potential threats and coordinating with relevant government agencies nationally, regionally and globally to reduce the impact of the cyberattacks.
Czech Republic	The Czech Republic has two response teams: 1) a Government Computer Emergency Response Team (GovCERT.CZ) and 2) a national Computer Security Incident Response Team (CSIRT.CZ). The Government CSIRT (GovCERT.CZ), https://www.govcert.cz/ (Czech); https://www.govcert.cz/en/ (English), is based in Brno. Its main task is to collect reports of cyber incidents from specified entities, analyse them and provide assistance.
Denmark	The principle of sectoral responsibility is the rule. It implies that the authority responsible for a given function on a day-to-day basis is also the responsible authority when a serious incident occurs. This responsibility also includes planning how to maintain and continue to supply functions in the event of an extraordinary incident. Consequently, responsibility for cyber and information security, and thus the task of protecting critical infrastructure, is divided between the authorities responsible for the critical sectors, i.e. the transport sector, the healthcare sector and the financial sector. The 2018-2023 Defence Agreement significantly enhances the ability of the Danish Centre for Cyber Security (CFCS) to assist central government authorities responsible for the various sectors.
Estonia	Estonia has opted fora centralised coordination and supervision of the sectoral IT security within the framework of the NIS directive's implementation. The activities falling within the scope of the NIS directive go to different units within the RIA. In addition to the operation centre, which also houses the CERT-EE, there is a standardisation and review unit whose task is to ensure compliance with the CSA (Cyber Security Act) and, in the long run, the NIS Directive. RIA CERT-EE plays the role of government CSIRT, which gives the authority good knowledge of the systems.
Finland	The National Cyber Security Centre Finland (Kyberturvallisuuskeskus, also referred to as NCSC-FI; previously CERT-FI) is responsible for the supervision of all Finnish CSIRTs. Its mandate includes incident response, preparedness, training, regulation and control. Sector-specific authorities have competence for supervision, namely the Energy Authority, the Centre for Economic Development, Transport and the Environment and the Finnish Transport and Communications Agency.
France	CERT-FR is the Computer Emergency Response Team of the French national cyber security authority. Its mission is to coordinate and investigate IT security incident response for the French government, critical national infrastructure operators and operators of essential services as defined by the French law. The primary constituency is composed of French territories and covers all ministries, administrations and state services; critical national infrastructure operators

Countries	Summary of national approach toward IR in the Energy & Air Transport sectors
	and operators of essential services as defined by the French law and other key players in sensitive sectors. CERT-FR was created in 1999 as a governmental CSIRT and afterwards became the National CSIRT. There are CSIRTs specific to companies, such as EDF in the energy sector, but the creation of sectoral CSIRTs is currently under discussion, although not in the air transport sector.
Germany	The Federal Office for Information Security, BSI, has gained expanded powers with the entry into force of the NISD, in addition to being the supervisory authority for all sectors, CSIRT and national contact points. BSI was previously primarily responsible for the security of critical infrastructures, but with the adoption of the NIS directive, the mandate has been extended to include network and information security.
Greece	GR-CSIRT was established in 2018. It is a National CSIRT. The GR - CSIRT is in charge of handling incidents (cyber attacks) affecting Operators of Essential Services (OES), is responsible for incident detection, incident response coordination and decision-making, including coordination with other national stakeholders..
Hungary	The core operational cyber security capabilities and cyber incident management are centralised in the governmental computer emergency response team in Hungary, GovCERT-Hungary, which is part of the National Cyber Defence Institute and supervised by the Ministry of Interior. GovCERT-Hungary provides services for the entire Hungarian governmental administration – especially for the government backbone system, for critical infrastructures and municipalities. Sectoral CSIRTs are being established: beyond the existing CIIP CERT (operating under the National Directorate General for Disaster Management), another two are being set up, one for defence within the Military National Security Service, and another one for civilian intelligence within the Information Office.
Ireland	CSIRT-IE is the body within the NCSC providing assistance to constituents in responding to cybersecurity incidents at national level for Ireland. The team has a strictly defined constituency consisting mainly of Government bodies and Critical National Infrastructure providers. CSIRT-IE provides incident response services to Government bodies and Critical National Infrastructure providers across Ireland. CSIRT-IE also acts as a national point of contact for international partners who wish to inform Irish-based entities of cybersecurity matters, which may affect them. The Irish Reporting & Information Security Service (IRISS) is an independent not for profit CSIRT dedicated to the broader public rather than companies or government and entities.
Italy	Computer Security Incident Response Team - Italia sits within the Department of Security Information (DIS). Its missions consist in: - monitoring incidents at national level; - warning interested parties of potential/ongoing attacks; - intervening in case of incidents; - performing dynamic analysis of risks and incidents; And includes situational awareness; participation to CSIRT networks. Computer Security Incident Response Team - Italia cooperates with the private sector and promotes the use of common practices and standards in risk management and incident-response, as well as classification of incidents, risks and information.
Latvia	The Latvian Computer Emergency Response Team - CERT.LV (Latvian: https://cert.lv/lv; English: cert.lv/en) is responsible for monitoring and analysing developments in cyberspace, reacting to incidents and coordinating incident prevention. It also carries out research, organises educational events and training, and supervises the implementation of obligations defined in the Law on Security Information. CERT.LV is expected to develop resources with the public and private sectors for collecting intelligence on incidents for analysis and evaluation.
Lithuania	The National Cyber Security Centre (NCSC) at the Ministry of National Defence is the main Lithuanian cyber security institution responsible for unified management of cyber incidents, monitoring and control of the implementation of cybersecurity requirements, accreditation of information resources. It was established after the entry into force of the Law on Cybersecurity in January 2015. The NCSC's mission is to be the centre of cyber security expertise for effective cyber security incidents and a strong cyber security prevention system in the country.

Countries	Summary of national approach toward IR in the Energy & Air Transport sectors
Luxembourg	The Institut Luxembourgeois de Régulation (ILR) ensures regulation and supervises the following economic sectors: network and communication, **electricity, natural gas**, postal services**, transport (rail and air)**, radio frequencies. CIRCL is the CSIRT for the private sector, municipalities and non-governmental entities in Luxembourg. Luxembourg's government CSIRT (govcert.lu) covers incidents targeting government and public or private OES.
Malta	CSIRTMalta is responsible for coordinating incident response measures for entities engaged with Maltese critical infrastructure. The Information Security & Governance Department's Security Engineering Team covers government IT security.
Netherlands (The)	The National Cyber Security Centre (NCSC.NL) (Dutch, English) was established in 2012 and incorporates the Dutch Computer Emergency Response Team for the Dutch central government. NCSC.NL is responsible for the coordination of incident response measures for Dutch government institutions, as well as entities engaged with critical infrastructure. The NCSC covers multiple functions, such as managing the reporting of cybersecurity incidents with a multi-channel reporting structure to log said incidents. The Centre is also responsible for maintaining a national detection response network for the governmental sector and entities engaged in the event of a cybersecurity incident. The centre also actively participates in the work of the Information Sharing and Analysis Centres (ISACs) for sectors involved with critical infrastructure.
Poland	In Poland, entities involved in handling and responding to computer incidents at national level are the Computer Security Incident Response Team (CSIRT GOV), the Ministry of Defence Computer Emergency Response System (CSIRT MON) and the National Cybersecurity Centre (NC Cyber or CSIRT NASK). Their mission is to counter cross-sectoral and cross-border cyberthreats, to coordinate the handling of major, substantial and critical incidents, and to provide information about incidents, both within the network of government organisations related to cybersecurity and to the general public.
Portugal	The National Cybersecurity Centre (Centro Nacional de Cibersegurança) is the Portuguese cybersecurity national authority. It has regulatory, supervisory, enforcement and sanctioning functions and the power to issue cybersecurity instructions. It defines the national level of cybersecurity alert. In addition, a National Computer Security Incident Response Team (CERT.PT) operates within the National Cybersecurity Centre and its main competence is to: (i) Implement operational coordination in response to incidents, in particular in liaison with existing sectoral IT security incident response teams.
Romania	CERT-RO is the competent national authority for the implementation of the NIS Directive. CERT-RO's missions are to prevent, analyse, identify and respond to cybersecurity incidents related to Romanian cyberspace. CERT-RO acts as National contact point for cybersecurity incidents with similar structures within or outside Romania. CERT-AV-RO, which runs within Romania Civil Aviation Authority (RO-CAA, acts as the Romanian civil aviation sectoral CSIRT and there are plans for setting up other sectoral CSIRTs in the near future.
Slovakia	Created in 2016, the National Cyber Security Authority SK-CERT provides national and strategic activities in the field of cyber security management, threat analysis as well as coordination of national security incident resolution. The National Cyber Security Centre also supports governance, development, management and support of cybersecurity competence centres, including training, educational activities, and research.
Slovenia	The Slovenian Information Security Administration (Uprava RS za informacijsko varnost - ZInfV) acts as a National CSIRT, the national response centre primarily responsible for examining security incidents. The ZInfV also provides for the establishment of state administration authorities' CSIRT. The Slovenian Information Security Administration operates under the authority of the Ministry of Government Administration. The Slovenian Information Security Administration began operating on 1 January 2020.
Spain	The CCN-CERT is responsible for the management of cyber-incidents affecting public or private sector organisations. In the case of critical public sector operators, the management of cyber-incidents is carried out by the CCN-CERT in coordination with the Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).
Sweden	CERT-SE is the National CSIRT of Sweden. Its constituency consists of Swedish society, including but not limited to, governmental authorities, regional authorities, municipalities, and companies. In addition, CERT-SE is also Sweden's governmental CSIRT.

As illustrated in the table above, the sectoral Incident Response layout and set-up at European level in both the Air Transport and Energy sector is still recent and evolving. The ecosystem is organised around the following elements:

At national level, Incident response set-up is structured around:

- **Generic IR services provided by the national/governmental CSIRT in each EU Member State for all sectors, including Energy and Air Transport.** This is particularly relevant in countries with a centralised IR model;
  These national/governmental CSIRTs either have specific experts and specialists within their organisation for these two sectors or a dedicated unit. In these Member States, Energy and Air Transport OES are also developing their own internal CSIRTs or are externalising this activity to certified Digital Service Providers (DSPs);

- **For two Member States, dedicated Sectoral CSIRTs coordinate incident response at national level, supervised by the national CSIRT.**

At European level, the landscape also includes international organisations' sectoral CSIRTs intended to develop requirements and regulations and to provide a forum for sector stakeholders.

Both sectoral IRC/OES IRT at national level and Sectoral CSIRT of international organisations tend to be recent (less than 5 years old) and are still in the development phase of their capabilities.

→ **Summary:** All Member States recognise the need for specific IR expertise for NISD sectors at national level to support OES and sectoral actors. This specific IR expertise can either be mutualised within the National CSIRT or organised as a separate and dedicated sectoral entity. This expertise is essential as IR capabilities must be aligned with the risk management process specific to each sector.

3.2 KEY FINDING #2 – CREATION OF SECTORAL CSIRTS

The EU countries which decided to create a dedicated sectoral CSIRT for the Energy or Air Transport sector were driven by organisational and functional needs rather than technical ones.

A closer look reveals that for those two Member States who decided to create a dedicated sectoral CSIRT for Energy or Air Transport at national level, the main drivers were organisational and functional needs rather than technical ones.

Both the Energy Sectoral CSIRT and the Air Transport Sectoral CSIRT created at national level responded to a need and a specific demand from sector stakeholders to organise Incident Response nationally.

"[there is a] need for facilitating oversight and compliance" (Air Transport Sectoral CSIRT)

Table 2: Case Study – Creation of the Austrian Energy CERT

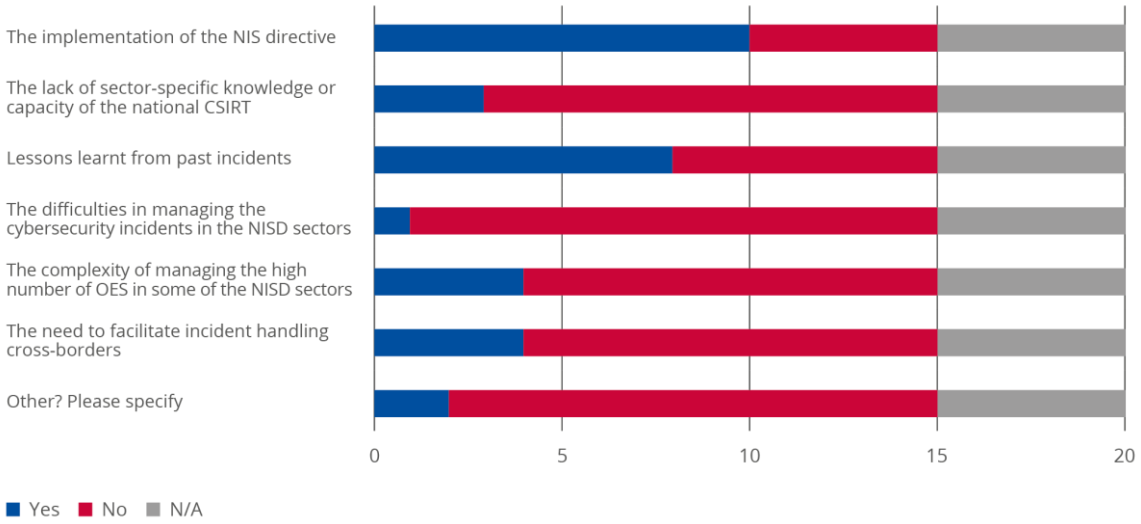
Case study
Austrian Energy CERT (AEC)
Background and context of creation
The Austrian energy sector regulator (E-Control Austria), the sector association (Oesterreichs Energie) and the most important energy companies in the electricity, oil and gas subsectors worked together on an analysis and evaluation of security of supply in 2015. This work intended to identify the risks arising from the use of ICT infrastructure and to examine them in detail. This resulted in a successful joint initiative in the form of a public-private partnership (PPP). This partnership further enhanced mutual understanding and trust. It also increased awareness and acceptance of preventative measures to boost resilience. One of these measures was the creation and operation of a computer emergency response team (CERT) for the Austrian electricity and gas sectors.
Sources
https://www.energy-cert.at/en/about-us/ http://www.aec.arge.or.at/index.php/en/about-us.html https://www.geode-eu.org/wp-content/uploads/2019/07/3-4-Selhofer-Armin.pdf

Although not a member of the European Union, Norway is also an interesting case to mention among the European Free Trade Association (EFTA) countries. KraftCERT (Norwegian energy sector CSIRT) is the result of a joint initiative from NorCERT and the Norwegian Water Resources and Energy Directorate (NVE). The Sectoral CSIRT aims to support the entire power industry at national level in the prevention and handling of security incidents[15].

As illustrated below, the creation of sector-specific IR Capacities was not the result of the lack of sector-specific knowledge of the National CSIRT, nor the inability to manage cybersecurity incidents in the sectors at national level.

[15] https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf

Figure 3: Drivers to create sector-specific IR Capacities



NB: Five respondents decided not to answer this question as they do not have a national sectoral CSIRT and for the moment do not intend to create one in the near future.

According to 50% of respondents, the need to facilitate the implementation of the NIS Directive is one of the most important drivers behind the creation of such sector specific IR capacities. It shows that European legislation has an important and positive impact in pushing actors to develop sectoral capacities[16].

The need to be prepared and to facilitate the implementation of the requirements of the NIS Directive is shared by those two Member States currently preparing or discussing the creation of sectoral CSIRTs and by sectoral private operators who decided to create an internal IR capacity.

Both Denmark and Belgium are currently discussing the creation of an energy CSIRT at national level. According to Denmark's sectoral strategy[17], « *it is considered that such a sector CERT with sector-specific competences is relevant to the energy sector to act on the cyber threats* ». Danish authorities will explore how a sectoral CSIRT could be established and whether there is a basis for establishing a common CSIRT with specialist competence in cybersecurity in the energy sector. Depending on its structure, a sectoral CSIRT will be able to contribute specific knowledge and experience-based competencies such as advising and training. In Belgium, the creation of an oil-sector CSIRT is currently under discussion[18].

[16] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62799
[17] https://fmn.dk/eng/news/Pages/New-sectoral-strategie-stop-repare-society-for-cyberattacks.aspx
[18] https://www.energy-community.org/dam/jcr:23cf8d77-32dd-4152-b040-51e3a17bd19c/FPS Economy, Cybersecurity in the oil sector.pdf

Table 3: Case Study - Bulgarian Cybersecurity Strategy

Case study
Bulgaria
Background and context of the will to create Sectoral CSIRTs
In October 2018, the Bulgarian Parliament approved a new Cybersecurity Act, which is the transposition of the NIS Directive into national law. The Cyber Security Act determines the overall organisation, management and control of cybersecurity at national level and establishes new authorities and their responsibilities. According to the Act, the "Electronic Governance" State Agency (or the "E-Governance Agency") is the national competent authority and is thus empowered to establish a national Computer Security Incident Response Team (CSIRT). Currently, a Bulgarian CSIRT Centre exists (https://govcert.bg), which assists in reducing the risks of information security incidents and resolving such incidents if they have already occurred. The Act states that **Computer Security Incident Response Teams are to be established within competent local authorities in various sectors** (i.e. **energy, transport**, banking, financial market infrastructures, health, and digital) and will coordinate their activities with the national CSIRT.
Sources
https://www.cms-lawnow.com/ealerts/2018/11/bulgaria-adopts-new-cyber-security-act http://www.aec.arge.or.at/index.php/en/about-us.html

The response of a private electricity provider from a large member state, which decided to create its own CSIRT in January 2019 is an illustration of this trend.

"There was a growing awareness of the need to create an internal capacity to handle incident response in the organisation. The Chief Information Officer was aware of the lack of preparedness and had the will to invest to be prepared for the upcoming changes (GDPR, NIS Directive implementation, upcoming status of OES). We wanted to anticipate the future taking into account the growing number of attacks targeting other actors."

Another point to reflect on is that both Energy and Air Transport Sector deal with cross-border aspects. There is, therefore, a need for cross-border communication between entities, which could be facilitated by the creation of sectoral CSIRTs.

→ **Summary:** The creation of sectoral entities tends to facilitate the functioning of IR at national level, the implementation of cybersecurity regulations and cross-border cooperation for sectoral actors.

3.3 KEY FINDING #3 – SECTORAL CSIRTS SERVICES

National energy and air transport sectoral CSIRTs tend to provide their constituency with very sector-specific expertise in addition to the generic services provided by national CSIRTs.

As illustrated in chapter 3.1, a majority of EU countries tends to either rely on the generic services of their national CSIRT or to support the development of Incident Response capabilities of operators of essential services in the energy and air transport sectors. The focus of the study was therefore to analyse the differences between specific services provided by National Sectoral CSIRTs as opposed to those provided by National CSIRTs.

According to survey responses, and as confirmed by additional desktop research, Sectoral CSIRTs at national level tend to provide very sector-specific expertise and maintain closer relationships with their constituents.

Additional services provided by Sectoral CSIRTs at national level differing from those of National CSIRTs include:

- Specific information and in-depth knowledge in their sector;
- Sector-specific network of contacts;
- Closer relationships with vendors of the sector;
- Expertise on sector-specific hardware and systems;
- Sector-specific conferences, workshops, and training;
- The creation of uniform frameworks for audit documentation at sectoral level;
- Faster sectoral communication channel, as their constituency base is smaller than the one of a National CSIRT;
- Sector-specific recommendations.

"It [the Sectoral CSIRT] could provide more in-depth knowledge of the sector's specificities & challenges" (National CSIRT)

"A Sectoral CSIRT at national level could provide a more in-depth knowledge of the sector's specificities & challenges." *(National CSIRT)*

In addition to those services, Sectoral CSIRTs would be an important player to organise sectoral exercises as they have good communication channels and closer relationships with the main sectoral stakeholders at national level.

In Romania, the creation of a dedicated sectoral CSIRT for Air Transport at national level was driven by the following key needs:

- The need for a real-time and integrated response capability;
- The need for a continuous and up-to-date situational awareness;
- The need to facilitate oversight and compliance;

CERT-AV-RO was created as a consequence within the Romanian Civil Aviation Authority to facilitate the monitoring, detection and coordination of the response to correlated incidents, as well as cooperation and hierarchical reporting. The services provided by CERT-AV-RO compared with those of the National CSIRT are presented below.

Table 4: Case Study - CERT-AV-RO - Specific mandate and services compared with those the National CSIRT

Case study	
Romania	
National CSIRT's mandate (CERT-RO)	**Sectoral Aviation CSIRT's mandate (CERT-AV-RO)**
CERT-RO is the competent national authority for the implementation of NIS Directive. Its mandate includes: – the prevention, analysis, identification and response to cyber security incidents related to Romanian cyberspace. – a national contact point for cybersecurity incidents for similar structures within or outside Romania. – the development of national IT security policies and strategies along with other Romanian public authorities and the proposition of regulations regarding the national cybersecurity strategy. – the official advisor of the national public authorities for the cyber-protection of critical infrastructure.	CERT-AV-RO is responsible for integrated incident management for the entire civil aviation sector. Each civil aviation entity has full responsibility for the management of cybersecurity incidents in their organisations. CERT-AV-RO and RO CAA's responsibility is limited to integrated and correlated monitoring and detection of cybersecurity events and incidents, as well as to the coordination of incident response when an incident impacts more than one organisation.
National CSIRT's services	**Sectoral Aviation CSIRT's specific services**
Proactive • Cybersecurity warnings and pre-announcements; • Cybersecurity audits and vulnerability assessments; • Cybersecurity application development; • Security-related information and dissemination. **Reactive** • Cybersecurity alerts; • Incident coordination and response; • Incident analysis & investigation; • Incident management at national level. **Support** • Training other CSIRT teams and security response teams; • Building cybersecurity awareness (events, conferences, courses etc.).	**Reactive** • Coordination of incident response in the Civil Aviation sector; • Correlation & integration of cybersecurity events and incidents detected in the Civil Aviation sector. **Compliance** • Facilitation of oversight and compliance of the civil aviation entities with respect to the cybersecurity regulation. **Support to cybersecurity R&D** • Facilitation of the Research & Development & Innovation (R&D&I) efforts in order to ensure the creation and implementation of dedicated cybersecurity solutions.
Sources	
https://www.terena.org/activities/tf-csirt/meeting36/tofan-cert-ro.pdf Interview with CERT-AV-RO	

Table 5: Case Study - Future Belgian Sectoral CSIRTs - Specific tasks compared with those of the National CSIRT

Case study	
Belgium	
National CSIRT's mandate (CERT-BE)	**Future Sectoral CSIRT's mandate**
The Centre for Cybersecurity Belgium acts as the national coordination authority and as the national CSIRT in the EU-CSIRTs Network. Its tasks include: - Coordination for all sectoral CSIRTs; - Monitoring incidents at national and international level; - Issuing of early warnings, alerts, announcements, dissemination; - Response to incidents; - Provision of a dynamic risk and incident analysis - Detection, observation and analysis of computer security problems - Promoting the use of common or standardised practices in the field of procedures for the treatment of incidents and risks, and systems for the classification of indigents, risks and information - Ensuring cooperation-oriented contacts - Participation in EU CSIRTs Network.	Future sectoral CSIRT tasks include (in cooperation with CCB): - Monitoring sectoral incidents and obligations to notify CCB through the common notification platform (www.nis-incident.be); - Issuing of early warnings, alerts, announcements and dissemination of information on risks and incidents to relevant stakeholders in the sector; - Response to sectoral incidents; - Dissemination of knowledge of the dynamics or risks of sectoral incidents and ensure situational awareness; - Ensuring cooperation-oriented contacts with the sector's suppliers; - Participation in meetings of the CSIRTs Network dedicated to its sector.
Sources	
Implementation in Belgium of the Directive EU 2016 1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, CCB	

In addition to their sector-specific service offer, both Sectoral and OES CSIRTs provide generic services in the four main services areas identified by the FIRST CSIRT Services framework[19]:

- Information Security Event Management;
- Information Security Incident Management;
- Vulnerability Management;
- Knowledge Transfer.

According to survey responses, both National and Sectoral CSIRTs' main services and functions relate to Information Security Incident Management and Vulnerability Management, among others.

Sectoral CSIRTs tend to be recent and therefore dedicate their resources to these two services and focus less on knowledge transfer activities.

→ **Summary:** Sectoral CSIRTs play an important role in facilitating operational collaboration and information sharing at Sectoral level.

FIRST CSIRT SERVICES FRAMEWORK
The FIRST CSIRT Services Framework seeks to assist CSIRT teams by identifying and defining core categories of services and their sub-components.

[19] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

3.4 KEY FINDING #4 – SECTORAL IR PROCESSES AND TOOLS

The tools and processes used by sectoral CSIRTs to deliver their services are similar to of national CSIRTs.

The main IR tools in service in both National and Sectoral CSIRTs are a combination of open-source, commercial and internally developed tools which are mostly in service in mature CSIRTs. Recently created entities, in particular recently created OES CSIRTs, are still testing open-source or commercial tools.

Table 6: Case Study - Commonly-used tools in service in both National and Sectoral CSIRTs, categorised by service area

CSIRTs key service areas	Tool Family	Commercial tools in service	Free tools in service	Others (data sources, methodologies, etc.)
Information security event management	SIEMs	Splunk, RSA, Darktrace, ManageEngine	HIDS OSSEC	Security Incident Management (SIM), Log System, Security Operation Management (SOM), Business Process Modeling (BPM) , GRC/ IRP
	DLP Systems	ManageEngine DataSecurity		
	Resources/Inventory management	ITmanager		
	Helpdesk software	Service Desk Plus		
	Others	Incident Register, Sharepoint		
	Ticketing		Request Tracker (RT), RTIR	
	Threat intel sharing		MISP, IntelMQ, ThreatExchange, OTR (Open Threat Exchange)	
Information security incident management	SOARs (Security Orchestration Automation Response)	OTRS	TheHive, Request Tracker, RTIR, IntelMQ	Active & passive monitoring tools, security assessment tools, RT SIEM, IT-Service-Management, semi-public or commercial feeds
	Analysis Tool	Commercial Sandbox	Free Sandbox	
Vulnerability management	Vulnerability scanners	Nexpose, Nessus, Tenable, Retina, SIM	Opensource Nexpose Nessus, Kali OpenVAS	Penetration testing
	Ticketing		Request Tracker (RT), RTIR	
	Resources/Inventory management	ManageEngine Desktop Central, Ivanti		
	Antivirus, UTM (Unified Threat Management):	AD Audit Plus	ADAudit	
	Intrusion/Detection System	Vectra Cognito		

CSIRTs key service areas	Tool Family	Commercial tools in service	Free tools in service	Others (data sources, methodologies, etc.)
Situational awareness	SIEMs IT park management tools Other Free Generic	Splunk Nagios, SCOM ONMSi, SOFTIKA, ProofPoint Sharepoint	MISP, Request Tracker (RT) Intranet portals, business e-mail, websites, monitoring and visibility tools, Dedicated alerting & reporting dedicated portals	Social media, Cyber Threat Intelligence feeds, conferences, metrics, active & passive monitoring tools, security assessment tools, bulletins, training platforms, Cybersecurity solutions incorporating behavioural analytics, e-learning policies and procedures, internal and external notifications, TTP (Tactics, Techniques, and Procedures)
Knowledge transfer		Mattermost, TSM, Microsoft Sharepoint,	Free: MISP Generic: Wiki, file exchange platforms, Mail; Dedicated alerting & reporting dedicated portal business e-mail, GitLab, SMS notifications, websites	Trainings, policies and procedures, governance; TTP, metrics Conferences, Twitter;

Most IR teams have Standard Operating Procedures (SOPs) and procedures in place except for the most recent CSIRTs. Those teams are still testing or selecting tools and therefore are still preparing associated procedures and SOPs.

Despite varying maturity levels, most CSIRTs tend to have very organised procedures in place to handle incidents.

According to ENISA CSIRT Maturity assessment[20] Model, CSIRTs can self-assess their team's maturity based on a list of 44 parameters over 4 categories: O (Organisational), H (Human), T (Tools) and P (Processes). Each main category includes a diverse range of parameters such as those defined for Organisational parameters, which analyse the mandate, constituency, authority, responsibility, or services of the CSIRT.

The ENISA CSIRT Assessment model defines a list of key parameters to analyse a CSIRT Tool maturity including the following:

- An IT Resource List;
- An Information Sources List;
- A Consolidated E-mail System;
- An Incident Tracking System;
- A resilient Phone, email and Internet Access;
- An Incident Prevention, Detection and Resolution Toolset.

[20] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

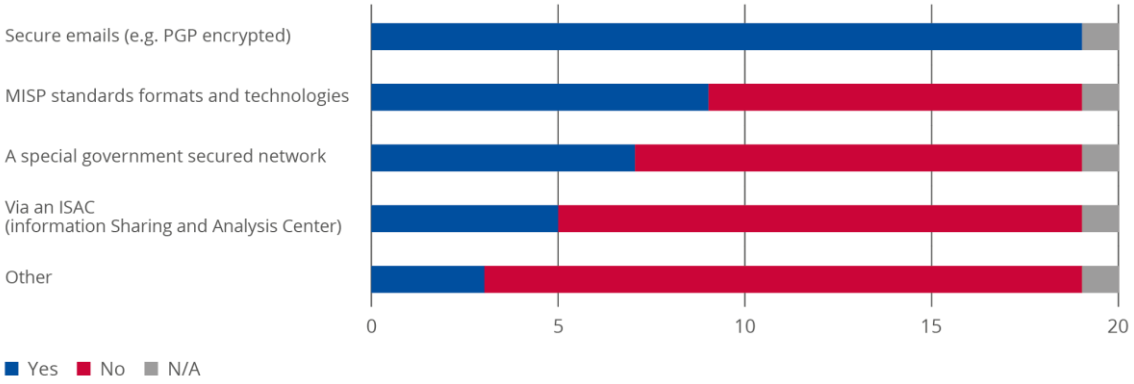
The evaluation of the presence, existence of guidelines/procedures and effective use of the elements listed above are an excellent method to assess the maturity of CSIRT tools. There are several methods available for maturity assessment in addition to the one proposed by ENISA.

The analysis of the CSIRTs through the survey (National CSIRTs in charge of IR in energy and Air Transport Sectors; Sectoral CSIRTs at national level, OES IRTs), gave the following results:

- 70% of respondents have formal SOPs that OES teams should follow in case of an incident. Among the remaining 30%, some are in the process of developing such guidelines and two participants did not provide an answer to this question.

- 82% of respondents use a formal incident notification template and those who do not have an SOP yet are in the process of establishing one.

Figure 4: Specific information exchange tools for notification of incidents



- 100% of respondents have specific information exchange tools (commercial or dedicated) to enable the notification of incidents. Among these tools, the most commonly used is secure e-mail.

France is an interesting case study in terms of good practices. The Member State has various procedures in place at national level according to the nature of the actor targeted by a cyberattack.

Table 7: Case Study - French National Cybersecurity Agency Notification Portal

Case study	
France	
Notification template for Operators of Vital Importance (OVI)	**Notification template for Operators of Essential Services (OES)**
OVI must report to the National Cybersecurity Agency any information security incident having a significant impact on continuity of service. Information reported: - General information: date, name of OVI, reference of the vital information system, type, localisation, address; vital IS entry at stake, vital IS description; - Technical information: main vital IS components and technical characteristics, number of inter-connections, connection to Internet; - Outsourcing information: outsourcing of IS hosting, exploitation or maintenance & name of providers; - Security information: security needs, description of the impact, presence of an event detection system & type, date of last audit & type of audit. Confidentiality & dissemination: Classified ("*confidentiel défense*"), notification and dissemination restricted to secure channel adapted to classified documents. Notification template [In French] https://www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf	OES must report to the National Cybersecurity Agency any information security incident having a significant impact on continuity of service. Information reported: - General information: date, name of OES, type; - Contact details of the person reporting the incident; - Contact details of 1 to 3 persons to contact for additional information; - Incident description: network and IS affected, physical localisation of the network, date & time of the attack, incident description; - Impact: number of users affected, duration, geographical impact, reporting to other MS; - Significant impact: criterion from Directive EU 2018/151; - Incident management: qualification, root causes, modus operandi, current status, actions taken; assistance needed; - Other: other reporting scheme implemented, reporting to law enforcement; - Comments. Confidentiality level & dissemination: Restricted, dissemination restricted Notification template [In French] https://www.ssi.gouv.fr/uploads/2018/05/formulaire-incidents-ose_anssi.pdf
Notification template for Digital Service Providers (DSPs)[21]	
DSPs must report to the National Cybersecurity Agency any information security incident having a significant impact on continuity of service. Information reported: - General information: date, name of DSP, type; - Contact details of the person reporting the incident; - Contact details of 1 to 3 persons to contact for complementary information; - Incident description: network and IS affected, physical localisation of the network, date & time of the attack, incident description; - Impact: number of users affected, duration, geographical impact, reporting to other MS; - Significant impacts: criterion from Directive EU 2018/151; - Incident management: qualification, root causes, modus operandi, current status, actions taken; - Other: other reporting schemes implemented, reporting to law enforcement;	

[21] Some Air Transport and Energy stakeholders rely on the services of Digital Service Providers (DSPs) to conduct vulnerability management, incident management or other services. It is therefore interesting to also analyse their reporting requirements.

- Comments. Confidentiality level & dissemination: Public, no restriction. Notification template [In French] https://www.ssi.gouv.fr/uploads/2018/05/formulaire-incidents-fsn_anssi.pdf
Sources
https://www.ssi.gouv.fr/en-cas-dincident/

These IR tools and procedures tend to be included in CSIRT constituents' codes of conduct or are directly promoted by the National CSIRT.

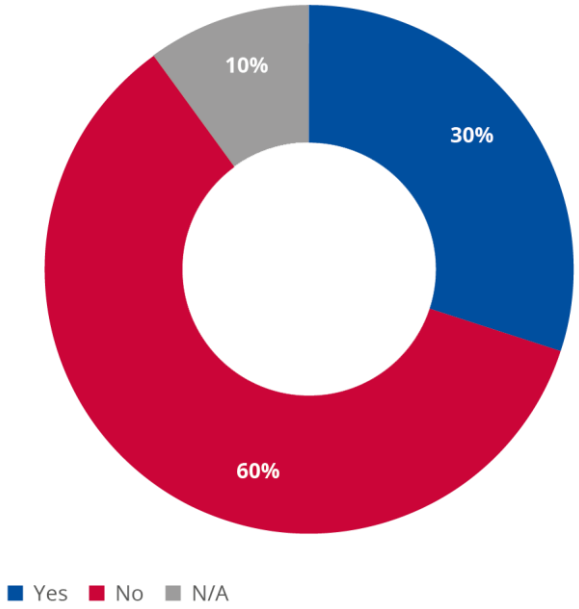
→ **Summary:** Sectoral IR stakeholders are constantly fostering their capabilities and benefit greatly from open-source tools and free commercial tools.

3.5 KEY FINDING #5 – SECTORAL IR MATURITY DEVELOPMENT

Though IR stakeholders did not request specific guidance when developing their capabilities, they tended to use dedicated tools made available by EU authorities, regulators and national CSIRTs.

According to the survey, a majority of CSIRTs, whether national CSIRTs, national sectoral CSIRTs or OES CSIRTs, did not seek any specific support or guidance from external stakeholders to design and implement sectoral IR capacities.

Figure 5: Specific information exchange tools used for notification

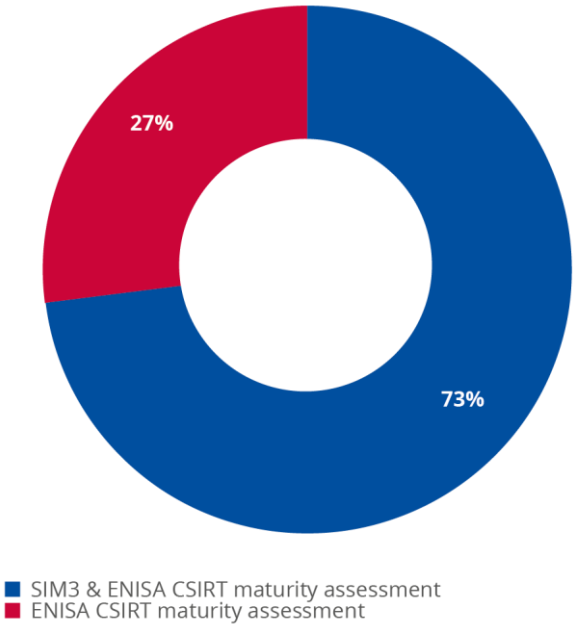


Even if they don't directly ask for support, they all tend to leverage the guidelines, tools and know-how made available by EU authorities, regulators or other national CSIRTs.

As an example, 60% of respondents use specific CSIRT maturity assessment methodologies to support the development of IR Capabilities in their sector. 70% out of these use both the ENISA CSIRT Maturity assessment[22] and SIM3[23]. Both methodologies are seen as valuable tools to enhance the maturation of CSIRTs.

[22] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey
[23] http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

Figure 6: CSIRT maturity Assessment methodology used



Together with National CSIRTs, regulators and professional associations are key enablers for capability development for the Energy and Air Transport Sectoral CSIRTs as well as OES CSIRTs. Several initiatives were recently implemented at sectoral level to foster these capacities, some by sectoral operators themselves.

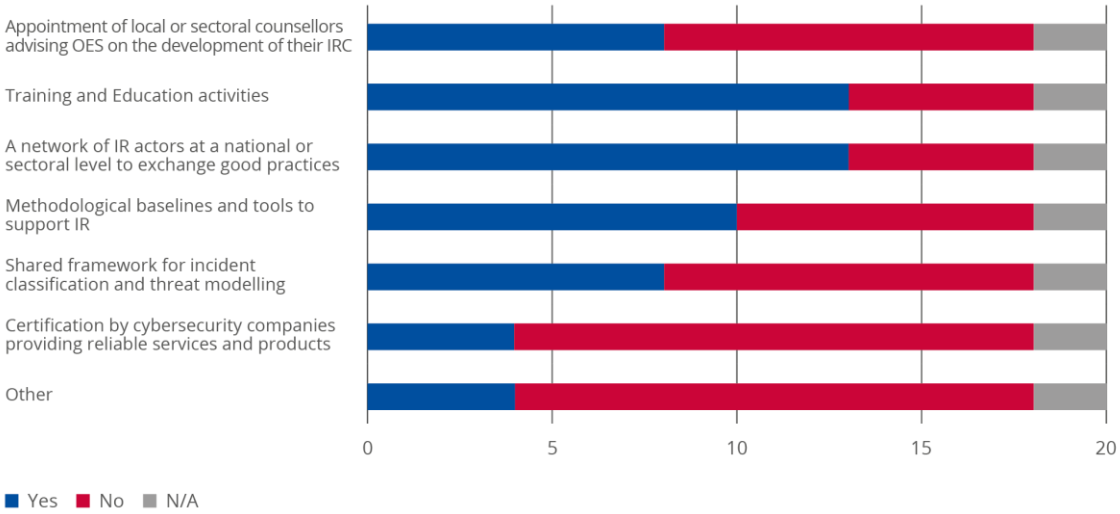
A noteworthy initiative in the energy sector is the 2019 launch of a cyber range dedicated to electricity operators. The German energy company Innogy opened its "CyberRange-e" training centre. The cyber range "*allows up to 12 network and IT specialists at a time to practice how to manage cyberattacks under real-life electricity grid conditions, including war-game methods, pitching the participants against real hackers*"[24]. According to Professor Andreas Pinkwart, Minister for Economic Affairs, Digitisation, Innovation and Energy of the State of North Rhine-Westphalia, this facility addresses the need to better protect and safeguard data, procedures and processes in the energy industry.

At European level, sectoral regulators are also developing initiatives to enhance sectoral stakeholders' incident response capabilities. As an example, the Council of European Energy Regulators offered a dedicated training on cybersecurity and the protection of the European energy sector[25] back in 2016.

At national level, many ministries, National Cybersecurity Agencies or National CSIRTs provide different support tools and initiatives to sectoral actors.

[24] https://www.energylivenews.com/2019/07/02/german-power-grid-operators-steel-themselves-for-cyber-attacks/
[25] https://www.ceer.eu/training/training_courses_2016/cyber_security_sept_2016#

Figure 7: Resources in place to support IRC development



The NIS Cooperation Group identified multiple examples in their "Sectorial implementation of the NIS Directive in the Energy sector" report[26] as illustrated below:

Table 8: Case Study - 9 Member States initiatives to support Energy Sector operators with their cybersecurity capacity-building[27]

Member State	Initiative
Austria	The Austrian Energy CERT organises frequent meetings with technical personnel as well as frequent meetings with senior management in the energy sector with a focus on their performance and development.
Czech Republic	State-organised workshops, exercises, methodology (a shared framework is currently being developed for all sectors) and supporting materials.
Denmark	Electricity distribution system operators (DSO's) can incorporate some of their cybersecurity expenses in their revenue cap, which offsets cybersecurity investments.
Estonia	State-organised trainings, penetration-testing, information-sharing facilitation.
Finland	Technical support programmes.
France	Publication of guidelines, audits, architecture support, technical services, regular threat reports and information on vulnerabilities from the CERT-FR and ANSSI. In 2003 a closed 'InterCERT-FR' CSIRT community was launched by ANSSI. It has since expanded and is now co-managed by ANSSI and community representatives. It is cross-sector and aims to support resilience and IR capacity building.
Luxembourg	Set-up of a comprehensive ecosystem with free or low-cost offers. Such offers include regular trainings, conferences, awareness sessions, tools for risk assessment and management. In the NIS context, OES will benefit from a free, sector-specific, customised risk assessment and management tool with integrated reporting to the competent authority and later from a centralised, one-stop notification platform for NIS, Telecom, GDPR and Critical Infrastructures. No fees will be recovered from OES.
Poland	Ongoing development of a public-private partnership under the control of the Ministry for Energy to enhance cybersecurity.

[26] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62799
[27] Source: Op.Cit

Member State	Initiative
Portugal	Training, awareness and maturity models for the assessment of the measures and procedures implemented is undertaken with the support of the Portuguese National Cybersecurity Centre.

Some sectoral CSIRTs also look for support from non-EU actors and tend to reach out to national cybersecurity and sectoral authorities from third countries. As an example, the Romanian Civil Aeronautical Authority (RO CAA) CSIRT (CERT-AV-RO) used:

- MITRE Corporation[28];
- The NIST Cybersecurity Framework[29];
- The Australian Cyber Security Centre;
- The United Kingdom Civil Aviation Authority and the UK National Cyber Security Centre (NCSC);
- The Centre for Internet Security (CIS) Best Practices based on “CIS Controls” and “CIS Benchmarks”[30].

→ **Summary:** ENISA and other EU institutions and stakeholders should continue their efforts to support capacity development across the European IR community by facilitating open access to resources and tools for operational stakeholders.

[28] US NGO: https://www.mitre.org/capabilities/cybersecurity/cyber-threat-intelligence
[29] https://www.nist.gov/topics/cybersecurity
[30] https://www.cisecurity.org/cybersecurity-best-practices/

3.6 KEY FINDING #6 – SECTORAL CSIRTS CHALLENGES AND GAPS 1/2

Sectoral CSIRTs in both air transport and energy sectors face a similar challenge, i.e. the overlap of multiple legislations and increasing time spent on compliance issues.

Both Air Transport and Energy operators share common specificities and similar challenges when it comes to incident response. Both sectors are considered to be the backbones of societies to such extent that any disruption could have a major impact on populations and economies. Shared specificities are:

- **Complex ecosystems with large supply chains**: both sectors count a wide variety of public and private-sector actors, ranging from government, regulators and professional associations to large industries, critical SMEs and digital service providers;

- **Infrastructure interdependencies:** both sectors have infrastructures strongly interconnected to others across the European Union and beyond. This can potentially lead to a cascading effect, and could result, in case of one system targeted, in all others being compromised. As an example, a gas pipeline can run through several countries, and an airport infrastructure is a commercial hub for essential products in a country.

- **Legacy systems and lack of security-by-design:** both sectors are composed of basic infrastructure elements (e.g.: transformers and generators in the Energy sector), all designed and built much before cybersecurity became an issue, and of more recent equipment used for automation and control, and increasingly dependent on ICT.

- **Real-time requirements and 24h coverage:** In both the Energy sector and Air Transport, several cybersecurity measures would be challenging to implement in real-time such as 24/7 monitoring coverage or systems shut down. This is particularly true for infrastructures that cannot be easily shut down given the prohibitive operational costs (financial and for users) associated with such a measure.

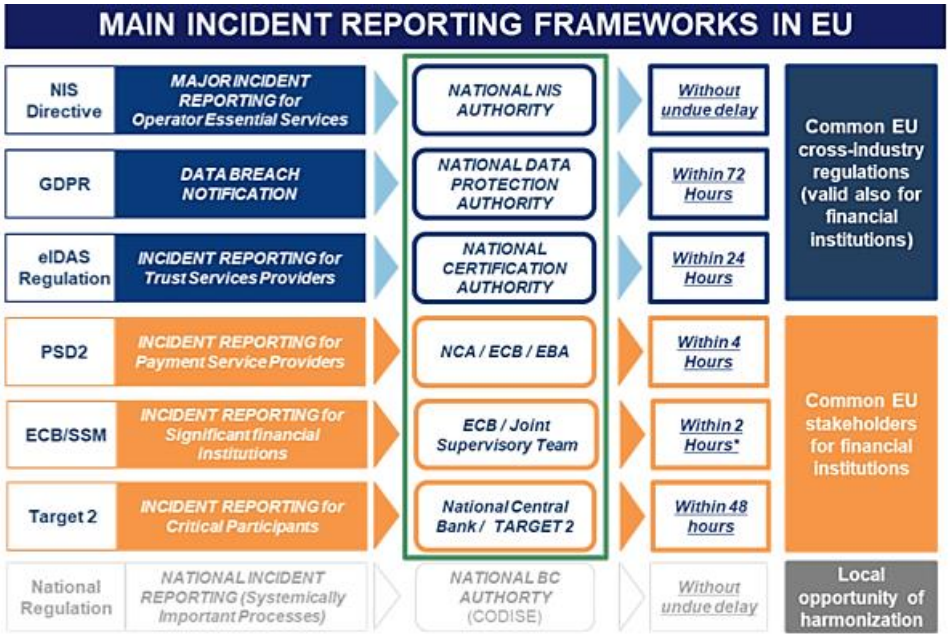
Because of these specificities, sectoral incident response stakeholders in both the Air transport and Energy sectors face common challenges.

One of the most common challenges raised by sectoral stakeholders, and common to all sectors and impacting the entire cybersecurity community, is how to deal and comply with the multiplication of requirements from national/EU authorities and sectoral actors (professional association and regulators).

"There is a high need for sync[hronisation] between EU regulatory bodies, regarding the harmonisation between the general cybersecurity regulation (i.e. NIS Directive) and the special/ specific cybersecurity requirements of each of the industries. Some of the industrial entities (which are defined specifically as under the NIS Directive jurisdiction, e.g. OES) refuse to respect the NIS Directive and the transposed national legislation, motivating that they are only under the jurisdiction of the special legislation. NIS Directive and special legislation shall complement each other, creating a framework of common base [and] complementary regulatory provisions." (Air Transport Sectoral CSIRT)

The European Banking Federation points to an interesting example of competing cyber-incident reporting schemes to be applied in the European Union.

Figure 8: Main Incident Reporting Schemes in the EU (Source: EBF)[31]



As illustrated, for specific cyber-incidents involving a data breach, both Energy and Air Transport stakeholders could apply at least three common EU cross-industry regulations (namely the NIS Directive, the GDPR, the e-IDAS Regulation) along with the National reporting regulation in place in their countries.

In Air Transport sector, several actors lead different activities related to cybersecurity. EUROCONTROL is currently the only one receiving direct information on incidents in ATM systems, leaving other activities focusing more in collaboration. An effort towards a coordinated common vision is required.

The multiplication of security and reporting requirements pushes operational actors to spend time updating their procedures to stay compliant. While costly for all, this can be particularly tough for smaller entities with less resources available to ensure compliance.

"The efforts that we consume for the justification of the cybersecurity realities in front of the financial control authorities' overpass, often, the efforts for the actual development and implementation of the domain. This is a critical issue, keeping the entire development process to the ground." (Sectoral CSIRT).

Sectoral stakeholders have called for a harmonisation of security regulation as a mitigation action meant to leverage revision processes. DG ENER, for instance, created a stream for private actors in the NIS revision process. At the same time, Air Transport stakeholders are continuously exchanging with regulators to share their operational requirements and input.

→ **Summary:** The upcoming revisions of the NIS Directive and GDPR could be an opportunity to harmonise legislation by considering sectoral stakeholders' feedback.

[31] EBF position on Cyber incident reporting, EBF, October 2019 source: https://www.ebf.eu/wp-content/uploads/2019/10/EBF-position-paper-on-cyber-incident-reporting.pdf

3.7 KEY FINDING #7 – SECTORAL CSIRTS CHALLENGES AND GAPS 2/2

Sectoral CSIRTs in both the air transport and energy sectors face a common challenge in formally and rapidly share ex-ante information in a particularly tense context

Energy and Air Transport stakeholders are well aware of the need to enhance information-sharing at sectoral level, yet they share a common difficulty in rapidly sharing ex-ante information. According to sectoral stakeholders, incident response community fora are useful to promote discussion among stakeholders but are rarely used to exchange real-time technical information about vulnerabilities and threats.

"There should be a wider dissemination of both technical and non-technical information related to incidents across the EU." (OES CSIRT)

All survey respondents use various international, European, national and sectoral groups and fora (ENISA CSIRTs Network, the FIRST Community, National inter-CSIRTs Network, etc.) to exchange information and best practices. Yet they tend to rely on mastered tools, such as private MISP instances, or mass communication tools tweaked for a specific use, such as WhatsApp, to exchange operational or real-time information with peers in an informal way.

Both Energy and Air transport sectors include a multiplicity of actors and have a very wide surface of exposure to attacks. Incident response is therefore even more challenging and requires in-depth expertise and important capabilities to successfully ensure 24/7 coverage and rapidly share information about cyber threats.

"[There is a need for] setting up fast channels of information exchange on cybersecurity threats" (Sectoral Ministry)

"There is a need for setting up fast channels of information exchange on cybersecurity threats." ***(Sectoral Ministry)***

A recurrent explanation is that stakeholders prefer to share ex-post rather than ex-ante information to avoid reputational and commercial damages.

To mitigate this, stakeholders confirm that dedicated sectoral fora are beneficial for information-sharing. Within those fora, information is sector-focused, up-to-date and exchanges are often made real time. Participants are more encouraged to share information with peers from the same sector as they use the same tools. They also rely on similar infrastructure and face similar threats.

Several sectoral initiatives can provide interesting good practices and lessons learnt, such as the Energy ISAC[32], the Health ISAC[33], the Aviation ISAC[34] or the Energy Community of Users that the European Cybersecurity Community is currently developing.

Sectoral ISACs are seen a "useful mechanism" and a trusted place to share operational information with peers. As such, they should be better recognised. Certain tools such as MISP or automated solutions could be explored to enhance information-sharing.

→ **Summary:** Sectoral communities of users constitute a key tool to enhance operational information-sharing. Besides, the use of automation should be explored.

[32] https://www.ee-isac.eu/
[33] https://h-isac.org/
[34] https://www.a-isac.com/

3.8 KEY FINDING #8 – SECTORAL CSIRTS LESSONS LEARNT

Though ongoing programmes and information-sharing initiatives have successfully supported IRC developments in both sectors, there is still a strong demand for more frameworks, guidance and know-how

Existing capacity-building initiatives implemented at both national and European level are very useful for Incident Response stakeholders. Such initiatives help IR stakeholders to foster CSIRT development in both the Energy and Air Transport sectors.

Stakeholders who participated in the survey pointed to several successful initiatives such as:

- the CEF programme,
- ENISA guidelines,
- the CSIRTs Network,
- EU ISACs,
- National CSIRTs tools,
- Regulators and European Sectoral CSIRTs Guidelines, etc.

According to a National CSIRT, its ultimate objective is for sectoral operators "*to be autonomous in incident response*". As a result, it focuses on anticipation and prevention on the one hand and building resilience of its constituency on the other, by training personnel, providing robust tools and certifying DSPs. This goal is shared by several National and Sectoral CSIRTs all keen to foster their effort to support capacity-building at sectoral level.

A number of these initiatives are public, and therefore highly dependent on public budgets, whether national or European. The ongoing COVID-19 pandemic and the dramatic economic crisis in its wake massively impact public budgets and the resources available for such initiatives.

The Air Transport sector continues to suffer from the impact of the pandemic, with air traffic drastically reduced and offices closing all over the world. Contingency planning does not always feature cybersecurity to the extent it should, increasing the threat to millions working remotely, using less secure networks and thus increasing their exposure to cyber threats.

For many Air Transport and Energy sectoral operators, the pandemic has led to temporary and permanent job and wage cuts and staff reallocation. This in turn challenges the upkeep of organisations' security cultures and incident response capabilities. Even if they are critical, cybersecurity teams have also suffered from job cuts and tense environments. This could have severe consequences on cybersecurity in the long run, making the strengthening of IR capabilities even more important than ever.

Several measures could be taken by European institutions to keep up their ongoing efforts[35] to enhance Sectoral IR capacity-building:

- Measures to foster cross-sector and cross-border cooperation for incident management;
- IR sector-specific knowledge for public stakeholders as they face competition with the private sector;
- Additional guidelines and reviews on new tools and equipment to assist IR teams in selecting appropriate IR tools;

[35] For example Connecting Europe Facility https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

- More training and drills.

→ **Summary** No-one doubts that the support provided by European institutions and professional associations is beneficial to the whole sectoral IR community in a particularly tense context fuelled by the COVID-19 pandemic.

4. RECOMMENDATIONS

This study is intended as a snapshot of the current situation. The data collected indicates that it is still too soon to formulate sector specific recommendations. As a result, the following recommendations are general rather than sector specific.

R#1_Capabilites:
Sectoral actors should encourage the sharing of lessons learnt on the use of open-access or commercial tools, especially those automated within their sector to better benefit from each other's experience and accelerate the maturation of newly created IR entities.

R#2_Regulations:
Sectoral actors should continue to identify overlaps, systematically raise awareness of challenges in cybersecurity regulations[36] and cooperate with policy makers to address these issues by being involved in their revision processes.

R#3_Collaboration:
Sectoral actors should continue their efforts to make use of existing reporting schemes such as NISD repostign and build trusted sectoral communities of users[37] where they could securely exchange both ex-ante and ex-post incident information leveraging existing tools and automated solutions.

[36] For example information on Electricity network codes and guidelines https://ec.europa.eu/energy/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes_en?redir=1
[37] For example Empowering Information Sharing Analysis Centres https://www.isacs.eu/

5. BIBLIOGRAPHY

Avionics International, Will today's cybersecurity guidelines and standards become mandates for connected aircraft systems? April 2020

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

ECSO, Energy network and smart grids. Cyber security for the energy sector, European Cyber Security Organisation, November 2018

ECSO, Transportation sector report - Cyber security for road, rail, air, and sea, European Cyber Security Organisation, March 2020

ECSP, Strategy for Cybersecurity in Aviation, European Strategic Coordination Platform, September 2019

EECSP, Cyber Security in the Energy Sector. Recommendations for the European Commission, Energy Expert Cyber Security Platform, February 2017

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

ENISA, Power sector dependency on time service, European Union Agency for Network and Information Security, April 2020

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

IATA, Aviation Cyber Security Toolkit, Kossena, M., Cyber security in air transportation, May 2019

KPMG, Complying with the European NIS Directive. Cybersecurity for critical infrastructures, KPMG, April 2019

Norton, R. F., Cybersecurity law in the aviation sector, August 2019

PA Consulting, Overcome the silent threat - building cyber resilience in airports,

WEBSITES AND ONLINE PUBLICATIONS:

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

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

CSIRTs Network, ENISA online directory
Available: https://csirtsnetwork.eu

EASA, “Krakow Declaration”, November 2016, [Online]
Available: https://www.easa.europa.eu/sites/default/files/dfu/DECLARATION-Krakow-Cybersecurity.pdf

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

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”, 2020. [Online].
Available: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

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

IATA, Aviation Cyber Security Toolkit
Available: https://www.iata.org/en/publications/store/aviation-cyber-security-toolkit/

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

MISP Threat Sharing, “Features of MISP, the open source threat sharing platform”, Date[38] [Online].
Available: https://www.misp-project.org/features.html

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

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

[38] At the time of writing of this report

A ANNEX: PRESENTATION OF THE RAW DATA

DESKTOP RESEARCH – SECTORAL IR SET-UP

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

Data structuring and classification criteria

The raw data gathered during the study was consolidated in an Excel table. It was first organised by Member States.

In addition to Member State classification, it was decided tthat the the scope of the research would be extended to sectoral IR Capabilities in non-EU countries to provide insight into approaches of neighbouring countries, namely Albania, Bosnia-Herzegovina, Georgia, Iceland, Kosovo, Moldova, Montenegro, North Macedonia, Norway, Ukraine, the United Kingdom, Serbia and Switzerland.

For each country, the following information was initially provided (where available):

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

Then, the list of existing and newly created CSIRT and IR entities was extracted to build a separate consolidated table.

For each entity, the following information was provided (where available):

- **CSIRT/IR entity name**
- **Sector (energy /air transport / cross-sector national CSIRT)**
- **Country**

- **Type (public/private)**
- **Description & mandate**
- **Status (existing / to be created)**
- **Cooperation set-up & processes**
  - Cross-border IR aspects.
- **Development of capabilities and other initiatives**
  - Operational Preparedness and capacities;
  - Tools;
  - Initiatives, communities, etc.

OVERVIEW OF THE SECTORAL IR SET-UP IN THE 27 MEMBER STATES AND A SELECTION OF NON-EU COUNTRIES

Desktop research – key figures

Table 9: Desktop research – Data collection overview

Nature of information collected	Data collection
Summary of national approach toward IR in the NISD sectors	Identified in 14 MS and 8 non-EU countries
Competent authorities for the two targeted sectors	Identified for the 27 MS and 10 non-EU countries, partial data for 1 non-EU country
Existing/newly created or planned CSIRT or IR entities	68 existing/newly created identified 2 planned identified
Role of OES	Identified for 24 MS
Role of DSP	Identified for 22 MS
Cross-border IR aspects	Minimal data in 5 MS and 4 non-EU countries
Operational preparedness and capacities	Minimal data for 5 MS and 10 non-EU countries
Tools	Minimal data for 2 MS and 1 non-EU country
Initiatives, communities, etc.	Minimal data for 9 MS and for 9 non-EU countries

SURVEY AND INTERVIEWS – IR APPROACH AND SECTORAL CAPABILITIES

The objective of the survey and of the complementary interviews was to bridge information gaps in the desktop research and gain deeper insight into IR set-up in the 27 Member States.

These activities also focused on the recent changes and evolutions of Sectoral IRC. They were designed to also improve the knowledge on sectoral CSIRTs processes, procedures and tools following the publication of the NIS Directive.

SURVEY - DATA STRUCTURING AND CLASSIFICATION CRITERIA

The raw data gathered from the survey was consolidated in an Excel table.

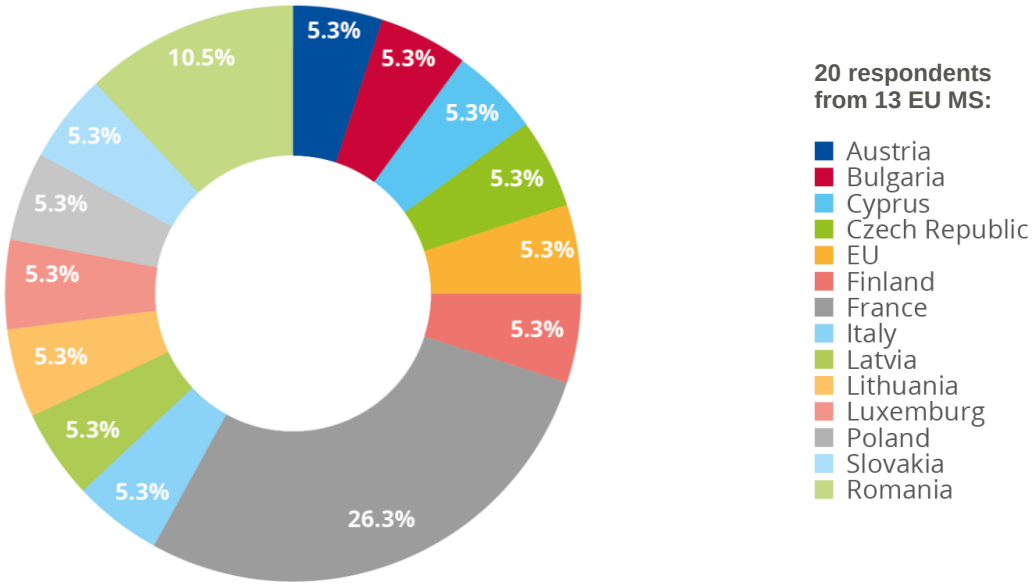
The table was structured around the answers of each respondent according to the questions of the survey (see B Annex Survey – questionnaire (p. 48)).

OVERVIEW OF THE SECTORAL IR SET-UP IN THE 27 EU MEMBER STATES

Survey - Key figures

The data collection relies on **20 responses from 13 EU Member States**. It also includes the answer from an Air Transport organisation very active in the areaof cybersecurity and IR at EU level.

Figure 9: Respondents by countries



Half of respondents were **national CSIRTs** with IR teams ranging **from 2 to 25 people** (full-time equivalents)**.**

Figure 10: Respondents by entity

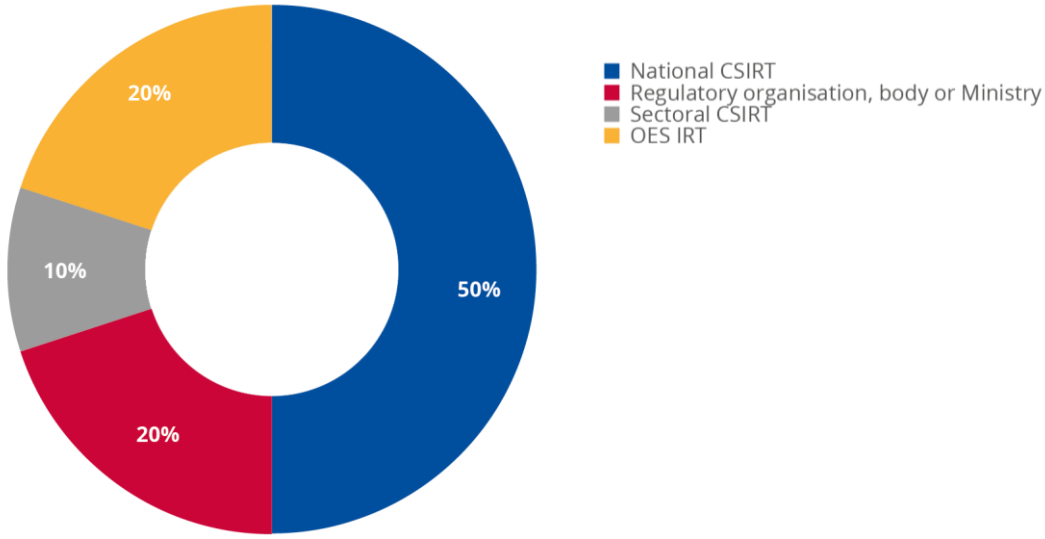
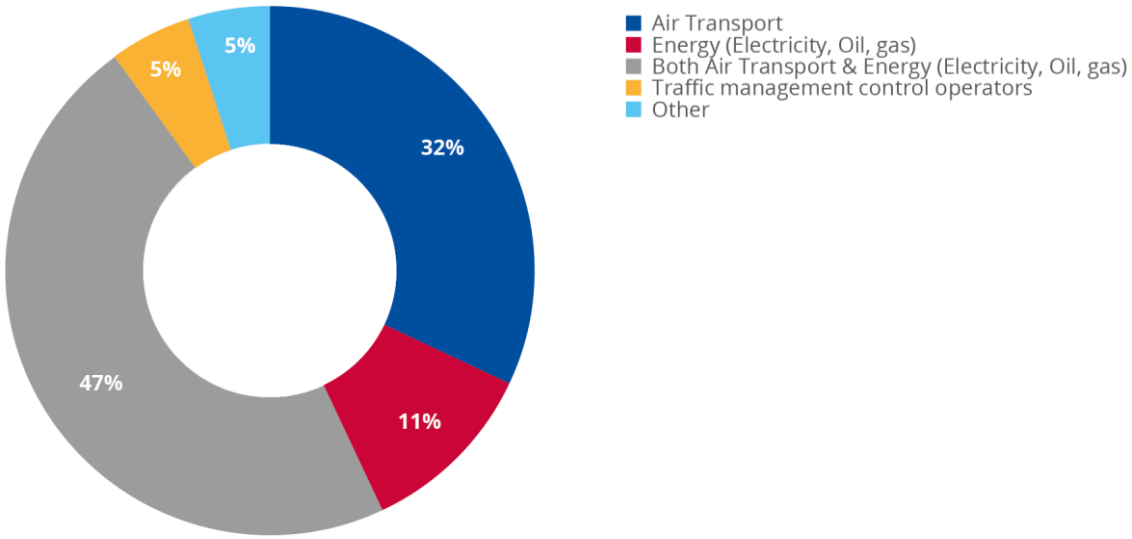


Figure 11: Respondents by sectors



COMPLEMENTARY INTERVIEWS – RATIONALE AND KEY FIGURES

The main objective of the interviews was to collect additional information and insights into IR set-up, along with qualitative assessments of recent changes and considering the impact of the NISD. After reviewing initial survey results, complementary interviews took placewith:

- Sectoral cybersecurity experts;
- Members of the Informal Expert Group on Incident response Capabilities.

B ANNEX: SURVEY – QUESTIONNAIRE

ABOUT YOUR ORGANISATION

Name: ……

Incident Response Team Full Time Employees: ……

- **What type of organisation are you?**

☐ National CSIRT

☐ Government or Military CSIRT

☐ Regulatory organisation, body or Ministry

☐ Sectoral CSIRT

☐ OES Incident Response Team

- **Please select relevant sector or sub-sector**

☐ Energy

☐ Electricity

☐ Oil

☐ Gas

☐ Air Transport

☐ Air carriers

☐ Airport managing bodies

☐ Traffic management control operators

☐ Other. Please specify: ……

Comments

1. **What are the services and associated functions provided by the sectoral CSIRTs or sector-specific IR capabilities in your sector[39]?**

Service Area 1 – Information security event management

☐ Monitoring and detection

- Log and sensor management
- Detection use case management
- Contextual data management

☐ Event analysis

- Correlation
- Qualification

Service Area 2 - Information security incident management

☐ Information security incident report acceptance

- Information security incident report receipt
- Information security incident triage and processing

☐ Information security incident analysis

- Information security incident triage
- Information collection
- Detailed analysis coordination
- Information security incident root cause analysis
- Cross-incident correlation

☐ Artifact and forensic evidence analysis

- Media or surface analysis
- Reverse engineering
- Run Time or dynamic analysis
- Comparative analysis

☐ Mitigation and recovery

- Response plan established
- Ad-hoc measures and containment
- System restoration
- Other information security entities support

☐ Information security incident coordination

- Communication
- Notification distribution
- Relevant information distribution
- Activities coordination
- Reporting
- Media communication

☐ Crisis management support

- Information distribution to constituents
- Information security status reporting
- Strategic decisions communication

Service Area 3 - Vulnerability management

☐ Vulnerability discovery / research

- IR vulnerability discovery
- Public source vulnerability discovery
- Vulnerability research

☐ Vulnerability report intake

- Vulnerability report receipt
- Vulnerability report triage & processing

☐ Vulnerability analysis

- Vulnerability triage
- Vulnerability root cause analysis
- Vulnerability remediation development

☐ Vulnerability coordination

- Vulnerability notification/reporting
- Vulnerability stakeholder coordination

☐ Vulnerability disclosure

- Vulnerability disclosure policy & infrastructure maintenance
- Vulnerability announcement / communication
- Post-vulnerability disclosure feedback

☐ Vulnerability response

- Vulnerability detection/scanning
- Vulnerability remediation

Service area 4 – Situational awereness

☐ Data acquisition

- Policy aggregation, distillation, and guidance
- Asset mapping to functions, roles, actions and key risks
- Collection
- Data processing and preparation

☐ Analysis and synthesis

- Projection and inference
- Event detection
- Information security incident management decision support
- Situational impact

[39] See the FIRST CSIRT framework for details: https://www.first.org/education/csirt_service-framework_v1.1

☐ Communication

- Internal and external communication
- Reporting and recommendations
- Implementation
- Dissemination / integration / information sharing
- Management of information sharing
- Feedback

Service area 5 – Knowledge transfer

☐ Awareness building

- Research & information aggregation
- Reports and awareness materials developed
- Information dissemination
- Outreach

☐ Training & Education

- Knowledge, skill, and ability requirements gathering
- Educational and training materials development
- Content delivery
- Mentoring
- CSIRT staff professional development

☐ Exercises

- Requirements analysis
- Format and environment development
- Scenario development
- Exercise execution
- Exercise outcome review

☐ Technical and policy advisory

- Risk management support
- Business continuity and disaster recovery planning support
- Policy support
- Technical advice

Comments

1. CREATION OF SECTORAL CSIRT/IR CAPABILITIES

2. Which of the following sectors have (or will have) a dedicated CSIRT in your country? If yes, please specify in the comment box for each sector if the CSIRT status : exists, under creation, creation process is to be launched in 2020 or 2021, plans in the coming years, no plans yet.

☐ Energy

☐ Electricity

☐ Oil

☐ Gas

☐ Air Transport

☐ Other. Please specify: **Comments (please specify if the CSIRT is/are listed, accredited, certified.**

3. What are the key drivers to create such sector specific IR capacities?

☐ The implementation of the NIS Directive

☐ The lack of sector-specific knowledge or capacity of the National CSIRT

☐ Lessons learnt from past incidents

☐ The difficulties in managing the cybersecurity incidents in the NISD sectors

☐ The complexity of managing the high number of OES in some of the NISD sectors

☐ The need to facilitate incident handling cross-borders

☐ Other. Please: specify:
……

4. In your opinion, what are the additional and/or new services, roles or functions of the sectoral CSIRTs in contrast to those supplied but the national, governmental or military CSIRT?

Comments

5. In your opinion, what are the specific services, roles or functions of the sectoral CSIRTs in contrast to those supplied but the national, governmental or military CSIRT?

Comments

6. Based on your experience, what are the key factors facilitating the development of sectoral CSIRTs and/or IR capacities?

☐ The lessons learnt from past incidents

☐ The establishment of sector-specific regulations clarifying the security requirements and responsibilities

☐ Recommendations from a previous audit and certification programmes

☐ Requests from stakeholders or participating organisations/future members

☐ The establishment of cooperation agreements between national and sectoral actors

☐ Access to funding and support of IR capability development through the Connecting European Facility (CEF) programme or other fundings

☐ The establishment of public-private partnerships. Please specify the nature of these PPPs:
……

☐ The dissemination of threat intelligence, exchange of good practices and lessons learnt

☐ Other. Please specify:
……

Comments

7. What specific resources and tools are in place to support the development of constituents' incident response capabilities (IRC) in your sector?

☐ Appointment of local or sectoral counsellors advising OES on the development of their IRC

☐ Training and Education activities

☐ A network of IR actors at a national or sectoral level to exchange good practices about information exchange, capabilities, cooperation etc.

☐ Methodological baselines and tools to support IR (e.g.: specific software tools, risk assessment methodologies, best practices, frameworks)

☐ Shared framework for incident classification and threat modelling

☐ Certification by cybersecurity companies providing reliable services and products

☐ Other. Please specify

Comments

8. **Do you need / have you asked or looked for any specific support or guidance from external stakeholders to design and implement sectoral IR capacities?**

☐ Yes ☐ No

If yes, please specify from who:

☐ European Union entities ☐ Professional associations or industry players

☐ International authorities ☐ CSIRT communities/peers

☐ National authorities ☐ Other

Comments

9. **Do you use to a specific CSIRT maturity assessment methodology to support the development of IR capabilities within your sector(s)?**

☐ Yes ☐ No

10. **If yes, which one?**

☐ SIM3 (Security Incident Management Maturity Model)[40]

☐ ENISA CSIRT maturity assessment[41]

☐ Your national CSIRT maturity tool

☐ A CSIRT maturity assessment methodology from the private sector (please specify in comments)

☐ Other (please specify in comments)

Comments

[40] https://opencsirt.org/csirt-maturity/sim3-and-references/
[41] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

11. IR CAPABILITY DEVELOPMENT IN THE SECTORS

12. Which specific tools[42] does your organisation rely on to conduct the following services?

Service area and Services	Tools status: *Tool in service/ planning to implement one/out of scope or perimeter*	Tools used & supporting procedures/SOPs/ Playbooks
Service Area 1 – Information security event Management **Monitoring and detection** **Event analysis**		
Service Area 2 - Information security incident management **Information security incident report acceptance** **Information security incident analysis** **Artifact and forensic evidence analysis** **Mitigation and recovery** **Information security incident coordination** **Crisis management support**		
Service Area 3 - Vulnerability management **Vulnerability discovery / research** **Vulnerability report intake** **Vulnerability analysis** **Vulnerability coordination** **Vulnerability disclosure** **Vulnerability response**		
Service area 4 – Situational awareness **Data acquisition** **Analysis and synthesis** **Communication**		
Service area 5 – Knowledge transfer **Awareness building** **Training & Education** **Exercises** **Technical and policy advisory**		

13. Do you have standard operating procedures (SOPs) that OES' teams should follow in case of incident?

☐ Yes ☐ No

If yes, please detail for which services or functions?

[42] Example: Cyber Threat Intelligence system, Request tracker for Incident Response (RTIR), or equivalent, Open Technology Real Services, or equivalent, osTicket, or equivalent, dedicated alerting & reporting dedicated portal, Active & passive monitoring tools, Use of public, semi-public or commercial feed, Digital forensic tools, Security assessment tools)

14. Do you use an incident notification template?

☐ Yes ☐ No

If Yes, who has (or will have) access to the notification template? constituents, participating organizations, LEA, third-party organizations, CSIRT peers? ……

If yes, please indicate the nature of the information reported.

☐ Description of the incident and IOCs and TTPs ☐ Root cause

☐ Services affected ☐ Severity

☐ Cross border impact ☐ Lessons learnt

☐ Indicators to measure the nature and impact in addition to those of the NISD.

☐ Current situation of the incident (actions taken or needed, investigation status etc.)

☐ Other……

Comments

15. Do you have specific information exchange tools to enable the notification of incidents?

☐ Secure emails (e.g. PGP encrypted) ☐ MISP standard formats and technologies

☐ A special government secured network ☐ via an ISAC (Information Sharing and Analysis Center)

☐ Other. Please specify: ……

16. How do you ensure the uptake of these tools and procedures by constituents?

☐ Obligation stipulated in legislature ☐ Code of conduct

☐ Promotion by national CSIRT ☐ Post-attack measures implemented by national CSIRT

☐ Other (specify below)

Comments

17. IR COOPERATION AND OPERATIONAL MODELS WITHIN THE SECTORS

Cooperation with OES/Critical Infrastructure (in particular from the private sector)

18. In case of incident, do you have:

☐ **Specific cooperation agreements between the national cybersecurity authorities and the IR teams of OES (in particular for private companies)**

☐ **Specific consultation process involving OES' incident response capabilities (in particular for private companies)?**

☐ **Specific process allowing OES to request operational assistance from the national, governmental or military CSIRT**

☐ **Specific process to share lessons learnt among national and sectoral CSIRT after a crisis (e.g.: after incident standard report, meetings etc.)**

Comments

19. What are the main challenges faced when collaborating with OES in the energy/air transport sectors?

☐ Confidentiality issues
☐ Cross-border issues
☐ Commercial issues
☐ Regulatory issues
☐ GDPR-related issues
☐ Resources or expertise issues
☐ No 24/7 coverage / capabilities
☐ Supply chain management
☐ Lack of security culture among OES
☐ The management (and the security) of OES IT infrastructure is often outsourced
☐ Lack of established cooperation tools and channels with OES IR teams
☐ Cross-sector interdependencies and cooperation
☐ Other. Please specify: ……

Comments

Incident response in cross-border crisis situations

20. Do you have specific procedures to address cross-border incidents within the sectors?

☐ Yes, we have such procedures at a national level
☐ Yes, we have such procedures at a sectoral level
☐ Yes, indirect (through a trusted third-party Point-of-Contact such as governmental CSIRT, LEA...)
☐ No, but these are planned to be implemented
☐ No, it is not plan at the moment

Comments

21. What is the nature of these procedures?

☐ Bilateral agreement with the other MS.

☐ Designation of a Point of Contact at national or sectoral level to facilitate cross-border cooperation in case of incident

☐ Participation of representative of the other country in the crisis response process

☐ Organisation of cross-border exercises

☐ Information sharing platform (existing or about to be implemented)

☐ Other. Please specify: ……

22. Do you have specific measures in place to inform the relevant actors (national authorities and OES) in neighbouring countries about an incident that may impact them?

☐ Yes, direct

☐ Yes, indirect (through a PoC, a trusted third-party...)

☐ No, but it is planned to establish some

☐ No, it is not planned at the moment

If yes, please specify

23. What main barriers or difficulties do you face when developing cooperation procedures between national and sectoral IR actors?

☐ Identifying and involving the relevant stakeholders

☐ The cross-border nature of the services, sectors and companies at stake

☐ Exchanging technical information about incident and risks

☐ Addressing the commercial issues of asking competitors to collaborate and share information about incidents affecting their business

☐ Common terminology, standards and formats

☐ Legal issues related to the nature of the information exchanged and different legislation (from one sector to another and/or from one country to another)

☐ GDPR-related issues

☐ LEA-related issues

☐ No 24/7 coverage / capabilities

☐ Other. Please specify:
……

24. GDPR COMPLIANCE AND DATA BREACH MANAGEMENT

25. **Do you have, in your team, an appointed "privacy champion"? If yes, can you detail his/her functions and tasks (full time/partial time, exclusively/partially dedicated to privacy, …?**

Comments

26. **Did you receive awareness training in GDPR? If yes, can you describe the training policy: frequency, percentage of the team been trained, refresh, … If not, where can you receive guidance related to GDPR matters?**

Comments

27. **Does your Incident Response Policy specify how to identify a Data Breach, as defined by the GDPR (articles 33 & 34)?**

Comments

28. **Does your Incident Response Management Process indicates the information of the DPO, or any other person or institution in charge of the privacy/GDPR compliance concerns?**

Comments

29. **Do you have a forensics manual or guidelines to handle evidence related to a Personal Data Breach?**

Comments

30. LESSONS LEARNT AND RECOMMENDATIONS

31. **Do you use groups/forum to exchange with peers IR information, good practices and experience in your sector with peer?**

☐ Yes ☐ No

If yes, please specify

32. **What possible measures undertaken by European Union entities, ENISA, international or national authorities or bodies, or private body in a specific sector would help improve the effectiveness of sector IR capacities?**

Comments

33. **What specific tools or processes in place in your organisation would help improve the effectiveness of sector IR capacities?**

Comments

34. **Do you have any other inputs about your work / the IR capacities within the NISD sectors in your country you would like to share with us?**

Comments

END OF QUESTIONNAIRE

C ANNEX: FIGURES AND TABLES

LIST OF FIGURES

LIST OF TABLES

TP-03-20-822-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit 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 978-92-9204-444-2
DOI 10.2824/123795