INTERNATIONAL
HELLENIC
UNIVERSITY

The Directive on security of network and information systems (NIS Directive) from a practical view – Challenges for the Aviation Industry

Nikolopoulou Antonia

SID: 3307160008

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communication and Cybersecurity

DECEMBER 2018

THESSALONIKI – GREECE

The Directive on security of network and information systems (NIS Directive) from a practical view – Challenges for the Aviation Industry

Nikolopoulou Antonia

SID: 3307160008

Supervisor:	Prof. Komninos Komnios
Supervising Committee Members:	Assoc. Prof. Marios Gatzianas Assist. Prof. Aggeliki Tsohou

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

DECEMBER 2018

THESSALONIKI – GREECE

Abstract

This dissertation was written as part of the MSc in Communications and Cybersecurity at the International Hellenic University.
More specifically, this paper critically examines the implementation of Network and Information Systems Directive (NISD) by the identified operators of essential services (OESs) of the Critical Infrastructure (CI) sectors (public and private) and certain digital service providers (DSPs) for all Members in the European Union.

To introduce the unfamiliar reader to cybersecurity conception, this thesis provides an analytic description of the general provisions of the NISD alongside the proposed security measures for all Member States.

Following, it examines the way Greece has transposed the context of the directive into national laws and analyzes in detail its effectiveness, providing some conclusions about it.

Subsequently, the thesis tries to reach some general conclusions about the context of the NISD, by understanding its significance since it must be regarded as a national priority among Member States.

Finally, this paper studies the implementation of the NISD into Greek aviation industry making a recommendation for the air transport sector to set up an aviation cybersecurity strategy.

It is also worth stating that the findings for this thesis were drawn from the literature, and empirical studies in Cybersecurity area.

My deepest thanks and gratitude go to my respected supervisor Asst. Prof. Dr. Komninos G. Komnios. His patient and gentle guidance alongside the encouragement and advice has contributed immensely towards the fulfillment of this thesis by helping me to overcome my concerns and see new, interesting aspects of this work in my working environment.

Besides my supervisor, I would like to thank my friends, especially Mary, for their encouragement and colleagues for the provision of significant information and assistance. Special thanks go to my dearest Yvonne for her continuous assistance to my family and my fellow lab mates Jakob and Stefanos for working together in the last two years and teaching me how constructive the collaboration and coordination can eventually become.

Finally, I must express my very profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study. I am deeply grateful to my mother for standing by my family’s needs at least for the last two years and to my little princesses, Fotini and Smaragda, for their unconditional love and understanding, particularly during the writing process of the dissertation.

This accomplishment would not have been possible without all of you. Thank you!

Keywords: information, networks, cybersecurity, threats, risk management.

Nikolopoulou Antonia

Date 12/12/2018

Contents

1 Cybersecurity in Europe

1.1 Introduction

In modern times, everyday human activities include the extended use of a networked computer environment, creating “virtual communities" with no social, territory and cultural borders, by providing them with a two-way direct communication, and making them feel more and more as a global citizen.

Terms such as ‘information’, ‘cyber’ and ‘digital’ are commonly used in everyday discussions[1], creating new vocabulary such as ‘information system’, ‘cyberspace’, ‘cybersecurity’, ‘digital information’, ‘digital market’ etc[2].

Although there is no precise definition of these terms, they have been used extensively in daily routine which signal that we all are citizens of the so-called ‘information age’. According to the literature, the key characteristics of this era[3] are:

1. The widespread use of technology in the economic and social framework activity of individuals and nations;
2. The heavy dependency of the society on this technology.

Indeed, the use of computers is not any more limited to support the operation of the industrial production, e.g. the use of supervisory control and data acquisition (SCADA)[4] solutions in many modern industries, like energy, manufacturing, water transportation, etc. nor to support the business management in general, by providing a group of services such as, project management, support and database services, and other more. Instead of that, the constant development of more advanced ICT[5] products, in combination with their low cost and ease of use, contributes to the establishment of the information revolution phenomenon; the interoperability offered through the “marriage of

[1] In the press, political speeches, popular books, scholarly journals, and everyday conversations.

[2] *Myriam Dunn Cavelty,* Cyber-Security and Threat Politics: US efforts to secure the information age, p. 14, New York 2008

[3] *Myriam Dunn, Sai Felicia Krishna-Hensel and Victor Mauer*, Power and Security in the Information Age, 2007, pp. 19-28.

[4] SCADA systems organize multiple technologies that allows to process, gather and monitor data at the same time to send instructions to those points that transmit data.

[5] Information communication technology.

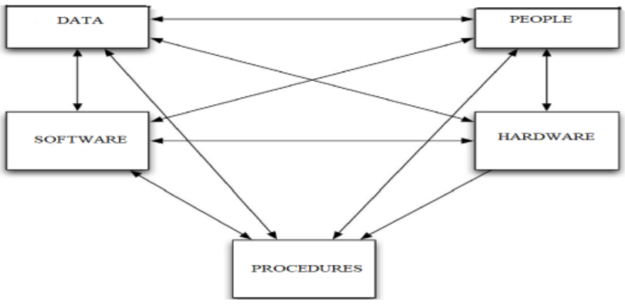
computers, telecommunications and the worldwide assembly of systems[6], has made electronic information widely available"[7] in the provision of the essential everyday services.

1.2 The power of information

Since we live in the digital era the dominant power that features our world is the information; "Where once economies were built on industry and conquest, we are now part of a global information economy"[8].

The term information security includes not only the protection of data that flows through the interconnected information systems but also the physical existence of the information systems components.

An information system (IS) therefore, is a combination of software, hardware utilities and networks created by people. These people use an IS, by following specific procedures, aiming to collect, create, store and distribute useful information resources (data) in an organization[9]. Picture 1 shows the components of an information system.



Picture 1: The components of an information system.

The benefits we may enjoy due to the extended growth of ICT products may also provoke serious concern on the appearance of emerging and sophisticated threats, challenging the proper operation of information systems and therefore the social stability in terms of prosperity and peace within nations.

[6] Databases, and telecommunications networks.

[7] *Myriam Dunn Cavelty,* Cyber-Security and Threat Politics: US efforts to secure the information age, p. 19, New York 2008

[8] Frank Webster, *Theories of the Information Society*, 2006.

[9] *Joseph Valacich, Christoph Schneider,* Information Systems Today: Managing in the Digital World, 2016.

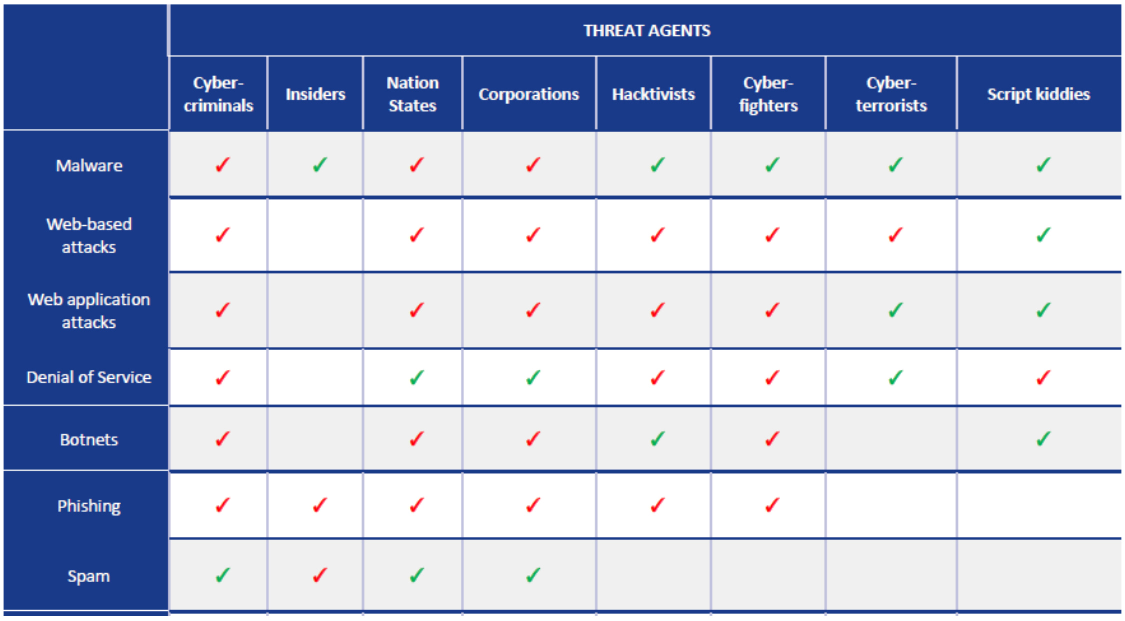
The protection of an information system should concern the adoption of appropriate security measures for each of the above components[10] individually, taking into serious consideration the existing interoperability, due to their interconnected nature.

Each of the components may be vulnerable to a different type of threat[11].

For example, according to a recent study of the European Union Agency for Network and Information Security (ENISA), the new cyber-challenges landscape includes the following top types of threats: malware, phishing, web-based attacks, web-application attacks, spam, Denial-of-Service (DoS), ransomware, botnets, insider threats, physical manipulation/damage/theft/loss, data breaches, identity theft, information leakage, exploit kits and cyber espionage. As we may observe this frequent alternation of the cyber threat landscape entails also the identification of new types of threat agents[12] such as Cyber-criminals, Hacktivists, Cyber-fighters, Cyber-terrorists, script kiddies etc.

Table 1 presents the involvement of the above threat agents in the deployment of the identified top cyber-threats[13].

Table 1: Involvement of threat agents in the top cyber-threats.



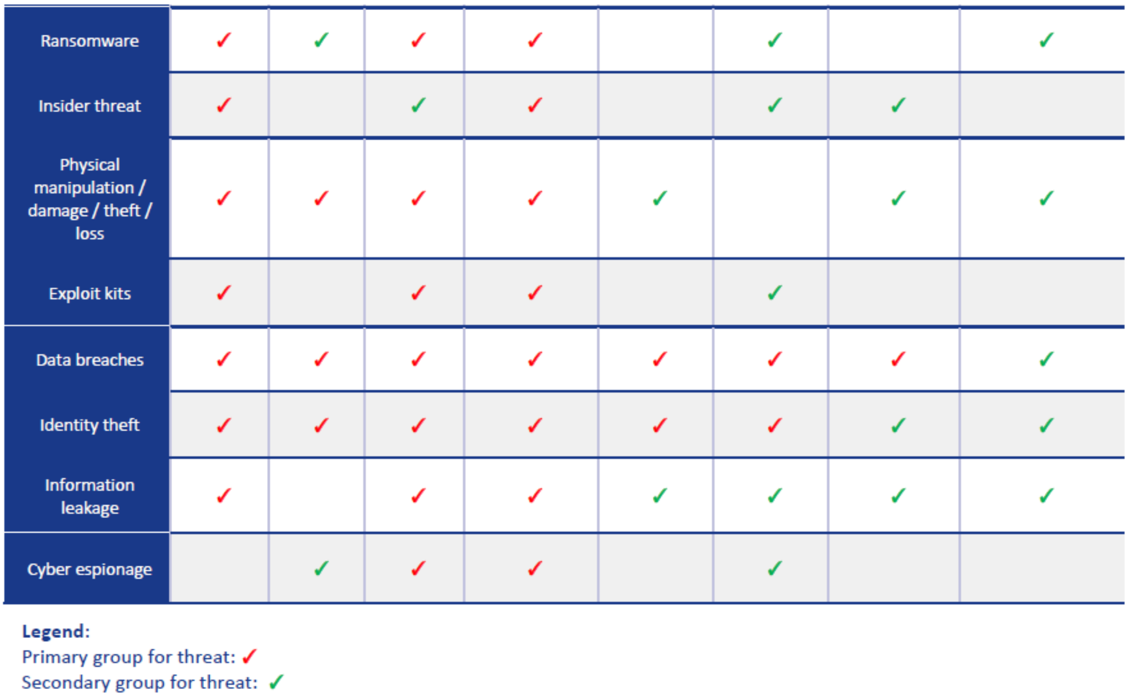
	THREAT AGENTS							
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓		✓
Phishing	✓	✓	✓	✓	✓	✓		
Spam	✓	✓	✓	✓				

[10] Software, hardware, people, networks, data and procedures.

[11] Relative studies have been conducted for providing information about the types of threats, the actors involved, the techniques used for and the frequency the environment changes, testifying the rapid change in the threat landscape in cyberspace.

[12] Malicious actors.

[13] *ENISA*, Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends, p. 98, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017



Ransomware	✔	✓	✔	✔		✓		✓
Insider threat	✔		✓	✔		✓	✓	
Physical manipulation / damage / theft / loss	✔	✔	✔	✔	✓		✓	✓
Exploit kits	✔		✔	✔		✓		
Data breaches	✔	✔	✔	✔	✔	✔	✔	✓
Identity theft	✔	✔	✔	✔	✔	✔	✓	✓
Information leakage	✔		✔	✔	✓	✓	✓	✓
Cyber espionage		✓	✔	✔		✓		

Legend:
Primary group for threat: ✔
Secondary group for threat: ✓

In the past, the traditional network security measures applied for resisting and responding to cyber-attacks, such as firewalls VPNs, INTRANETs, Access control systems etc., were nothing more than a fragmented approach, lacked in flexibility and interoperability. More specifically, the security of an information system was regarded as an IT department's concern for implementing hardware and software security solutions during the implementation process of an installation, but most of the times, after the occurrence of a significant incident.

The implementation for example, of a 'commercial off the shelf' (COT) product, does not anymore seem to be appropriate for every system. On the contrary, the serious concern should be based on determining the regulatory, statutory and policy constraints on business systems before applying them[14].

So, a new conception of information system security requires everybody to take into serious consideration the interdependences and interoperability between various implemented products within different information systems, in order to quickly see any change in the expected systems' operational behaviour.

These changes may be caused either from offensive or defensive activities.

[14] *Michele Motsko, Patricia Oberndorf, Ellen-Jane Pairo, James Smith,* Rules of Thumb for the Use of COTS Products, 2002.

While Offensive activities refer to malicious activities from cyber terrorists and cyberrime area, defensive activities refer to the protection of Critical Information Infrastructure (CII). More specifically to the protection of CII, the interruption of their essential services to the society may not only be caused by physical threats such as natural disasters, but it may also be provoked by malicious human acts of terrorist and criminal activities taking advantages of the existing vulnerabilities of the implemented information systems and networks within the organizations.

Therefore, the insecure communication environment of internet although cannot be easily governed, in terms of addressing effectively criminal activities, it is necessary for a common rule to be established at national level, within the European Union (EU), for addressing all possible threats that may have a negative impact on the security of the EU and the well-being of its citizens.

1.3 The initial cybersecurity approach in Europe

European Union operates as a single European market that meets no borders in facilitating the free movement of persons, goods, services and capitals. However, the heavily dependent activities of people on the internet and the related computer networks, provide them with a borderless flexibility and directness in their daily activities.

This means that European citizens do face offensive activities, that cannot be tackled effectively due to different national legislation.

Although there has been some progress on a national level, the emerging increased level of cyber threats, in combination with the overall societal impact, is not entirely satisfactory, due to:

1. The asymmetry in growth between the changing threat landscape and the advance in the development of ICT products;
2. The differences in building national capabilities for resisting to cybersecurity challenges; and
3. The European fragmented approach on dealing with cybersecurity issues, by establishing a series of legal and regulatory instruments, that overlap rather than adopting an overarching framework[15].

[15] *George Christou*, Cyber security in the European Union: Resilience and Adaptability in Governance Policy, 2016, pp. 119-131.

For example, Germany, in 2015 adopted legislation (IT-Sicherheitsgesetz[16]) for regulating the cybersecurity challenges in German corporations into the telecommunication sector, by defining a minimal set of security measures. Similar actions were taken by France since 2009, that has established the National Network and Information Security Agency (ANSSI) in charge of cybersecurity in the country, and from 2008 till 2013, has already published three high-level policy documents relevant to cyberspace activities[17].

1.3.1 The convention of Cybercrime (Budapest Convention)

In 1997, a group of experts on cybercrime was designated by the Council of Europe, with the objective to create a common criminal policy on fighting cybercrimes, while promoting a strong and progressive international co-operation for the provision of electronic evidence.

More specifically, they were focused on the identification of new threats aiming to define new types of cybercrimes and establishing of jurisdictional rights and criminal liabilities, for enhancing the international cooperation in information sharing processes. The result of this first international treaty, on addressing cyber-crimes through the internet and the use of computer networks, was the Convention of Budapest Treaty No.185, in 2001[18], and constitutes the first binding international instrument on cybercrime.

The main concerns of this treaty were the infringement of intellectual property, the computer-related fraud, child pornography and generally the attacks on computer networks.

In terms of this international agreement, the European Commission (EC), in 2001, issued a Communication on Network and Information Security (NIS)[19], underpinning the significance of Network and Information Systems alongside with its increasing concern on cyber threats. Later, in 2006, the above communication was adopted in the Strategy for a Secure Information Society[20].

[16] Available at: http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

[17] Such as: a) “White Paper on National Defense and Security of 2008”; b) “France’s Cyber Strategy 2011”; and c) “White Paper on National Defense and Security of 2013”.

[18] Also known as the convention on cyber crimes, available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[19] Proposal for A European Policy Approach (COM (2001) final, available at: https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf

[20] A strategy for a Secure Information Society – “Dialogue, partnership and empowerment” COM (2006), available at: http://ec.europa.eu/information_society/doc/com2006251.pdf

Unfortunately, the content of this treaty remained largely a symbolic policy[21] at a global level, with a limited impact on counterfeiting effectively the cybercrime in the long term, because of inconsistencies in terms of laws and resources among different nations[22] [23].

1.3.2 The establishment of ENISA

In the meantime, the awareness of the lack of an institutional body, responsible for developing co-operation, coordination and research in the field of the information security and networks within EU, led to the establishment of ENISA, in 2004. (More about ENISA in paragraph 1.5)

1.3.3 The Critical Information Infrastructure Protection

Subsequently, in 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[24] regarding the continuity of their essential services. The enhanced approach by the Commission was the introduction of framework activities focusing on preventing and responding to cybersecurity risks.

On the 27th of May in 2011, the European Council communicated its conclusions on CIIP highlighting the requirement for ICT systems and networks to develop appropriate and proportionate security measures against all possible disturbances[25].

[21] This term is used for describing the policies that have no actual or significant change rather than making the public feel that something will be done. (Edelman, 1964). *Nancy E. Marion,* The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation, 2010.

[22] *Grabosky Peter*, Electronic Crime. Upper Saddle River, 2007.

[23] Till today 67 States have signed this agreement, together with nine international organizations apart from EU to participate either as members or observers, available at: https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime.

[24] Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009)149, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[25] Many of the recommendations of the Council have been considered in the cyber security strategy published in 2013 and with the proposal for a Directive on network and information security. Council conclusions on Critical Information Infrastructure Protection-Achievements and next steps: towards global cybersecurity, 2011, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybersecurity_/sede150611cccybersecurity_en.pdf

1.3.4 The Digital Agenda for Europe

In 2010, the Commission communicated the digital agenda for Europe[26] explaining how the European citizens and businesses may be benefitted from digital technologies and underpinned the necessity for setting the trust and security as the fundamental precondition, in order to create a digital single market beneficial for all the European businesses.

1.4 The EU recent cybersecurity approach

So far, we may object that the European Commission had selected an approach to ensuring the protection of its citizens while performing online activities. However, from 2013 till today, the Commission enhanced its cybersecurity approach by focusing more on the following key objectives[27]:

i. Increasing cybersecurity capabilities and cooperation;
ii. Making the EU a strong player in cybersecurity;
iii. Mainstreaming cybersecurity in EU policies.

The selection by the EU action plan for strengthening its resilience to cybersecurity risks is simultaneously driven in 5 axes:

1. EU strategies;
2. EU legislation;
3. Networks and organizations[28];
4. EU funding[29]; and,
5. International activities[30].

[26] Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PD

[27] *EC*, EU cyber security initiatives –working towards a more secure online environment, January 2017, p. 2, available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[28] Such as: ENISA, CERT –EU, EC3.

[29] Such as the 7th Framework Programme and The Horizon 2020.

[30] Relative activities performed by the European External Action Service (EEAS) and the Commission in cooperation with Member States.

1.4.1 EU strategies

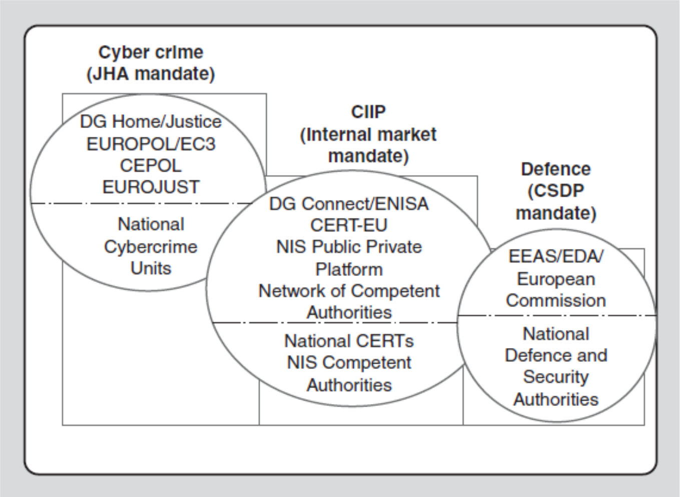
a. The EU cyber security Strategy

In this strategy (in 2013) it is outlined the EU's vision on promoting a secure cyberspace by introducing the appropriate action plan required for deterring the cybercrime[31].

The proposed action plan covers five priorities[32]:

1. The building on a more cyber resilient environment;
2. The extremely reduce of cybercrime;
3. The development of an EU cyber defence policy;
4. The development of industrial and technological resources relative to cyber protection;
5. The establishment of a coherent international cyberspace policy within the EU and promote core EU values.

In picture 2 are illustrated the central pillars of the EU Cybersecurity Strategy.



Picture 2: The central pillars of the EU Cybersecurity Strategy[33].

[31] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1.

[32] *EC*, EU cyber security initiatives –working towards a more secure online environment, January 2017, p. 2.

[33] *Christou George*, Cyber security in the European Union: Resilience and Adaptability in Governance Policy, p. 3, 2016.

b. European Agenda on Security (2015)

This strategy sets the fighting of the cybercrime as a priority, for the period 2015-2020, by proposing specific actions on reviewing the existing framework[34].

1.4.2 EC Communications

Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[35] (2016)

This communication includes measures for:

- Improving cooperation within Europe, by encouraging the Member States to adopt the cooperation mechanisms underlined by the NIS Directive for being capable of handling large-scale cyber incidents;
- Supporting for creating a certification scheme for the security of the ICT products and services in the EU; and,
- Establishing a contractual public-private partnership (PPP) with industry, to promote cybersecurity industrial sharing experience and innovation in the EU.

1.4.3 The need for a common EU Legislation

The EU realizing that different legislation approaches taken by countries, for handling the cybersecurity challenges harden their effective handling at international level, adopted a series of relevant Directives for achieving an EU coherent approach, such as:

- In 2013 – The Directive 2013/40/EU[36] for attacks against information systems, replacing the Council Framework Decision 2005/222/JHA.
- In 2014 – The Directive 2014/65/EU[37] on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[34] Replaces the previous Internal Security Strategy: The European Agenda on Security COM (2015)185 (2010-2014), and Prioritizes terrorism, organized crime and cybercrime as interlinked areas with a strong cross-border dimension. Available at https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

[35] Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry COM (2016) 410.

[36] The Directive 2013/40/EU, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

[37] The Directive 2014/65/EU, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014L0065.

- In 2015– The Directive (EU)2015/2366[38] on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- In 2016 – the General Data Protection Regulation (GDPR)[39] replacing the Data Protection Directive 95/46/EC.
- In 2016 – The NIS Directive[40] concerning measures for a high common level of security of network and information systems across the Union

1.4.4 NETWORKS / ORGANISATIONS

In order to achieve a better coordination between different Member States in the handling of significant cyber-related incidents with facing no border limits, the EU parliament decided on establishing apart from ENISA additional key agencies, such as:

- EU Computer Emergency Response Team[41] (CERT-EU): a group of security experts was created in 2012 with the responsibility to share information between EU institutions, agencies and bodies for responding to security incidents and cyber threats.
- Europol’s Cybercrime Centre[42] (EC3): it was set up in 2013 serving as a focal point in fighting and handling any cybercrimes with cross-border implications.

[38] The Directive (EU)2015/2366, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015L2366.

[39] GDPR, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[40] The NIS Directive, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[41] CERT-EU, available at: https://cert.europa.eu/cert/plainedition/en/cert_about.html

[42] EC3, available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

1.5 ENISA and NIS Directive

ENISA is the European Union Agency for network and information systems security, the named centre of network and information systems experts for the Member States, the private sector and the citizens in European Union, with a shared vision of providing networks and information systems security on a high common level.

1.5.1 Background and objectives

The European Network and Information Systems Agency were originally founded by the European Parliament and the Council on 10/3/2004 in accordance with the Regulation (EC) No 460/2004, to function as a point of contact of information exchange between stakeholders enhancing the cooperation in parallel. In the meantime, its mandate has been extended[43] two times (Regulation (EC) No 1007/2008 on 24/09/2008 and Regulation 580/2011, on 8/6/2011) establishing the European Network and Information Systems Agency as regards its duration and reviewed once with the latest changes implemented with Regulation (EU) No 526/2013[44] which contains the valid provisions of ENISA. Recently, its role has been upgraded recently, under the Digital Agenda 2020 for Europe 2020, "Trust and Security"[45]. The Agency is located in Greece with the administrative seat in Heraklion on Crete and the core operations in Athens.

ENISA’s action framework aims mainly to prevent cyber-attacks from network and information systems and in a case where it does happen, to respond and finally address them in an effective and without undue delayed manner.

According to its strategy,[46] five areas of activities are identified:

[43] EC, *Evaluation in the Commission Reporting on Results Annual Evaluation Review 2006 Conclusions and findings from evaluations in the Commission*, 2006, page 150. This is the first evaluation of ENISA) reported that the operational staff was probably below the critical mass needed for effectiveness. The Commission included in its 2007 proposal for review of the telecoms packages a plan to establish a new European authority (European Electronic Communication Market Authority (EECMA)) to serve as its main advisor on all European regulatory affairs by taking over ENISA’s functions. However, this proposal was rejected by both the Council and Parliament. In 2008, the Council and Parliament adopted the Commission’s proposal to extend ENISA’s mandate for another 3 years (until 2012) without any changes to its tasks or set-up

[44] The new mandate was extended for a period of seven years, until 2020.

[45] COM (2018) 630, 2018/0328 (COD): The Commission conducted an evaluation of the Agency by 20 June, 2018 and proposed to modify its mandate into a permanent EU agency for cyber security. In September 13, 2018, negotiations started within the EU to reach a final agreement on the EU Cyber security Act.

[46] ENISA strategy 2016–2020 - Europa EU, available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy.

- Expertise: Developing and maintaining a high level of experts;
- Policy: Assisting in developing policies necessary to meet the legal and regulatory requirements;
- Capacity: Assisting in enhancing capacity building;
- Community: Enhancing cooperation (e.g. support to the Computer Emergency Response Teams (CERTs), coordination of pan-European cyber exercises);
- Enabling: promoting the engagement with the stakeholders and international relations.

1.5.2 ENISA's Tasks

Although most of the tasks performed by ENISA are new, there are also cases that the tasks were passed on from other institutions:" half of its tasks have been taken over from the Commission, the other half coming from the Member States. However, this is a matter of definition. Some analysis work in the area of network security was carried out before, both in the Commission and in various organizations, but overall there was no comprehensive approach at EU level or Member State level to this area, before ENISA"[47].

The main tasks of ENISA in accordance with the Regulation are:

- ✓ Advising and assisting the Commission and the Member States on information security.
- ✓ Advising and assisting the Commission and the Member States in their dialogue with industry to address security-related problems in hardware and software products.
- ✓ Collecting and analyzing data on security incidents in Europe and emerging risks.
- ✓ Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- ✓ Raising awareness and strengthening co-operation between different actors in the information security field, notably by developing public/private partnerships with industry in this field;

[47] RAMBOL, *Evaluation of the EU decentralized agencies in 2009*, Final Report Volume III, Agency level findings (2009).

- ✓ Supporting the development of cybersecurity exercises in Europe and the involved stakeholders in cyber exercises in Europe[48].

1.5.3 Recent activities of ENISA

One of the key objectives of ENISA is to support the less advanced Member States on building their capabilities and capacities relative to the protection of Critical Infrastructures, into one acceptable level of security. For that purpose, ENISA has issued recommendations and guides on best practice, such as[49]:

- ➢ Methodologies for the identification of Critical Information Infrastructure assets and services[50];
- ➢ Technical Guidelines for the implementation of minimum security measures for Digital Service Providers;
- ➢ Critical Information Infrastructures Protection (2015);
- ➢ Guides on the formulation of national cybersecurity strategies: "NCSS best practice guide" (2016);
- ➢ Technical Guideline on Security Measures (ENISA 2013);
- ➢ Cloud Computing Risk Assessment (2009);
- ➢ Guideline on Threats and Assets (2015).

Additionally, ENISA has issued Guidance and recommendations on the industrial ICT control systems, such as:

- ➢ Protecting Industrial Control Systems (2011);
- ➢ Good practice guide for CERTs in the area of Industrial Control Systems (2012).

ENISA also supports:

- ➢ "The European Public-Private Partnership for Resilience", EP3R 2010-2013 which was launched for enhancing cooperation between the public and private sectors on strategic security issues;

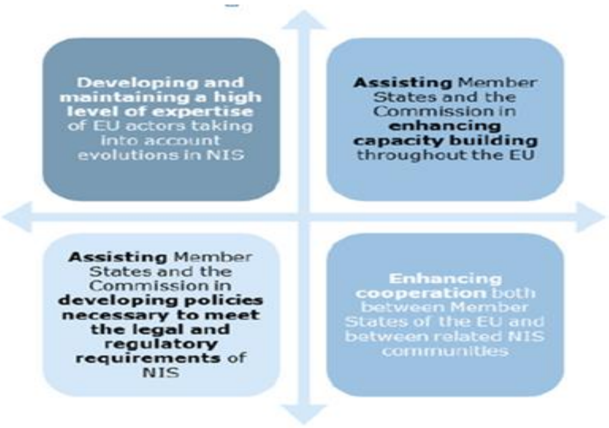
[48] ENISA Cyber exercises platform, available at: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform

[49] ENISA counts 43 publications with recommendations and best practices. More information at: https://www.enisa.europa.eu/publications#c5=2008&c5=2018&c5=false&c2=publicationDate&reversed=on&b_start=0&c10=Critical+Infrastructures+and+Services

[50] ENISA, Rossella Mattioli methodology, 2014.

- “The European Forum for the Member States” (EFMS) as a trusted shared mechanism for enabling discussions and information exchange between national competent authorities and national CERT teams for good practice relative to the resilience of ICT infrastructures, the organization of exercises at pan-European level etc;
- The establishment of a national CERT providing guidance: “A Step-by-Step approach on how to set up a CSIRT”;
- The development of the European Information Sharing and Alert System European (EISAS) for supporting the Member States their obligation to set up a national platform for reporting any significant cyber with the aim to raise public awareness on security issues: “How to raise information security awareness”.

In picture 3 we can see the ENISA’s activities framework.


Developing and maintaining a high level of expertise of EU actors taking into account evolutions in NIS
Assisting Member States and the Commission in enhancing capacity building throughout the EU
Assisting Member States and the Commission in developing policies necessary to meet the legal and regulatory requirements of NIS
Enhancing cooperation both between Member States of the EU and between related NIS communities

Picture 3: Strategic objectives of ENISA[51]

[51] Ramboll Management Consulting, based on ENISA website.

2 Network and Information Systems Directive (NISD)

2.1 NIS Directive general description and objectives

Building upon other non-binding EU policies[52], the Network and Information Systems Directive (NISD) is the first EU-wide legislation on cybersecurity in the framework of the so-called "EU Cybersecurity strategy". The Directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. In pursuant to its context, Member States should have transposed it into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.

The content of NISD may be translated as the European Union's answer to the partial disregard of states to include cybersecurity within their national priorities.

Particularly, although there have been established legislation regarding the protection of critical infrastructure, there have also been identified huge discrepancies at national readiness level, either because there were no adequate financial resources or because there was lack of awareness to a very high percentage.

For this reason, the European Commission requires from all Member States, including the owners of the Critical infrastructures of the private sector[53], to upgrade the cybersecurity issue among their key priorities, wishing to point out on the one hand that cyber risks do occur and, on the other hand, the need for universal application of specific technical and operational measures, for achieving a common maturity level within EU countries for resisting and responding effectively to these possible threats.

The NIS Directive sets up the following three strategic pillars as its main objectives:

- To raise public awareness and promote a culture of security across all vital sectors of social life;

[52] *Fahey*, The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security, European Journal of Risk Regulation 2014, pp. 49-51.

[53] Since most the operation critical infrastructures are based on the digital services provided by the private sector.

- To support the Member States on strengthening their national capabilities[54];
- To promote better coordination and cooperation within EU by building trust among the Member States while building on the international cooperation.

Critical actors of this focused European cybersecurity effort are the owners of the Critical Infrastructures (CI) since their provided operations and services are extremely essential to the economic growth of their country and highly depended on the extended use of ICT products. In other words, the European Commission forces certain key technology businesses and infrastructure providers focusing on maintaining a minimum common level of European security standards.

Although the context of the Directive applies to all Member States it, however, applies to "operators of essential services" in the energy, transport, banking, financial market infrastructures, health sector, water and digital infrastructure sectors[55]and to certain "digital service providers".

Pursuant to Directive's content the following two distinct groups will be affected:

I."**Operators of essential services**", in terms of a public and private entity, which fulfils any of the following criteria:

- provide a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- An incident affecting those systems would have significant disruptive effects on the provision of that service; any security incident[56] that may cause the disturbance of the provided critical services is considered an essential one[57].

Additionally, individual Member States must identify and draw up a list of these operators. This list will include the larger operators from the above-mentioned CI and it will be reviewed periodically, not only from the individual Member States, but from the European Council (EC) too, for consistency purposes.

[54] Advanced cyber security capabilities always offer more perspectives of improved selected capacities since strategic planning may reveal the existing vulnerabilities that they were not easily visible from the beginning.

[55] From Annex II.

[56] The security incident may be caused due to physical and cyber threats or human errors.

[57] According to Article 4 (4) NISD 'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2).

II. **Certain digital service providers** (DSPs)[58] or internet enablers, such as:

- Online marketplaces;
- Online search engines; and
- Cloud computing services.

Excluded from these procedures are the "micro and small enterprises'[59].

All these owners of CI, from both two distinct groups, are required to update their incident handling processes and notify immediately to the Member States' representative (the defined national competent authority) of any cybersecurity incident, causing disturbance of their services[60].

Additional significant players in shaping the European cybersecurity area are the individual States. They particularly must locate the peculiarities and identify the existing governance mechanism behind these obligations, to decide on how they will be implemented into national laws.

More specifically the Member States are required to adopt a national cybersecurity strategy (NCSS) on the security of network and information systems [61] and to notify significant security incidents by designating national competent authorities (NCA), single points of contacts (SPOC) and Computer Security Incident Response Teams (CSIRT) responsible for the effective handling of these incidents. Additionally, the NCSS requires the creation of a Co-operation Group (Coop-Group) for assuming the overall responsibility, for coordinating the efforts made by Member States and all related stakeholders[62], alongside with the creation of a Cybersecurity Incident Report Team network (CSIRT network), with a view to responding rapidly to cyber threats and incidents[63], based on experience gained and use of best practices of the security communities.

The Member States were obliged to identify until 9.11.2018, businesses operating in their territory as "operators of essential services"[64] and create a relevant list. To make sure that all Member States will follow a common approach for the identification of the

[58] From Annex III.
[59] As it is defined in Commission Recommendation 2003/361/EC.
[60] Article 2(d).
[61] Article 2(a).
[62] Article 2(b).
[63] Article 2(c).
[64] Article 5 (1) NISD.

Operators of Essential Services[65] (OESs), a list of each sector and subsector is provided through the Annex II of the Directive, to serve as a roadmap at the identification process.

While the NISD requires the Member States to identify operators of essential services in their territory, it does not do the same with the digital service providers.

According to the NIS Directive, identified operators OESs and DPSs are obliged to adopt appropriate security measures and notify serious cyber incidents to the relevant national authority.

The details for achieving the NIS Directive's implementation will be described into followings paragraphs.

2.2 General provisions of NISD

The NISD provides the theoretical background for the necessary measures, that relevant stakeholders[66] should set-up, having taken into consideration that its correct transposition into national laws would be jeopardized by the diversity at organizational and administrative level from nation to nation. Additionally, the European Commission adopted on 13.09.2017 a Communication in order to support Member States to implement the NISD coherently across the EU[67].

For the purposes of achieving a coherent European approach, the Directive provides criteria for identify OESs, and definitions for DSPs and technological digital provider products and terms, for ensuring the common understanding between Member States and CI relevant stakeholders. Additionally, it introduces certain processes to be followed by the Member States for:

- the provision of *lex specialis*;
- classification of the impact of the incident;
- controlling cross-border affection;
- identifying the operators of essential services;
- the content of the reviewed list of identified OESs;
- the relationship between the NIS Directive and other legislation.

[65] Article5.
[66] Member states, OESs and DSPs.
[67] Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 COM (2017) 476.

2.2.1 The provision of *lex specialis*

Under *lex specialis* principle of Article 1(7), the operators of essential services and the digital service providers are not required to apply the security and notification requirements demanded by the NIS Directive as long as “an EU sector-specific legislation provides for security and notification requirements, which are at least equivalent in effect to the corresponding obligations of the NIS Directive”[68].

2.2.2 Classification of the impact

The Directive defines an incident as critical when the continuity of the provided operations and services are negatively affected. However, the continuation of the service may be jeopardized not only in cases involving physical availability but also by malicious acts that endanger the provision of services. More precisely, as an incident may be considered any fact that has a real negative impact on the ability of networks and information systems to resist to any act that compromises the availability, authenticity, integrity and confidentiality of data stored or transmitted or processed, or any related services offered by or through its networks and information systems[69];

For the coherent application of the measures by all Member States and relative stakeholders from the public and private sector, some general criteria are provided for distinguishing critical incidents[70]:

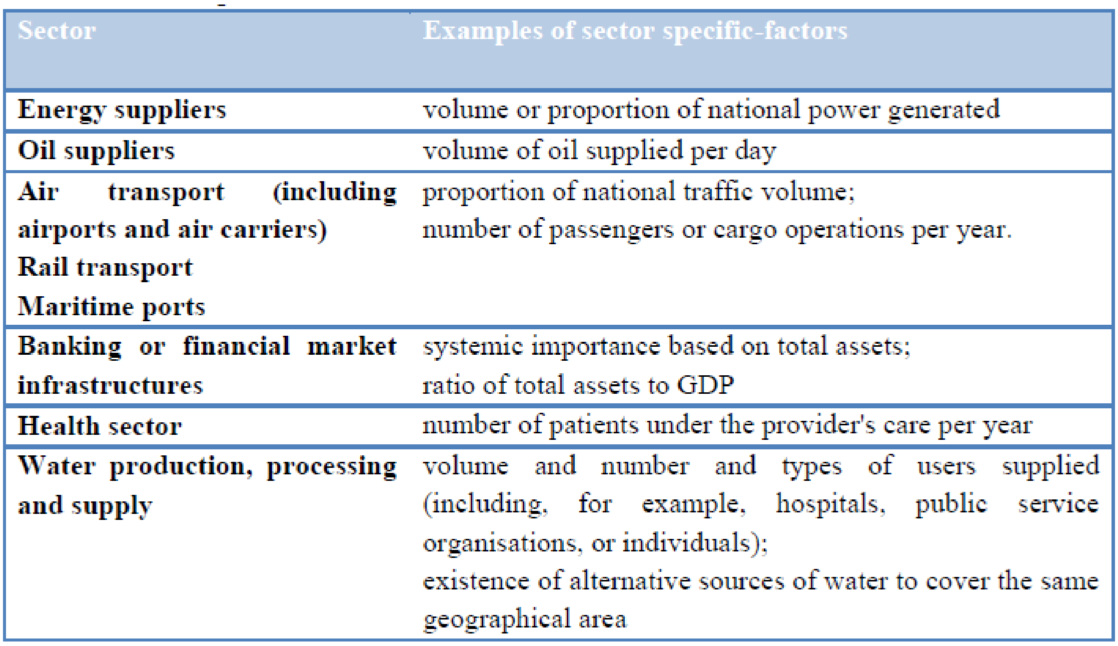
- “The number of users relying on the service provided by the entity concerned”[71];
- “The dependency of other sectors referred to in Annex II on the service provided by that entity”[72];
- “The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety”[73];
- “The market share of that entity”[74];
- “The geographic spread with regard to the area that could be affected by an incident”[75];

[68] Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148, COM (2017) 476, p. 36.
[69] Article4(7)(2)
[70] Article6(1)
[71] Article6(1)(a)
[72] Article6(1)(b)
[73] Article6(1)(c)
[74] Article6(1)(d)

- “The importance of the entity for maintaining a sufficient level of the service, taking into account, the availability of alternative means for the provision of that service”[76].

Further to the above-mentioned general criteria, the Member States should define **sector-specific factors,** that would probably cause a significant disruptive effect on provided essential services. Member States should consult with stakeholders of the critical infrastructure sectors indicated by Annex II of the Directive in order to decide jointly which other important criteria should be included so that the implementation and application of the above criteria would be effective. Examples of such criteria are given in table 2, such as for energy sector could be the volume or the proportion of national energy produced; for air transport sector (the airports and air carriers), sector-specific factor could be the proportion of national traffic volumes and the number of passenger or cargo operations per year[77].

Table 2: Examples of sector-specific factors to be considered for determining the significant disruptive effect in case of an incident.



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

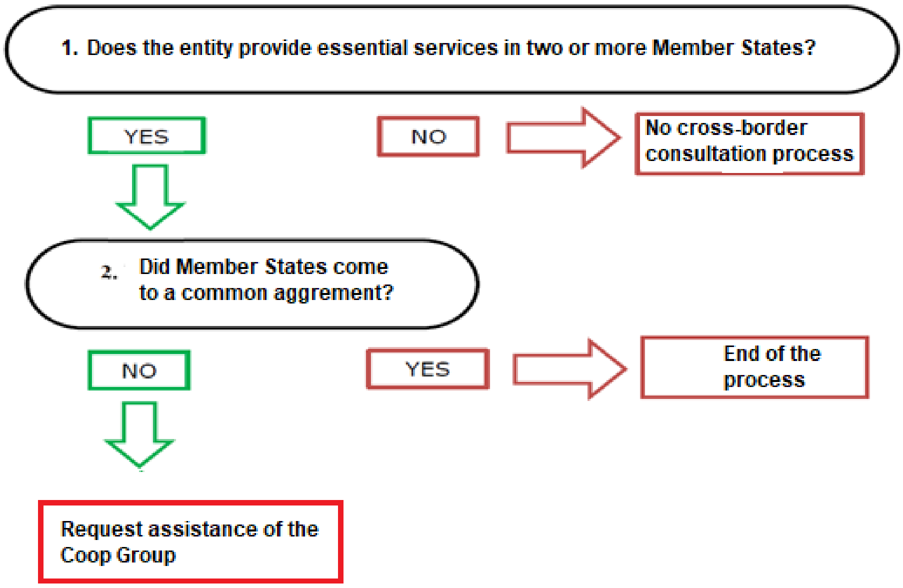
[75] Article6(1)(e)
[76] Article6(1)(f)
[77] Recital 28

2.2.3 The cross-border affection

When an entity provides services in two or more Member States, all Member States involved will include it on their OESs lists. Bearing in mind that the Directive does not oblige the use of specific technical security products, this automatically implies a disparity between the Member States concerning the preventing and ensuring the service's continuation. For that purpose, Member States are obliged to consult each other in order to agree in a joint action plan, which will ensure that they are dealt with under a common legal framework, in order to avoid any inconsistency, which will hinder the effectiveness of the Directive.

However, there is the possibility the Member States do not come to an agreement; in that case, they may request assistance from the Cooperation Group[78]. The schematic of the cross-border affection process, is provided in diagram 1.

Diagram 1: The cross-border affection process.


1. Does the entity provide essential services in two or more Member States?
YES
NO
No cross-border consultation process
2. Did Member States come to a common aggrement?
NO
YES
End of the process
Request assistance of the Coop Group

[78] Recital 24.

2.2.4 The identification of operators of essential services

To make sure that all Member States follow a common approach for the identification of the Operators of Essential Services[79], a list of each sector and subsector is provided in Annex II of the Directive to serve as a roadmap in the identification process.

Therefore, all Member States should initially record all the organizations, which are active in the following Critical Infrastructure sectors, either as public or as private entities, and in accordance with Annex II:

- Energy;
- Transport;
- Banking;
- Financial market infrastructures;
- Health sector;
- Drinking water supply and Distribution; and,
- Digital infrastructure;

Particular attention should be paid to the possible existence of an EU legal act which imposes security and/or notification requirements on OESs like the requirements imposed by the NIS Directive[80].

In case it does exist, the NIS Directive requirements should not be applied to the operator of the services; otherwise, the identification process of the OESs should proceed.

The next step includes the following two questions[81] that need to be firmly answered for the service provider to fall within the scope of the NIS Directive:

a. Is it an organization that provides a service essential to maintaining the social and economic development of the region?
b. Is this service produced using networks and information systems?

Following the identification process, the next question should be:

- In the case of a cyber-attack on the provisions of the network and information systems, would this affect the continuation of this service?[82] (**The classification of impact process initiates**).

[79] Article 5.

[80] Article1(7). See also *Esays*, Breach notification requirements under the European Union legal framework: Convergence, Conflicts, and Complexity in Compliance, The John Marshall Journal of Information Technology & Privacy Law 2014, Article 2, pp. 317-368, specifically pp. 329 et seq.

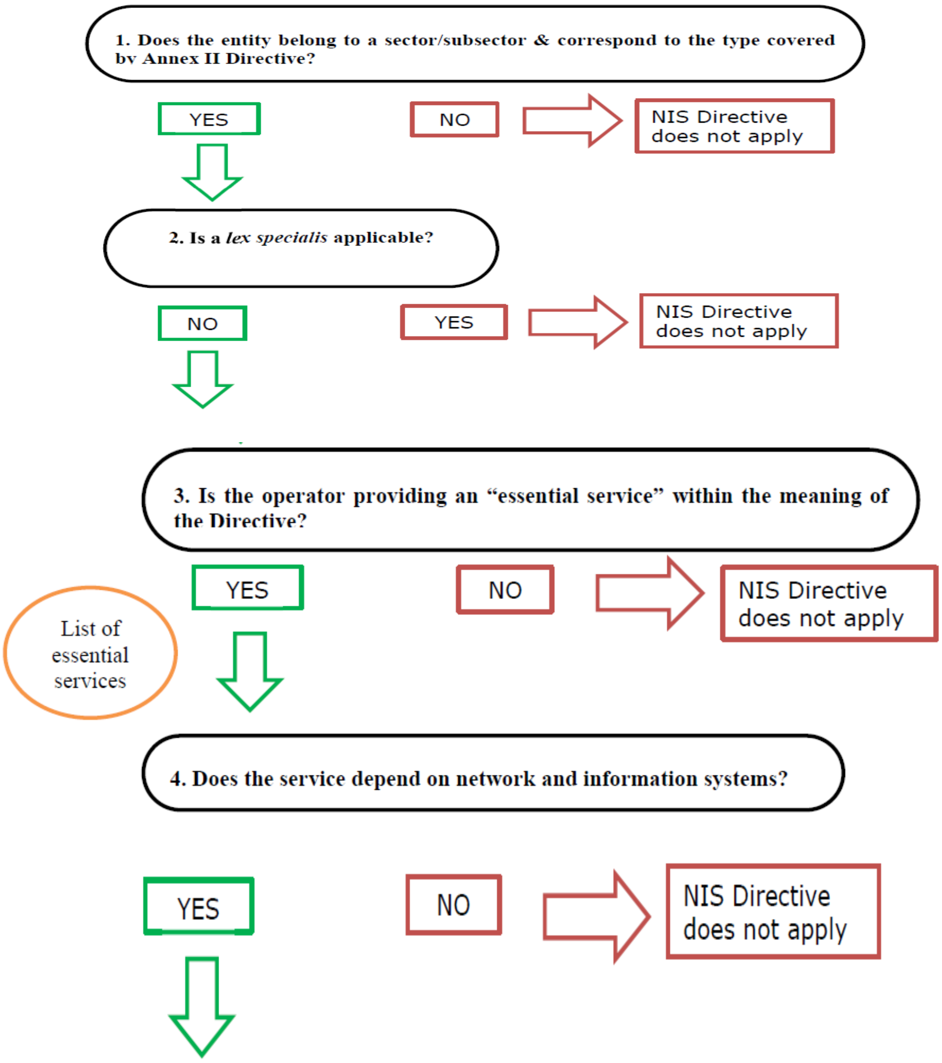
[81] Based on the criteria as mentioned in article 5(2)(a)(b).

Finally, Member States must answer the last one question to create the final form of the list with the identified OESs according to the NIS Directive:

- Does the operator provide basic services in other Member States[83]? (**The cross-border affection process initiates.**)

The identification process of OESs is provided by ENISA in diagram 2[84].

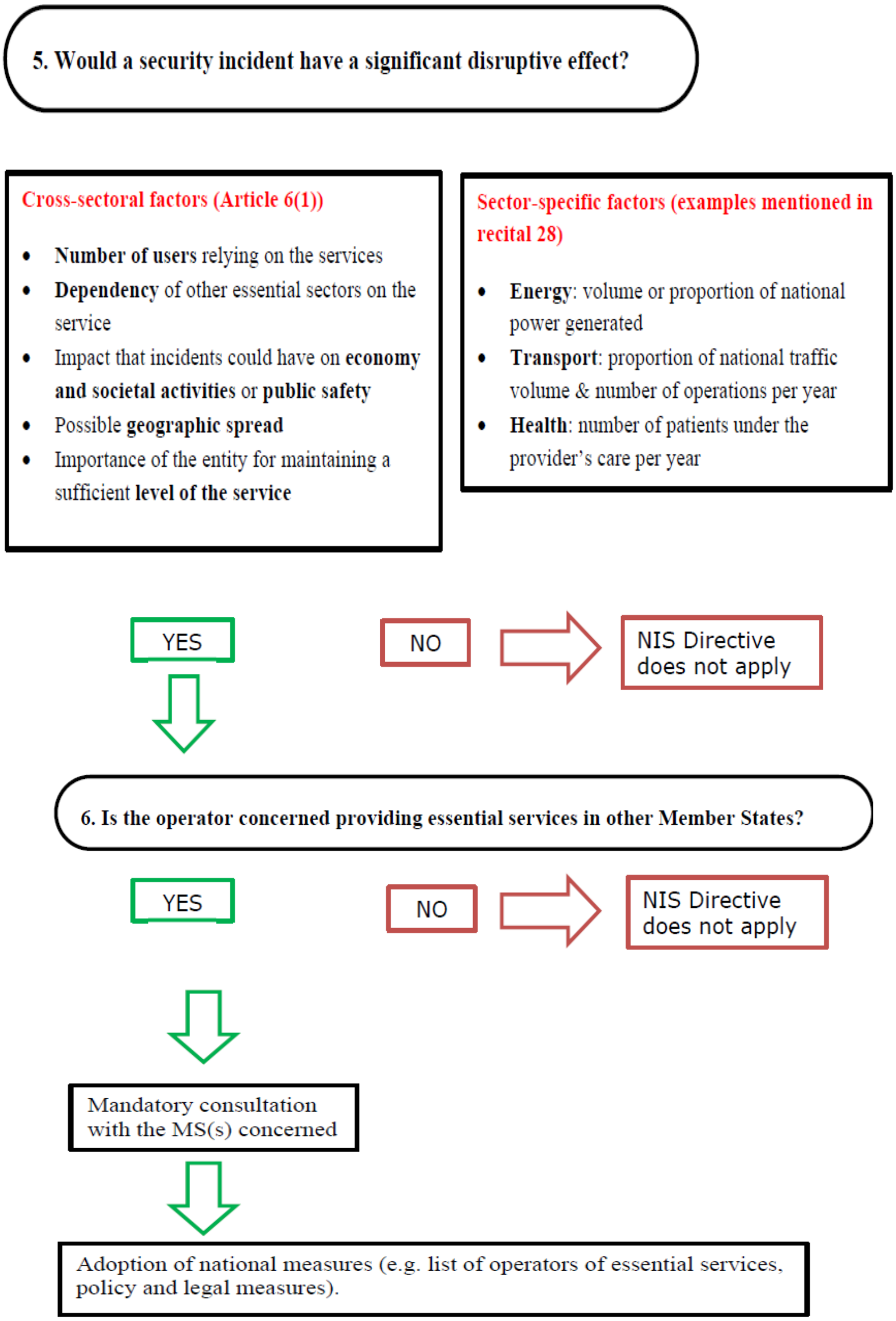
Diagram 2: OESs identification process.


1. Does the entity belong to a sector/subsector & correspond to the type covered by Annex II Directive?
YES
NO
NIS Directive does not apply
2. Is a lex specialis applicable?
NO
YES
NIS Directive does not apply
3. Is the operator providing an "essential service" within the meaning of the Directive?
YES
NO
NIS Directive does not apply
List of essential services
4. Does the service depend on network and information systems?
YES
NO
NIS Directive does not apply

[82] Which condemns the devastating consequences of the interruption of this service, article 5(2)(c), the classification of impact process initiates.

[83] The OESs are required to notify the competent authority of the Member State where they have their main establishment, the cross-border affection process initiates.

[84] Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 COM (2017) 476 p. 28.



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

Cross-sectoral factors (Article 6(1))

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

Sector-specific factors (examples mentioned in recital 28)

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

YES

NO

NIS Directive does not apply

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

YES

NO

NIS Directive does not apply

Mandatory consultation with the MS(s) concerned

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

2.2.5 The reviewed list of OESs

The above-mentioned list of OESs established by each Member State should be communicated to the European Commission in order to monitor the correct implementation of the identification process of the OESs at each national level. Moreover, Member States are required to submit to the Commission by 9 November 2018 and every two years thereafter the following information:

- The list of essential services[85];
- The number of identified OES for each sector referred to in Annex II and the relevance of those operators for the sector[86]; and,
- Thresholds identified for determining the supply level by reference to the number of users relying on that service or to the importance of that particular operator of essential services[87].

2.2.6 The relationship between the NIS Directive and other legislation.

- Directive 2002/21/EC[88]:

The Directive underpins that the security and notification requirements for operators of essential services and digital service providers identified from Annexes II and III are not applicable if these EU sectors are subject to the requirements of Article 13a and 13b of Directive 2002/21/EC. However, there is the possibility of the same company to provide digital services that are subject to the NIS Directive, such as cloud computing or services such as the Internet Exchange Point (IXP)[89]. In that case, the company will be subject to the security and notification requirements of the NIS Directive and should be included in the list of the identified operators of essential services by the Member States. So, the Member States should identify properly all the providers of Domain Name Server (DNS), Internet Exchange Point (IXP)or Top-Level Domain (TLD) ser-

[85] Article 5(a).

[86] Article 5(b).

[87] Article 5(c).

[88] Recital 7.

[89] Annex II (7). According to COM (2017)476 final, p. 21, "The term Internet Exchange Point is defined in Article 4(13) and clarified further in recital 18 and can be described as a network facility that enables the interconnection of more than two independent technically stand-alone systems, with the primarily purpose to facilitate the exchange of internet traffic".

vices that belong to the operators of essential services and thus should comply with the requirements of the NIS Directive.

- Regulation (EU) No 910/2014[90]:

The NIS Directive shall not apply to trust service providers that are subject to Article 19 Regulation (EU) No 910/2014[91].

- Directives 2008/114/EC[92], 2011/93/EU[93], 2013/40/EU[94]:

The NIS Directive applies without prejudice to Council Directive 2008/114/EC and Directives 2011/93/EU and 2013/40/EU of the European Parliament and of the Council[95].

- Processing of personal data:

Processing of personal data pursuant to NISD shall be conducted according to the Directive 95/46/EC at the national level (since 25.5.2018 according to the General Data Protection Regulation), while at Union level under the Regulation (EC) No 45/2001.

- Protection of essential interests:

The Member States retain the right not to disclose data during the notification of incidents that may affect the national security or may allow for the investigation, detection and prosecution of criminal offences[96].

2.3 Setting up the EU preparedness

In order to deal with the problem of non-uniformity in the national legal framework effectively, it is necessary for all Member States to implement the NISD coherently. For that purpose, the Directive sets out a series of measures and obligations for the Member States such as:

1. To develop a national strategy for the security of network and information systems, the so-called National Cybersecurity Strategy (NCSS)[97].

[90] Recital 7.

[91] Article 1(3).

[92]Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008) p. 75.

[93] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

[94] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8.

[95] Article 1(4).

[96] Recital 8.

Through this measure the Member States are invited to set national targets and priorities, to adopt comprehensive policies and regulatory compliance measures that ensure high levels of the security of the networks and information systems.

In order to do so, the NCSS should include:

- Strategic objectives, priorities and governance framework;
- Identification of measures on preparedness, response and recovery;
- Cooperation methods between the public and private sectors;
- Awareness raising, training and education;
- Research and development plans related to NIS Strategy;
- Risk assessment plan;
- List of actors involved in the strategy implementation

2. To adopt the following governance structure by setting-up[98]:
   - National Competent Authorities (NCA) to monitor the implementation of the Directive;
   - Single points of Contact (SPOCs) responsible for ensuring the cross-border cooperation between the Member States; and
   - CSIRTs responsible for the handling of incidents reported relative to the security of Network and Information Systems.

Therefore, the Member States should begin by deciding first which key critical sectors should be considered significant for maintaining their economic prosperity, and the development of the society.

In the view of the author, the Member States should stay strictly limited to the given criteria concerning whether an organization provides essential services for maintaining the social and economic development of the internal market through the use of networks and information systems. Otherwise, diverse views could cause the incorrect application of the procedure,[99] jeopardizing the minimum harmonization for OESs[100].

[97] Article 1(2)(a).

[98] Article 1(2)(e).

[99] Identification process of OESs.

The Member States must communicate the list of OESs to the Commission[101] and are required to review it by the endorsement, every two years at least, after 9 May 2018[102].

Bearing in mind that the security of networks and information systems is a continuously changing field, since more frequent and sophisticated risks are emerging, this list should also be in line with the actual current cyber threats.

2.3.1 The National Cybersecurity Strategy (NCSS)

The NISD defines the national cybersecurity strategy as the appropriate instrument for defining the national frameworks on the security of networks and information systems. So, all Member States are required to set the cybersecurity concern as a priority into their national strategies, and finally adopt a National Cybersecurity Strategy. In case some Member States have already a national framework in place, where cybersecurity challenges are included in its generic key themes, they are additionally required to review it in a manner that it will be enhanced with the NIS Directive's objectives, in building on the preparedness and resilience[103] of the Member States, on addressing the cyber-attacks affecting the security of Network and Information Systems within the EU.

However, the cyber-protection of the EU is a collective effort. And the correct transposition of the NIS Directive into the national legal systems is a fundamental condition for the achievement of the NIS Directive's objectives.

Although the drafting procedure of the cybersecurity strategy is not described in the Directive[104], it emphasizes what should be included[105].

So, each Member State is required to create a national cybersecurity strategy including, a framework of activities serving as a complementary to the clearly defined strategic priorities and objectives on the security of network and information systems[106]. The creation of a national cybersecurity strategy includes two stages:

- ❖ The designing and developing;
- ❖ The implementation and maintenance.

[100] Article3.
[101] Article 7.
[102] Article5(5).
[103] Article 7 (1) (c).
[104] Neither Article 7 nor the corresponding recital 29 specify the process.
[105] It sets out the theoretical background for the developing issues on a NCSS.
[106] Article 7 (1)(a).

During the drafting process of NCSS, each country must define what the desired outcomes[107] are and how they can be accomplished.

It is useful for the Member States to adopt a national cybersecurity strategy that will encompass all those areas of considerable value for the social and economic activity of the country. The Directive obliges them to do so in order to set a minimum threshold for joint action[108].

The Commission recognizes that this process will be complex and demands the engagement from many different stakeholders, which are considered an expert in the specified field. For that purpose, the Commission introduces the continuous commitment from ENISA[109], due to its speciality being considered as an expert in the security of the Networks and Information Systems, with relevant workshop activities.

So, the Member States should initially document clearly and defined at least the following requirements for[110]:

- Identifying and reviewing an existing institutional framework involved in the implementation of the NCSS for ensuring an efficient and effective cooperation between national authorities[111] ;
- Creating a comprehensive legal framework covering all cases of network and information security, alongside with the cybercrime and the protection of personal data;
- Developing an information security policy focusing on the protection of hardware, software and physical working spaces, to an advanced level[112];
- Organizing educational programs by training and raising awareness in security topics, for citizens and user*;*
- Performing a risk assessment for assessing the existing security measures so as to develop, implement and review the strategy[113];
- Setting a clearly defined governance structure with roles, responsibilities and accountability of all relevant stakeholders[114];

[107] Article 1(a), objectives and priorities.
[108] Setting the minimum common level within Europe.
[109] Article 7(2).
[110]In accordance with the ENISA's guidelines on NCSS (NCSS Good Practice Guide), available at: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>
[111] Article 7(1)(g).
[112] Article 7(1)(a).
[113] The identification of measures relating to preparedness, article 7(1)(c) (f).
[114] Article 7(1)(b).

- Establish trusted information-sharing mechanisms for promoting and establishing cooperation and coordination between different relevant stakeholders from the public and private area[115], on both the national and international level[116];
- Identifying the operators of essential services[117];
- Identifying the mitigation treatment to specific cyber threats and risk levels[118];
- Developing National cyber contingency plans[119], including implementation of the selected mitigation treatment to specific cyber threats and risk levels[120];
- Organizing Cybersecurity exercises at the national level[121];
- Setting baseline security countermeasures for all the relevant stakeholders from both of public and private area;
- Developing incident reporting mechanisms while identifying and enhancing the national incident response capabilities;
- Communicating the incidents and impacts for raising users and public awareness[122];
- Organizing training and educational programmes performed at regular time intervals;
- Involving with international cooperation;
- Establishing a public-private partnership;
- Designating national competent authorities (NCA), CSIRTs and single point of contact (SPOC) within public agencies;
- Supporting Research and Development and Academic Education Programs[123];

[115] For facilitating cooperation between private and public sector, article 7(1)(c).
[116] Article 10.
[117] Article 7(1)(g).
[118] Implied from articles 7(1)(c) and (g).
[119] An identified measure for recovering from cyber threats, article 7(1)(c).
[120] Implied from articles 7(1)(c) and (g).
[121] "An indication of training programmes", article 7(1)(e).
[122] "An indication of relevant awareness-raising programmes", article 7(1)(e).
[123] "An indication of relevant education programmes", article 7(1)(e).

2.3.2 Setting up the national monitoring framework

In order the NISD to be properly implemented at the pan-European level, it is necessary to introduce the instruments responsible for monitoring the implementation of the Directive initially at the national level. So, each Member State is required to assign at least three roles for ensuring the correct transposition of the NIS Directive into the national legal framework. These roles are:

- national competent authority (NCA);
- a single point of contact (SPOC);
- a national CSIRT.

2.3.2.1 The role of the national competent authority

Each Member State is required to designate one or more[124]national competent authorities for being accountable mainly for the identified OESs and DSPs[125], without excluding the option to also cover additional sectors and services[126]. The role of the national competent authority is the monitoring of the implementation process[127] of the NIS Directive at the national level[128], and this role may be assigned within an existing authority[129].

Therefore, Member States are free to choose either a central authority dealing with all sectors and services covered by the Directive or several authorities, depending for example on the type of sector, based on the differences in national governance structures[130].

[124] Member States have the option to choose which governance approach would be more efficient and effective so as to function complementary to the overall national governance they use: a) the centralized approach; b) the decentralized approach; c) the hybrid approach.

[125]Annexes I &II.

[126]Article 8 (1):" covering at least the sectors referred to in Annex II and the services referred to in Annex III".

[127] In case of non-compliance the national competent authority has the right to impose an effective proportionate and dissuasive sanction, considering various factors such as the gravity or frequency of the infringement, article 21 NISD.

[128] Article 8(2).

[129] Article 8(1).

[130] Recital 30.

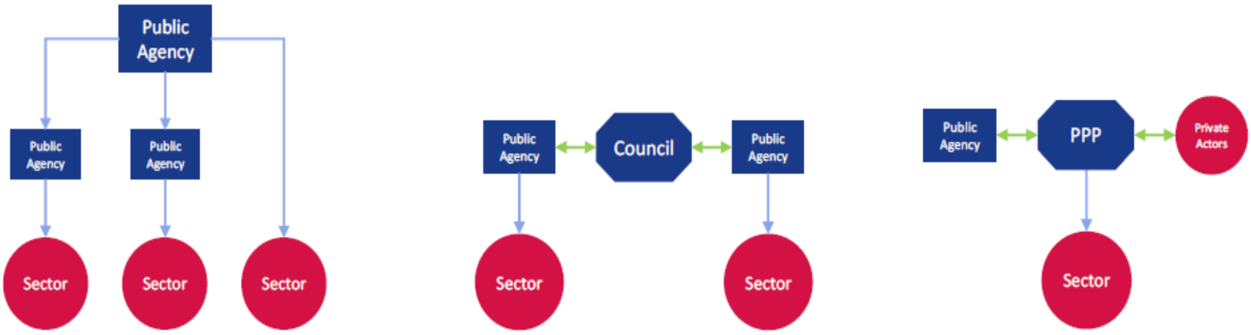
2.3.2.1.1 Governance structures

A. **Centralized approach***:* This type is characterized by a central cybersecurity authority with wide responsibilities and capabilities within different sectors.

B. **Decentralized approach***:* This type is characterized by a strong degree of cooperation between multiple sector-based authorities being responsible for specific sectors and services.

C. **Hybrid approach***:* This type is characterized by the combination of elements of both centralized and decentralized approaches.

Examples of the above-mentioned governance structures are given in picture 5[131].



Picture 5: Governance structures: A. centralized; B. decentralized; C. hybrid

2.3.2.2 The role of the single point of contact (SPOC).

Each Member State is required to designate a national competent authority as a single point of contact (SPOC), to function as an intermediary[132] with:

- ❖ The relevant authorities at the national level:

a national competent authority requests the single point of contact to forward the notification of an incident to initiate the cross-border affection process for the Member States that are affected by the incident.

- ❖ The corresponding SPOCs of other Member States:

The single point of contact of one Member State forwards the notification of the incident to the relevant national competent authorities and the CSIRTs for sharing information and managing the risk.

[131] NCSS Good Practice Guide, p. 18.
[132] Article 8(4).

- The cooperation Group:

The single point of contact of each Member State must submit every year a summary report to the Cooperation Group[133] on received incident notifications reporting the number of notifications, the nature of the incidents and the measures taken by the national authorities.

- The CSIRT network[134]:

in situations that the single point of contact is also the CSIRT for exchanging information relative to incident handling and reporting.

Therefore, we may see that the role of the single point of contact is quite strategic for establishing a "trusted cross-border information sharing mechanism[135]" in order to facilitate the identification and cooperation of competent authorities, between different Member States[136]; in case of a significant security incident occurrence, the incident notification process should strictly define as a proper communication process, only the direct communication of SPOC, with corresponding ones at Union level.

In case a Member State adopts a centralized governance approach, the designated national competent authority (NCA) will also have the role of the single point of contact (SPOC)[137].

The Member States are obliged to inform the Commission about the designation of the single point of contact and its tasks by the transposition deadline.

Afterwards, the Commission shall publish the list of designated single points of contact for ensuring transparency and effective coordination, between the relevant authorities at national and European level too[138].

[133] The Coop-Group is the responsible authority for coordinating the efforts made by Member States and all related stakeholders during the transposition of the NISD into national laws. Further analysis about the Coop-Group at paragraph 2.4.1.

[134] A network of national CSIRTs for operational cooperation between Member States under Article 12

[135] *ENISA*, NCSS Good Practice Guide, p. 20.

[136] Article 8(4), recital 31.

[137] Article 8(3).

[138] And even at global level too.

2.3.2.3 The role of the CSIRT

Each Member State is required to create a team of IT[139] security experts, responsible for responding to the computer security incidents[140], based on certain capabilities and requirements[141] defined in a relative policy document. This policy should be communicated to the Commission[142].

The role of the CSIRT includes:

- ✓ The monitoring of the incidents[143];
- ✓ The provision of early warning, alerts and information sharing to relevant stakeholders in case of incidents reported[144];
- ✓ The response to incidents[145];
- ✓ The provision of dynamic[146] risk and incident analysis and raising situational awareness[147];
- ✓ The Participation in a network of the CSIRTs[148] within EU.

The Directive defines the theoretical base, under which the framework of activities of the CSIRT should be adopted, aiming the strengthening of the EU resilience on cybersecurity risks. Additionally, ENISA has provided a relative guidance for the Member States in order to support their efforts in creating a CSIRT[149].

[139] Information technology.

[140] By providing to the relative stakeholders from the Critical Information, public and private sector, all the necessary services in order to handle the IT security incidents and support the continuity of the services.

[141] Annex I.

[142] Article 9.

[143] Annex I (2)(a).

[144] Annex I (2) (b).

[145] Annex I (2) (c).

[146] Dynamic in the sense that the data changes as the time passes by and the actions taken to cope with the incident will also change till the succeed respond to the cyber threat.

[147] Annex I (2) (d).

[148] Through partnerships with public and private area and cooperation with CSIRTs' from different Member States, based on the tasks referred in Annex I(2)(c)(d).

[149] ENISA, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2).

In accordance with ENISA study, the nature of the expected function of the CSIRT, should be characterized by[150]:

- *Pro-activity*: in terms of preparedness, through awareness building and training;
- *Reactivity*: in terms of providing incident handling and mitigation treatment activities[151];
- *Artifact handling*: performed through analysis of the evidence found[152];
- *Security and quality management services*: provided through clearly defined responding and mitigation plans.

The creation of a CSIRT includes two stages:

A. The development of the operation plan; and,

B. The implementation and maintenance of the operation plan.

A. The development of the operation plan

The Member States should develop an operation plan with clearly defined procedures ensuring the security, the quality and the strengthening of the provided services from the CSIRT. More specifically, the creation of the CSIRT entity should be complemented by a policy document focusing on the following priorities:

1. **Planning for monetary issues[153]:** The financial support[154] for the proper function of the CSIRT must be clearly defined.
2. **Defining the organizational structure:** The Member States have the right to choose the governance model that is in line with the already existing organizational framework for their operation and cooperation at the national level.

   It will be possible either to designate a centrally independent CSIRT that will be responsible for all OESs and DSPs, at least or more than one[155] CSIRTs.

[150] These are implied in the CSIRT tasks in Annex I (2), in accordance with European Commission - Fact Sheet “Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cyber security”.

[151] Based on the tasks of the Annex I (2).

[152] Based on the requirement of Annex I (3).

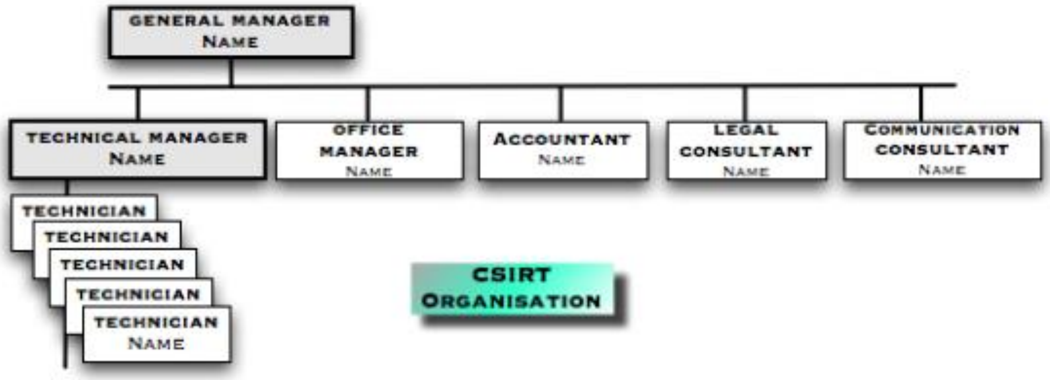
[153] Article 9 (2): “adequate resources”.

[154] E.g. use of existing resources, subsidiary, membership fee.

[155] Article 9 (1).

Example 1: ***The independent business model***

The CSIRT team is not part of the organization structure; it is an independent body, with its own administration and personnel (picture 6).



Picture 6: The independent CSIRT model[156].

Example 2: ***The built-in model***

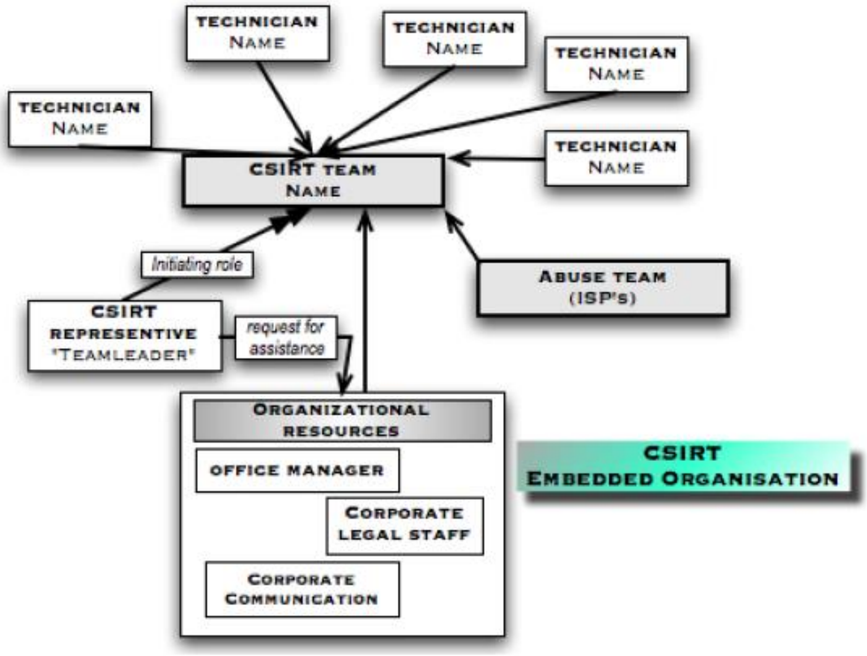
The CSIRT group is established within an existing organization[157] and uses the existing ICT infrastructure for performing its tasks.

By studying picture 8, we understand that in this model there is one person responsible for concentrating the necessary technicians[158] and coordinating their activities concerning the solution of each different problem that arises (picture 7).

[156] *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2).

[157] In the case of Greece, The National Authority Against Electronic Attacks (NAAEA) is also the national computer emergency response team.

[158] Based on their expertise capabilities.



Picture 7: The embedded CSIRT model[159].

3. **Hiring the right staff:** The CSIRT should consist of personnel with technical expertise[160] and very good communication skills[161] in order to perform their daily activities, while communicating either between the team members or with other response teams from different critical sectors. The number of the required skilled people to perform the job, should be defined with accuracy complemented by their roles and responsibilities and the dedicated communication channels through their establishment they are able to ensure availability at anytime[162].
4. **Describing the utilization and equipment of the office:** this section should include information concerning:
   1. General rules about the building, for ensuring that the office can be accessible only from the authorized personnel[163];

   2. The establishment and maintenance of communication channels[164] used from and to the CSIRT: these should be secure and strictly defined, due to the very

[159] *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2).
[160] E.g. broad knowledge of internet technology and protocols.
[161] E.g. flexible, creative and a good team spirit.
[162] Counting even the holidays for back up support, annex I (1)(c)(ii).
[163] This may be achieved by using access control systems, CCTV systems, CSIRT office, use of special lockers for the storage of important archives etc.

sensitive nature of the information exchanging. This implies that a list of the provided communication channels,[165] alongside with the designated roles and responsibilities should be provided;

3. **Defining the systems used for searching for records** either for the main function or for backup support such as:
   - Contact database with details of team members, of CSIRT network, or other CSIRT form different critical infrastructure sectors, for ensuring the availability of the CSIRT[166] ; and,
   - Tools used for the proper function of the CSIRT concerning:
     - Incident handling (e.g. RTIR);
     - CRM Tools [167](e.g. Sugar CRM and Sugarforce).
4. **Developing an Information Security Policy** in line with national legislation, European regulations and international agreements for addressing:
   a. The management of the protection of the existing ICT and building infrastructure[168] taking into consideration additionally possible physical threats and human errors whilst ensuring the availability of the CSIRT's assistance;
   b. General rules for IT equipment concerning the hardening of the systems[169] and the proper and secure use from staff[170]should be adopted and maintained. An indicative tool may be: "Email and message encryption software"[171](e.g. GnuPG, PGP).

[164] "Besides using e-mail, web-forms, phone or fax to facilitate incident handling (to receive incident reports from the constituency, coordinate with other teams or give feedback and support to the victim) most CSIRTs publish their security advisories on a publicly available website and via a mailing lists*"- ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2), page 16.

[165] Annex I(1)(a): "have several means for being contacted", ensuring a "high level of availability of their communications services by avoiding single points of failure ".

[166] "A high level of availability of their communications services by avoiding single points of failure", Annex I(1)(a).

[167] CRM (Customer Relationship Management) used for compiling customer data across different communication channels.

[168]Some of such security mechanisms for ensuring the physical protection of the building could be: access control system, CCTV system etc.

[169] The use of security software such as: firewalls, multiple anti-virus scanners, anti-spyware, etc.

[170] This may be achieved by establishing formal guidelines regarding the hardening of the systems used (e.g. patch and update all the systems before connecting them to the internet).

[171]Article 9 (3). See also *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2), p. 53.

c. The backup system and workspace defined for managing and routing requests, alongside with the roles and the responsibilities of the involved persons, ensuring the business continuity[172].

d. The promotion of cooperation through established communication channels and partnerships, with a public and private area, such as:

   - The CSIRT network[173];
   - The TF-CSIRT[174] Task Force through an established forum for sharing information with CSIRT in Europe.
   - FIRST[175].

e. The establishment of an education program implemented at three levels**:**

- The training of the CSIRT;
- The raising of awareness of the public and the CSIRT[176]; it is obtained through the communication of the incidents' impact.
- Developing and implementing exercises for assessing the readiness of each Member State.

B. The implementation and maintenance of the operation plan

Each Member State is required to establish and maintain processes regarding the incident handling and notification, complemented by the definition of the selected applicable technology infrastructure.

The core services of the CSIRT are:

- Alerts and Warnings;
- Incident Handling;
- Announcement.

[172] Annex I (1)(c).

[173] Article 9(2).

[174] TF-CSIRT: *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2), p. 30.

[175] On FIRST see *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2), p.30.

[176]By participating in training courses e.g. organized by TRANSIT and CERT/CC. Cf. *ENISA*, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2), pp. 54-55.

Additionally, the action plan should include procedures regarding the:

- Analysis and responses;
- Collaboration and coordination;
- Notification and communication.

i) Analysis and responses;

During this phase, the Member States must define clearly the selected way[177] for:

- ➢ Collecting information;
- ➢ Evaluating the information considering the relevance and the source;
- ➢ Performing a Risk assessment[178] for determining the acceptable risk level;
- ➢ Selecting and applying the appropriate security mechanisms alongside with the defining processes followed for handling the security incidents[179].

ii) **Collaboration and coordination;**

During this phase, the Member States must define in detail the process followed for communicating with the CSIRT network for sharing information related to incident responses, and the point of contact (representative) of each critical sector (public and private).

iii) Notification and communication.

During this phase, the Member States must define in detail, the process followed by the single point of contact, for initiating the cross-border affection notification and for the communicating the incident to the public.

[177] Based on a free choice of scientific methodologies, however considering clearly defined criteria for classification of incidents and impacts purposes.

[178] The confrontation of the vulnerabilities with the identified critical assets in order to identify the possible threat(s) for each asset.

[179] Annex I(2)(c).

2.4 Enhancing EU cooperation and coordination

The next strategic pillar of the NIS Directive focuses on increasing the EU level cooperation and coordination for building confidence and trust among the Member States.

This is planned through:

- The creation of a Cooperation Group; and,
- The creation of a CSIRT network.

2.4.1 The role of the Cooperation Group (Coop-Group)

The NIS Directive introduces the establishment of a Coop-Group, responsible for facilitating the communication and therefore the cooperation between the Member States.

The cooperation Group is composed of representatives from:

- ENISA
- The Member States[180], and
- the European Commission (EC), who acts as a secretariat of the Coop-Group.

The role of the Coop-Group is crucial in providing guidance to the CSIRT network for sharing information and best practice on the one hand, and generally to the Member States, for enhancing their capacities in relation to exchanging best practice, security measures and raising awareness.

More specifically, the Coop-Group's tasks, as referred to in article 11(3) are;

a) Defining the way, the CSIRTs network performs its tasks, by providing strategic guidelines to the CSIRT network[181];

b) The provision of guidelines to the CSIRT network for exchanging best practices for handling incidents[182];

c) The provision of non-binding guidelines to the Member States, supported by ENISA's workshop activities, for exchanging best practice, aiming to assist in building national capacities on the security of networks and information systems[183];

[180] The Presidency of the Council of the EU is the chair of the Cooperation Group.
[181] Article 11(3)(a).
[182] Article 11(3)(b).
[183] Article 11(3)(c).

d) The productive[184] provision of consultant support to the Member States for evaluating the national capabilities and capacities, on a voluntary basis, and the effectiveness of CSIRTs[185];

e) The exchanging of information and best practice concerning training and awareness-raising[186];

f) The exchanging of information and best practice on the security of network and information systems, relative to research and development[187];

g) Maintaining of communication with relevant Union institutions, bodies, offices and agencies and exchanges experiences on relative security issues[188];

h) Building on a standardization approach with the assistance of relevant European standardization organizations[189];

i) The concentration of best practice information relative to risks and incidents[190];

j) The examination, on an annual basis, of the summary reports from the Single Point of Contacts with information relative to the incident notification[191];

k) Organizing cybersecurity exercises, education programmes and training, supported by ENISA[192];

l) The establishment of the following processes, supported by ENISA's contribution:

   - The identification process of operators of essential services by the Member States;
   - The cross-border affection process for notifying incidents to the neighboring Member States[193];

m) The consistent work on defining proper non-binding guidelines on incident notifications[194].

The Group's decisions are made by consensus; it may establish sub-groups to examine specific questions related to its work. The duration of the work programs is two years[195]

[184] Through the discussion process the cooperation group identifies best practices and promotes them accordingly.
[185] Article 11(3)(d).
[186] Article 11(3)(e).
[187] Article 11(3)(f).
[188] Article 11(3)(g).
[189] Article 11(3)(h).
[190] Article 11(3)(i).
[191] Article 11(3)(j).
[192] Article 11(3)(k).
[193] Article 11(3)(l).
[194] Article 11(3)(m).

and every fifteen months it is required to provide a report to the Commission, clarifying the positive contribution of the cooperation[196]. This report also functions as input to the European Commission's review of the Directive.

The Coop-Group has so far produced the following five documents:

- Compendium on cybersecurity of election technology;
- Cybersecurity incident taxonomy;
- Guidelines on notification of Operators of Essential Services incidents (formats and procedures);
- Guidelines on notification of Digital Service Provider's incidents (formats and procedures);
- Reference document on the identification of Operators of Essential Services (modalities of the consultation process in cases with cross-border impact).

2.4.2 The role of CSIRT Network

While Coop-Group aims to promote EU-level strategic cooperation, CSIRT network aims to foster EU-level effective operational cooperation and again to build trust and confidence between the Member States.

The role of CSIRT network is the provision of a communication channel (a forum) through which CSIRTs from each Member State can cooperate in exchanging information and best practice in relevance with the reported cybersecurity incidents on the networks and the information systems of the operators of essential services and digital service providers. A necessary prerequisite for this communication to be effective is the existence of trust and confidence among the members of the CSIRT network and therefore among the Member States197.

The Members of the CSIRT network are representatives from[198]:

- Member States' CSIRTs and CERT-EU[199]; and,
- ENISA, who will act as the secretariat[200] and an active supporter for incident coordination upon request[201].

[195] "Every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken", Article 11(3).

[196] Article 11(4).

[197] Article 12(1).

[198] Article 12(2).

[199] The Computer Emergency Response Team for the EU institutions, agencies and bodies.

[200] The Commission will participate in the CSIRTs Network as an observer.

The CSIRT network is required to perform the following tasks:

a. The exchanging of information related to services, operations of the CSIRT[202];

b. During the investigation process a representative of the Member State’s CSIRT that has potentially been affected by the reported incident, may be requested to disclose confidential information; However, any Member State's CSIRT has the right to not contribute to that debating if this is going to jeopardize the investigation of the incident[203];

c. The sharing and making available on a voluntary basis non-confidential data concerning individual incidents[204];

d. The establishment of coordination responses to an incident that has been identified within the jurisdiction of that same Member State through the discussing with the representative of a Member State's CSIRT[205];

e. The provision of guidelines and support to the Member States for handling cross-border significant security incidents on a voluntary basis[206];

f. The identification of additional types of operational cooperation considering the:
    - categories of risks and incidents;
    - early warnings;
    - mutual assistance;
    - principles and types of coordination, when Member States reply to cross-border risks and incidents[207];

g. The preparation of a report containing its activities with the additional identified types of operational cooperation discussed pursuant to point (f), and forwarding it to the Cooperation Group in order to request for guidance[208];

h. The provision of activities for raising awareness from gained experience through the cybersecurity exercises, including from those organized by ENISA[209];

i. The provision of guidance to the Member States, through their representatives in the CSIRT, for enhancing their national capabilities and preparedness[210];

[201] European Commission - Fact Sheet- Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity, p. 2.

[202] Article 12(3)(a).

[203] Article 12(3)(b).

[204] Article 12(3)(c).

[205] Article 12(3)(d).

[206] Article 12(3)(e).

[207] Article 12(3)(f).

[208] Article 13(3)(g).

[209] Article 13(3)(h).

j. The issuing of guidelines to be followed for a coherent operational approach from all the CSIRTs regarding the coordination-cooperation[211] among them.

Two years after entry into force of the NISD (by 9 August 2018), and every 18 months thereafter, the CSIRTs Network is required to provide an assessment report of the benefits obtained through the operational cooperation, including conclusions and recommendations, to the Commission[212]**.**

2.5 Security requirements for OESs

The security requirements for OESs engage the participation of individual OESs and the Member States, for ensuring not only that OESs have implemented the appropriate and proportionate security measures, but also the significant security incidents that have been notified to relative entities. These are achieved by focusing on:

- The appropriate and proportionate security measures adopted by the operators for essential services;
- The compulsory notification of the significant incidents, by the operators of essential services;
- The compulsory notification of incidents with a significant impact on the provision of the essential services by the Member States;
- The role of the national competent authority as an external auditor.

2.5.1 OESs' Security measures

OESs are required to assess the effectiveness of the existing technical and organizational controls[213] in order to evaluate the level of their preparedness, regarding the security of the networks and information systems they use for the provided services[214]. The selected management risk approach should maintain the character of prevention, reaction and limitation of impact over the disruption of the provided essential, to the society and economy, services. Additionally, they are also required to develop, implement and

[210] Article 12(3)(i).
[211] The CSIRTs network shall lay down its own rules of procedures, article 12(3)(j).
[212] This will serve as a contribution to the review of the functioning of the Directive.
[213] To perform a risk assessment process.
[214] Article 14(1).

maintain a business contingency plan[215] with clearly defined roles and responsibilities of the involved entities in accordance with their tasks, and strictly defined communication channels, through which the availability, confidentiality and effectiveness will be strengthened. The Directive does not indicate the type of methodology for performing relevant risk assessments nor the form of technology[216] to be used. This implies that OESs that already have established an information security management system (ISMS)[217] for addressing relative security issues, should review whether the existing security policies and the corresponding procedures address essthe identified cyber risks or not, and adjust them to a new management risk approach[218]. The main concern is the level of the provided protection[219], for establishing a minimum common level of networks and information systems security, across the EU. It is worthwhile to mention that in case a significant incident has been notified by the operators of essential services, this does not increase their liability[220]; even if they had implemented the appropriate organizational and technical measures, required by the Directive, there is always the possibility that a new sophisticated cyber threat arises that challenges the proper operation of their networks and information systems[221]. At this point, the Directive implies that their risk management approach should include a “monitoring process” at two stages:

i. One after the selection of the specific control mechanisms that are assessed appropriate for the handling of risk; and,

ii. A second one, after the implementation of the finally selected control mechanisms.

At both above situations, the relevant stakeholders of OESs may improve their awareness and their educational culture on the frequent changing cyber threat landscape.

Summing up, we understand that the proposed security measures that should be adopted by the Operators of Essential Services should consider the following five points:

1. Identify;
2. Protect;
3. Detect;

[215] Article 14(2).
[216] The capacity of the selected measures.
[217] An *ISMS* is a set of policies and procedures documented for systematically managing an organization's sensitive data.
[218] Implement specific security mechanisms for controlling the risks.
[219] The capability of the selected measures.
[220] Article 14(3).
[221] “Notification shall not make the notifying party subject to increased liability”, article 14(3).

4. Respond; and
5. Recover.

So, the minimum security domains that all OESs should cover in the developing of the information security management system are[222]:

1. Risk Management and governance;
2. The information security policy for addressing systems and facilities;
3. Human resources policy;
4. Contingency plan;
5. Security education, Training and Awareness Program;
6. Communications and management Operations;
7. Incident reporting notification;
8. Monitoring, auditing and testing.

2.5.2 Notification requirements for OESs

OESs are obliged to report incidents that fall under the scope of the NIS Directive. Any significant incident, having a serious impact on the service provided, must be notified to the national competent authority (NCA) or national CSIRT immediately. As a reportable incident the Directive underpins any incident with a significant impact on the continuity of an essential service provided by OESs; in other words, the incident that may entail the interruption of the essential service and thus not being operational for a given period of time.

The Directive provides specific parameters/criteria to be applied by all operators of essential services for assessing the type of incident[223]. Thus, the "classification of the incident" should be determined by:

a. The number of users that were affected by the disruption of an essential service[224];
b. The time interval that the essential service was not operational[225];
c. The geographical spread of the area that was affected by the incident[226].

[222] The least required under the NIS Directive's objectives for achieving the minimum common level of security and operational measures at EU.
[223] To assess the significance of the incident, article 14(5).
[224] Article 14(a)
[225] Article 14(b)

The mentioned-above process for classifying the incidents implies that OESs should be required to review the corresponding processes by adopting the required by the Directive parameters for the classification of incidents.

Additionally, we have already seen that Directive provides the criteria for the “classification of the impact”, at paragraph 2.2.2.

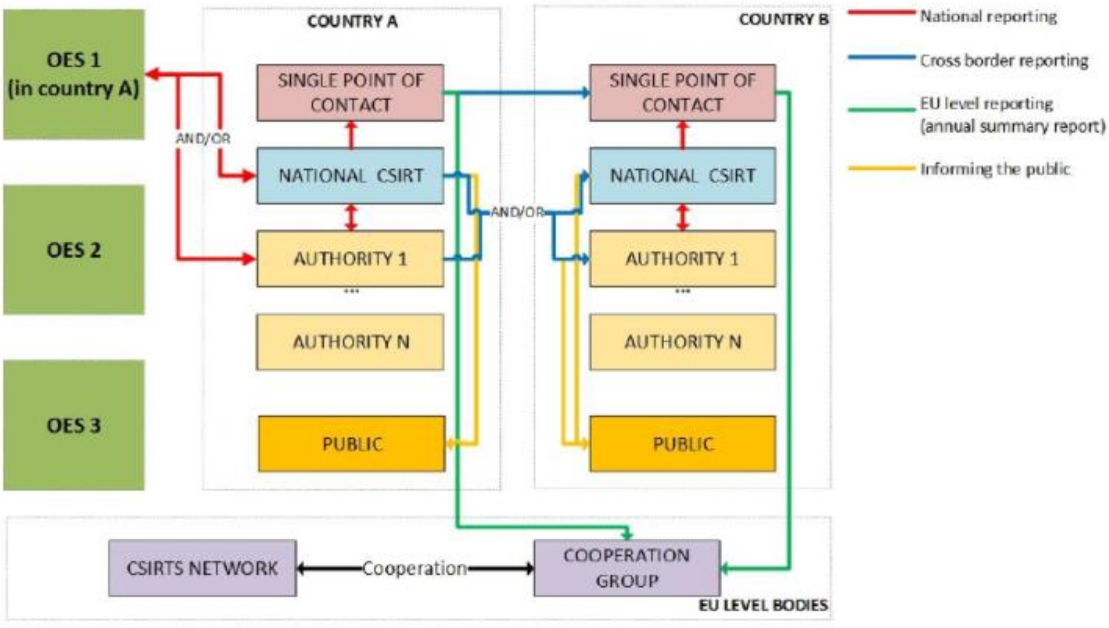
There is the possibility the same services of OESs are also provided to the other Member States. Additionally, there is also the possibility the affected services may be interconnected with other services either at the national level, or EU level. In both cases, the single point of contact (SPOC) of Member States, that notifies a significant incident, must forward the incident notification to the corresponding SPOC of the possibly affected Member State. To paragraph 2.2.3, we have already examined the process defined by the Directive for addressing the “cross-border affection”[227] between different Member States, and the outcome of this process will reveal the individual Member State with the responsibility to notify the security incident. In that case, the duplication of the reported incident is avoided.

The type of data that will be provided from the NCA or the CSIRT to SPOC for initiating the cross-border notification process, will preserve the security and commercial interest of the notifying party, as well as the confidentiality of the information provided in its notification.

Once the notification of the significant incident has been performed, NCA or CSIRT will support with incident handling assistance the notifying entity[228].

There is sometimes the necessity to communicate the incident to the public; in this situation Member States may choose either the NCA or CSIRT, after having consulted the notifying operator of essential services, to communicate the individual incident to the public, or the notifying operator itself, for raising public awareness on preventing or dealing with an ongoing incident[229].

[226] Article 14(c)
[227] Recital 24.
[228] Article 14(5).
[229] Article 14(6).



Picture 7: Overview of the incident reporting process for OESs[230].

By following the incident notification process for OESs, illustrated in picture 7 we identify the steps that should be taken by the responsible entities with this order:

1. OESs of country A may come across with a security incident.
2. OESs performs its defined “classification of incident” process, based on the parameters provided by the Directive in Article 14(4), so as to assess whether the incident should be reported to the NCA or CSIRT.
3. NCA, that receives the reported incident, should assess the significance of the impact on the provision of the essential service, by performing the “classification of impact” process defined in paragraph 2.2.2.
4. NCA additionally should assess whether other Member States may be affected[231] by the significant impact of the reported security incident by OES of country A.
5. In case the security incident should be communicated to more Member States, NCA or CSIRT forwards the reported incident to SPOC of country A, by requesting to be extended forward to the Member States that were indicated as being affected through the cross-border affection process (paragraph 2.2.3). Thus,

[230] NIS Coop-Group, Reference document on Incident Notification for Operators of Essential Services, p. 8.

[231] Perform the cross-border affection process.

SPOC of country A forwards the reported incident to SPOC of e.g. country B in order to forward it to the relative competent authority or CSIRT of country B.

6. The CSIRT will provide support to the notifying operator of essential services for handling the incident.
7. The national competent authority or the CSIRT or the notifying operator of essential services of country A will communicate the incident to the public for raising awareness purposes.
8. In the meantime, SPOC communicates with the Coop-Group for receiving guidance and support from CSIRT network for receiving the necessary for incident handling assistance, in case it is needed.

2.5.3 Member States' role as an external auditor under the incident notification requirement for OESs

National competent authorities are responsible for ensuring that OESs are compliant to their obligations as they are provided in Article 14, for taking the appropriate and proportionate security and operational measures, including documented security policies, for ensuring the state-of-the-art security level of the networks and information systems used for the provision of their essential services.

The role of national competent authorities is to serve as an external auditor to OESs with the responsibility to monitor their compliance with the NIS Directive's notification objectives. The proper and efficient function of this auditing team is highly depended on the establishment of an operational policy with the complemented strategic objectives and priorities (e.g. the educational background of personnel). This auditing team should additionally be equipped with appropriately qualified personnel complemented by the necessary capacity in numbers and facilities[232]. The Member States may determine the assessment types the competent authorities may follow during performing their tasks; usually, the auditors combine the review of existing security policies with interviewing the chief information security officer (CISO) about contingency planning[233].

[232] Article 15(1).

[233]*ENISA*, Technical guidelines on the security measures in Article 13a, p. 35, available at: https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

The operation procedures should be strictly defined covering at least:

- The roles and responsibilities of the accountable personnel[234];
- The type of the incident for ensuring interaction with relative legislation (e.g. the communication with the data protection authorities in case of incidents resulting in personal data breaches[235]);
- The identification of documented information required alongside with the purpose of requesting it[236];
- The frequency of the audits alongside with its preventive objectives [237];
- The dedicated communication channels between the relative entities; and,
- The provision of a documented report based on the evidence found through the assessment of the implemented security measures[238].

The documented report should underpin the level of compliance[239] for OESs' side (compliant-partial compliant –non-compliant); in case of partial or non-compliant national competent authority should provide a report with evidence integrated by binding instructions for OESs in order to correct or complete the missing items[240].

[234] Article 15(1).

[235] Article 15(4). *Cf. Cormack, Andrew*, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTED A Journal of Law, Technology & Society 2016, pp. 259-282.

[236] Article 15(2).

[237] Article 15(1)(2).

[238] By reviewing relative documents including descriptions of: i) policies, roles and responsibilities; ii) processes and procedures; iii) systems architecture and design; iv) test procedures and actual test results.

[239] Based on the guidance instructions by the Cooperation Group for setting the requirements for operators of essential services in accordance with article 14 of the NIS Directive.

[240] Article 15(3).

2.6 Security requirements for Digital Service Providers (DSPs)

According to the directive the term “digital service”[241] refers to the service provided under the following conditions[242]:

1. from a distance and by using electronic means;
2. at the request of the person concerned, to receive the service;
3. against remuneration.

The Digital Service Provider is defined as any legal person that provides a digital service. So, a natural person may not be considered as DSP. According to Recital 50,” hardware manufacturers and software developers” are not digital service providers[243].

The NIS Directive does not require from the Member States to identify[244] which DSPs should be set under its scope; on the contrary, it defines certain categories of DSPs.

I. The online marketplace

Article 4 (17) of NIS Directive defines online marketplaces as services that “allow consumers and traders to conclude online sales or service contracts with traders and is the final destination for the conclusion of those contracts”[245]. Intermediaries and price comparison services are excluded[246].

So, with the term online market service provider the Directive refers to the services that facilitate the economic activity of an entity with the use of electronic means[247], such as[248]:

- The state of processing transactions and aggregation of information regarding buyers, suppliers and products;
- The provision of a searching facility for appropriate products;
- The provision of products;
- The provision of special knowledge of transactions; and,

[241] Article 4(5).
[242] The legal definition according to EU 2015/1535, article 1(1)(b).
[243] See also *Holzleitner/Reichl*, European provisions for cyber security in smart grid – an overview of the NIS-directive, Elektrotechnik & Informationstechnik 2017, p. 16.
14-18
[244] Due to the cross-border nature of DSPs, recital 57.
[245] Definition of online marketplace, article 4(17).
[246] Recital 15.
[247] ICT technology.
[248] Recital 15.

- The provision of a matching capability between buyers and sellers[249].

II. The online search engine provider.

This type of provider allows users to search on all websites, independent on content and language. There is an exception, however, that provided services relating with search and price comparisons are excluded[250].

III. The cloud computing service provider

Article 4 (19) of the NIS Directive defines cloud computing service as meaning “a digital service that enables access to a scalable and elastic pool of shareable computing resources”[251]. The principle of service operation is the state that many computer users can use the same physical infrastructure - the so-called common resources - to process data on demand. These shared resources refer to any kind of hardware or software (e.g. networks, servers or other infrastructure, storage, applications and services). The computational resource can be expanded or reduced at any time, depending on the requirements of the users with automatic way, so that the resources always match as much as possible with current demand[252].

In accordance with the above mentioned, the following three main types of cloud computing provided are covered by the NIS Directive and are illustrated in picture 8:

- "Infrastructure as a Service”[253] (IaaS):
- “Platform as a Service”[254] (PaaS):
- “Software as a service”[255] (SaaS):

[249] COM (2017) 476 final, page 32.

[250] Article 4(18) and recital 16.

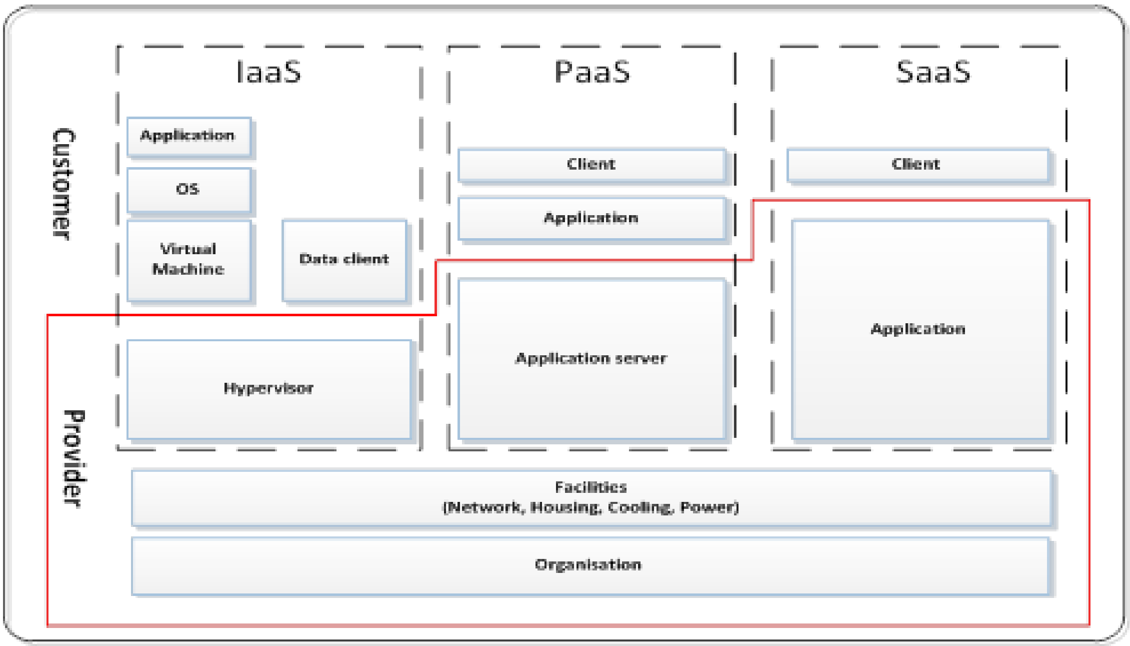
[251] For specific legal aspects of cloud security see e.g. *Kemp*, Legal aspects of cloud security, Computer Law and Security Review, 2018, pp. 22 et seq.

[252] Article 4(19) and recital 17.

[253] It provides virtual enterprise infrastructure in the form of hardware, networking and storage devices, for enabling businesses perform their daily operations; COM (2017) 476 final, p.33.

[254] It allows the companies to run either applications that already exist or to test new applications; Making the most of NIS, COM (2017) 476 final, p. 33.

[255] It is an application or software that allows the user to use it at any time and from any device via the Internet. It is not required to purchase the product in question for the user to use it; COM (2017) 476 final, p. 33.



Picture 8: Service models and assets in cloud computing[256].

2.6.1 Technical and organizational requirements for DSPs

The NIS Directive stresses that the Member States must ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services within the Union. "Having regard to the state-of-the-art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall consider the following elements[257]:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards".

[256]Making the most of NIS, COM (2017) 476 final Annex 1, p. 34.

[257] Article 16 (1) NIS Directive.

2.6.2 Sophistication level of measures

Although the risk of cyber challenges may be considered relatively new in the security area, the frantic spread of the risk with the parallel development of the technology on a fast spreading rate makes the choice for appropriate measures critical.

The EU understands that cybersecurity technology tools are developed in such a way to promote the growth of the digital economy.

On the other hand, they are also used to protect our security, our society and our democracy. Therefore, the EU considers the cybersecurity of the information systems as the highest strategic interest for the Union[258].

The information systems security refers to processes and methodologies mandatory for protecting both the system and the individual parts,[259] concerning the four basic security principles/requirements: confidentiality, integrity, authenticity and availability. The established processes are implemented by the organizations for managing security issues; therefore, these can be considered as a part of an organization's information management system.

The effectiveness of the measures depends largely on the extent on the design accuracy which involves:

- identification and monitoring;
- evaluation and comparison (testing); and
- communicating and reporting.

In accordance with the Directive's requirements, the designing process of the implemented information security measures should mandatorily include the state-of-the-art sophistication level which includes:

- continuous monitoring of implementation; and,
- structural review of implementation, taking into consideration changes, incidents, tests and exercises, to proactively improve the implementation of security measures.

[258]Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: <https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf>

[259] An information system is consisted of: humans, software, hardware, processes and data.

2.6.3 Security objectives for DSPs

The DSPs are required to prepare an Information Security Management System focused on clearly defined:

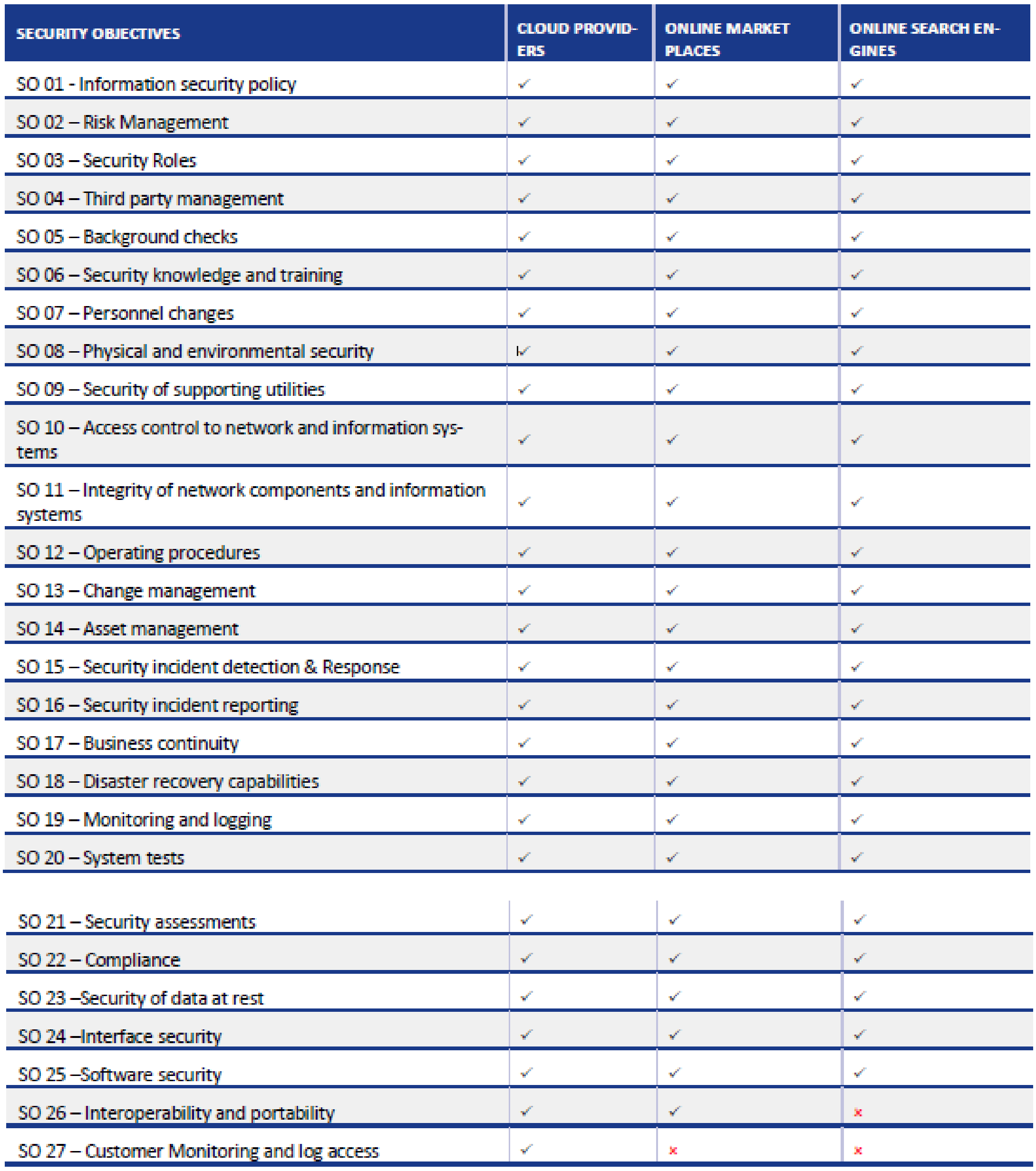
- ✓ strategic objectives;
- ✓ the ways, and
- ✓ the means,

through which the objectives could be accomplished. Pursuant to article 16(8) of NIS Directive, ENISA has prepared[260] a set of non-binding guidelines[261], to support and assist the DSPs in understanding, what should be included into their action framework during their effort to comply with the NIS Directive, regarding the technical and organization measures, as required in article 16(1).

[260] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, December 2016, available at: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

[261] The study was carried out by ENISA for the Commission's interest.

Table 3: Common security objectives for the three categories of DSPs[262].



SECURITY OBJECTIVES	CLOUD PROVIDERS	ONLINE MARKET PLACES	ONLINE SEARCH ENGINES
SO 01 - Information security policy	✓	✓	✓
SO 02 – Risk Management	✓	✓	✓
SO 03 – Security Roles	✓	✓	✓
SO 04 – Third party management	✓	✓	✓
SO 05 – Background checks	✓	✓	✓
SO 06 – Security knowledge and training	✓	✓	✓
SO 07 – Personnel changes	✓	✓	✓
SO 08 – Physical and environmental security	✓	✓	✓
SO 09 – Security of supporting utilities	✓	✓	✓
SO 10 – Access control to network and information systems	✓	✓	✓
SO 11 – Integrity of network components and information systems	✓	✓	✓
SO 12 – Operating procedures	✓	✓	✓
SO 13 – Change management	✓	✓	✓
SO 14 – Asset management	✓	✓	✓
SO 15 – Security incident detection & Response	✓	✓	✓
SO 16 – Security incident reporting	✓	✓	✓
SO 17 – Business continuity	✓	✓	✓
SO 18 – Disaster recovery capabilities	✓	✓	✓
SO 19 – Monitoring and logging	✓	✓	✓
SO 20 – System tests	✓	✓	✓
SO 21 – Security assessments	✓	✓	✓
SO 22 – Compliance	✓	✓	✓
SO 23 –Security of data at rest	✓	✓	✓
SO 24 –Interface security	✓	✓	✓
SO 25 –Software security	✓	✓	✓
SO 26 – Interoperability and portability	✓	✓	✗
SO 27 – Customer Monitoring and log access	✓	✗	✗

It is worth mentioning that according to the Technical guidelines for the implementation of minimum security measures for DSPs, all 27 identified security objectives have been derived from a set of commonly used standards[263], by DSPs in the EU's electronic communication sector.

[262] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, pp. 55-56

[263] International and national standards.

So, in accordance with table 3 the identified common security objectives[264] for all DSPs[265] is to achieve a minimum common level of resistance within EU, and are as follows:

SO. 01:Information security policy

An information security policy should be established and maintained by the digital service providers, aligned with business objectives, to address the security and continuity of the communication networks and the services provided.

In table 4 we may see examples of security measures grouped in 3 different sophistication levels: basic (level 1), industry (level 2) and state-of-the-art (level 3). The levels are cumulative. As it is expected, the next level encompasses the security requirements of the previous level.

Table 4: Security measures for ensuring the Information security policy[266].

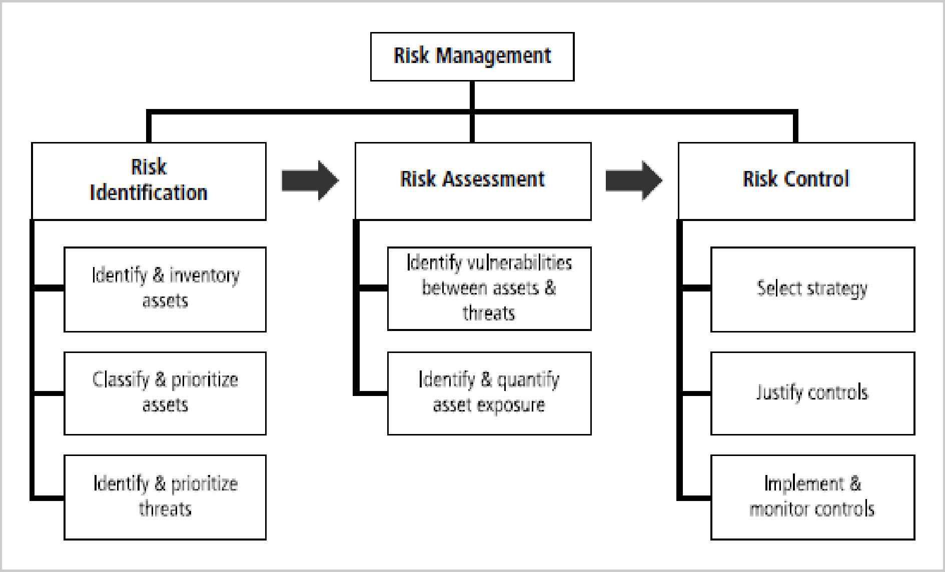
LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set a high-level security policy, which is aligned with business objectives and addresses the security and continuity of the communication networks8 and/or services provided. • Make key personnel aware of the security policy.	• Documented security policy, including networks, systems and services in scope, critical assets supporting them, and the security objectives. • Key personnel are aware of the security policy and its objectives (interview).
2	• Set detailed information security policies for critical assets and business processes. • Make all personnel aware of the security policy and what it entails for their work. • Review the security policy following incidents.	• Documented information security policy, approved by management, including applicable laws and regulations, accessible to personnel. • The information security policy is easily accessible to staff. • Personnel is aware of the information security policy and what it implies for their work (interview). • Review comments or change logs for the policy.
	• Review the information security policies periodically, and take into account significant system changes, violations, exceptions, past incidents, past tests/exercises, and incidents affecting other	• Information security policies are up to date and approved by senior management. • Logs of policy exceptions, ap-

[264] These are marked with a check mark.
[265] Included in Annex III.
[266] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 12.

3	(similar) providers in the sector	proved by the relevant roles. • Documentation of the review process, taking into account changes and past incidents. ○ Last planned review has been done according to to the review process. ○ Records of the management review. ○ Meeting minutes of review sessions. ○ Feeds and insights collected from internal security solutions and external databases

SO. 02: Risk management

A Risk Management policy should be established and maintained from the digital service providers for addressing the cybersecurity challenges to prevent, respond and mitigate the negative impact on their provided services. Although the Directive does not indicate the practical way that should be followed by the providers, however, it introduces the theoretical base of the risk management accountabilities and methodologies designed to meet strategy's requirements.


Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify & inventory assets
Classify & prioritize assets
Identify & prioritize threats
Identify vulnerabilities between assets & threats
Identify & quantify asset exposure
Select strategy
Justify controls
Implement & monitor controls

Picture 9: Components of risk management process [267].

[267] *Whitman/Mattord*, Principles of Information Security, 4th edition 2012, p. 120.

A risk management approach should consist of three stages, as it is presented in picture 9:

a. Risk identification;

b. Risk assessment;

c. Risk control.

a. **Risk identification**: during this process the relative stakeholders are invited to identify which parts of the information systems and services are critical to being protected, by considering the existing security measures, to finally produce a list of threats for each critical asset. Additionally, they should set up a procedure that evaluates the value of assets that can be either tangible or intangible.

b. **Risk assessment**: the stakeholders should correlate any existing vulnerability to each critical identified asset[268] in order to evaluate the risk level[269] of each identified threat. This process will help the company to understand the level of its preparedness[270] while preserving it as a point of reference for imposing each time appropriate security measures. This process should be repetitive[271] in order to be able to adapt to the needs that arise.

c. **Risk control**: this is the time to choose the appropriate and proportionate security mechanisms for addressing the challenges[272]. These security mechanisms should have the nature of prevention, response and mitigation of the impact.

In table 5 examples of security measures are given.

Table 5: Security measures for ensuring Risk management[273].

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Create a list of the main risks for security and continuity of the provided communication networks, systems or services, considering the main threats for critical assets. • Consider risks which stem from data protection or other sector-specific regulations or policies into the risk assessments. • Make key personnel aware of the main risks and	• List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security, continuity and privacy of networks and services. • Key personnel are aware of

[268]“Classify and prioritize assets”, during Risk Identification stage.

[269] The possibility the threat to cause damage. It is usually evaluated as: high, minimum, low.

[270] Article 16(1)(a).

[271] Article 16(1)(d).

[272] Article 16(1)(b).

[273] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 14.

	how they are mitigated.	the main risks (via interviews, ad hoc tests).
2	• Set up a risk management methodology and/or tools based on industry standards. • Ensure that key personnel use risk management methodology and tools. • Review the risk assessments following changes, security incidents or data breaches. • Ensure residual risks are accepted by management.	• Documented risk management methodology and/or tools which contains, at least: ○ Objectives, roles, and responsibilities; ○ The scope of the risk management methodology; ○ Procedures that support the risk assessment; ○ Catastrophic but improbable events that could affect the offered services. • Guidance for personnel on assessing risks. • List of risks and evidence of updates/reviews. • Review comments or change logs for risk assessments. • Management approval of residual risks.
3	• Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents	• Documentation of the review process and updates of the risk management methodology and/or tools. ○ Last planned review has been done according to to the review process. ○ Records of the management review. ○ Meeting minutes of review sessions

SO. 03: Security Roles

The DSPs should clearly define the roles and responsibilities of the designated personnel[274], complemented by specified processes.

In table 6 some examples of security measures are given.

Table 6: Security measures for defining security roles[275]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Assign security roles and responsibilities to personnel. • Make sure the security roles are reachable in case of security incidents.	• List of security roles (CISO, DPO, business continuity manager, etc.), who occupy them and contact information.
2	• Personnel is formally appointed in security roles • Make personnel aware of the security roles in your organization and when they should be contacted	• List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.). • Formal appointment of the key security roles and responsibilities. • Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	• Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents	• Up-to-date documentation of the structure of security role assignments and responsibilities. • Documentation of the review process, taking into account changes and past incidents.

[274] E.g. CSO, CISO, CTO etc.

[275] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 16.

SO. 04: Third party management[276].

The DSPs are required to establish and maintain a documented security policy, for ensuring that third parties are trained and aware of security issues[277]. The objective of this policy is to ensure that all procurement of services/products from third parties[278] are provided as they should be in accordance with the relative policy objective.

In table 7 examples of some security measures are given.

Table 7: Security measures within sophistication levels[279].

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Contractual agreements when dealing with third parties and customers have been established. • Include security requirements and relevant tasks in contracts with third-parties and customers. • Communicate residual risks which might affect the offered services to the customers. • Retain the right to perform second party audits where it is deemed necessary from a risk perspective. • Responsibilities regarding the maintenance, operation and owner-ship of assets have been defined	• List of relevant third-party contracts. • List of a customer access request. • Identify selection criteria. • Documented contractual agreements containing at least: o Service description; o Security measures; o Non-disclosure agreements; o Roles and responsibilities; o Target service levels; o Contacts and reporting lines; o The right for second party audits. • Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centres, interconnections, shared facilities, et cetera.
2	• Set a security policy for contracts with third-parties. • Ensure that all procurement of services/products from third-parties follows the policy. • Review security policy for third parties, following incidents or changes.	• Documented security policy for contracts with third parties. • Contracts for third-party services contain security requirements, in line with

[276] Article 16(5).

[277]This is a Security measure within sophistication level 1 for "security knowledge and training objective", according to the above-mentioned "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers", p. 20.

[278]There is an inventory of third-parties stakeholders identified in the relative policy.

[279] Technical guidelines for the implementation of minimum security measures for DSPs", p. 17.

	• Perform risk analysis before entering any outsourcing agreement. • Mitigate residual risks that are not addressed by the third party.	the security policy for procurement. • Past risk analysis reports. • Residual risks resulting from dependencies on third parties are listed and mitigated. • Documented third parties' contractual agreements contain special requirements in case of: o Major blackouts; o Natural catastrophes; o Accidents or other possible emergency situations; o Blackout resistance.
3	• Keep track of security incidents related to or caused by third-parties. • Periodically review and update policy for third parties and reevaluate outsourcing agreements at regular intervals, taking into account past incidents, changes, etc.	• List of security incidents related to or caused by engagement with third-parties. • Documented results of monitoring activities. • Documented results of auditing activities. • Identify the process(es) applied to manage recent changes and confirm: ○ Adequate warning to all stakeholders is provided; ○ Involves relevant personnel; ○ Includes procedures for backing-out from failed changes.

SO. 05: Background checks.

The organization's security policy will authorize the DSP to perform appropriate background checks for staff prior to recruitment, if necessary, for their duties and responsibilities, with clearly defined procedures for providing relative information.

In table 8 examples of security measures are given.

Table 8: Security measures within sophistication levels[280].

LEVE	SECURITY MEASURES	EXAMPLES
1	• Check professional references of key personnel (system administrators, security officers, guards, et cetera).	• Documentation of checks of professional references for key personnel.
2	• Perform background checks/screening for key personnel and external contractors, when needed and legally permitted. • Set up a policy and procedure for background checks. • Individuals screening criteria is established and reviewed for the organization's position	• Policy and procedure for background checks/screenings. Guidance for personnel about when/how to perform background checks/screenings. • Screening records containing at least: ○ Employment history; ○ Verification of the highest education degree received; ○ Residency; ○ Law enforcement records.
3	• Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents. • The screening process is in line with the defined policies and regulations. • Individuals are rescreened based on a defined list of conditions.	• Review comments or change logs of the policy/procedures. • Documented screening requirements. • Records of the rescreening process.

SO.06: Security knowledge and training

It is required by the DSP to verify and ensure that personnel are efficiently qualified and participate in regular security training.

In table 9 examples of security measures are given.

Table 9: Security measures within sophistication levels[281]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Regularly provide key personnel with relevant training and material on security issues. • Ensure that third parties are trained and aware of security issues	• Key personnel has followed security training and has sufficient security knowledge (interview). • Third parties have sufficient

[280] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 19.
[281] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 20

		security knowledge (interview).
2	- Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. - The program is approved by the management. - Organize training and awareness sessions for personnel on security topics important for the organization.	- Personnel have participated in awareness sessions on security topics. - Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g. training, awareness raising, etc.). - Records of individual awareness activities
3	- Contents of security training are based on assigned roles and responsibilities and specific requirements of the organization and the information system to which personnel have authorized access. - Review and update the training program periodically, taking into account changes and past incidents. - Test the security knowledge of personnel. - Contacts and communication channels with security groups and associations have been established in order to stay up to date with the latest recommended security practices, techniques, and technologies. - Provide to the organization personnel training sessions to obtain recognized security certifications	- Updated security awareness and training program. - The last planned review has been done according to to the review process. - Meeting minutes of review sessions. - List of contacts with security groups and associations. - Results of tests of the security knowledge of personnel. - Review comments or change logs for the program. - Results of the individual certification process.

SO. 07: Personnel changes process

The organization’s security policy should include this process clearly defined and documented for addressing the changes in:

- Personnel, or/and,
- their roles and responsibilities.

In table 10 examples of such security measures are given.

Table 10: Security measures within sophistication levels[282].

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Following changes in personnel revoke access rights, badges, equipment, et cetera, if no longer necessary or permitted. Brief and educate new personnel on the policies and procedures in place.	• Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, et cetera • Evidence that new personnel has been briefed and educated about policies and procedures in place.
2	• Implement policy/procedures for personnel changes, taking into account timely revocation access rights, badges, equipment. • Implement policy/procedures for education and training for personnel in new roles	• Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles • Evidence that personnel changes have been carried out according to the process and that access rights have been updated timely (e.g. checklists).
3	• Periodically check that the policy/procedures are effective. • Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents. • Automated process review access permissions that are initiated by personnel changes.	• Evidence of checks of access rights etc. Up to date policy/procedures for managing personnel changes. • Review comments or change logs. • Proof of automated process.

SO.08: Physical and environmental security

The security policy should address physical and environmental threats for protecting the datacenters of the digital service providers, by implementing security controls such as physical access controls, alarm systems and environmental controls etc.

In table 11 examples of security measures are given.

[282] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 22.

Table 11: Security measures within sophistication levels[283].

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls, to protect against unauthorized access, burglary, fire, flooding, etc. • A list of personnel with authorized access to facilities containing information systems and appropriate authorization credentials (e.g., badges, identification cards) is maintained by the organization. • Visitors are authenticated before authorizing access to the facility. • Data centre environmental conditions (e.g., water, power, temperature and humidity controls) shall be secured, monitored, maintained, and tested to ensure protection from unauthorized interception or damage.	• Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, CCTVs, et cetera. • List of personnel with authorized access. • List of authorized visitors. • Basic implementation of environmental controls.
2	• Implement a policy for physical security measures and environmental controls. • Document procedure for emergency cases • A designated official within the organization to review and approve the list of personnel with authorized access has been identified. • Visitors are escorted as required according to security policies and procedures. • Visitor's access records to the facility are maintained by the organization. • Physical access to the premises is monitored by the organization. • Industry standard implementation of physical and environmental controls.	• Documented policy for physical security measures and environmental controls, including a description of facilities and systems in scope. • Documented procedure with the specific steps to take in case of emergency. • Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases, et cetera. • Records of visitors' access to the facility. • Documented description of monitoring equipment.
3	• Evaluate the effectiveness of physical and environmental controls periodically. • Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents. • Physical access records are kept and stored in case of an audit or investigation. • Physical access records are retained as dictated by applicable regulations or based on an organization-defined period by approved policy.	• Up to date policy for physical security measures and environmental controls. • Documentation about the evaluation of environmental control, review comments or change logs. • Proof of different versions of physical access records. • Documented defined period of retention.

[283] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 24.

	- Separate facilities into different zones according to their contents.	- List with different access zones.

SO.9: Security of supporting utilities

Additionally, specified security measures should be imposed for ensuring the security of the supporting utilities (e.g. electricity). Examples of security mechanisms are given in table 12.

Table 12: Security measures within sophistication levels[284]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Ensure security of supplies, such as electric power, fuel or HVC.	- Security of supplies is protected in a basic way, for example, backup power and/or backup fuel is available
2	- Implement a policy for the security of critical supplies, such as electrical power, fuel, etc. - Implement industry standard security measures to protect supplies and supporting facilities.	- Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies. - Evidence of industry standard measures to protect the security of supplies, such as for example, passive cooling, automatic restart after a power interruption, battery backup power, diesel generators, backup fuel, etc.
3	- Advanced security measures to protect supplies. - Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents.	- Advanced implementation controls to protect the security of supplies, such as active cooling, UP, hot standby power generators, sufficient fuel delivery SLA, SLAs with fuel delivery companies, redundant cooling and power backup systems.

[284] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 26.

SO.10: Access control to network and information system

The establishment and maintenance of appropriate policies and measures for controlling the access to business resources are required for DSPs and some examples of them are given in table 13.

Table13: Security measures within sophistication levels[285]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Users and systems have unique ID's and are authenticated before accessing services or systems. • Implement (logical) access control mechanism for network and information systems to allow only authorized use.	• Access logs show unique identifiers for users and systems when granting or denied access. • Overview of authentication and access control methods for systems and users. • Documented methods of access control containing at least: ○ Authentication type; ○ Authorization schema.
2	• Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. • Based on the results of risk analysis, choose the relevant authentication mechanisms which are deemed relevant to different types of access. • Monitor access to the network and information systems, have a process for approving exceptions and registering access violations. • Security functions are restricted to the least amount of users necessary to ensure the security of the information system. • Track and monitor privileged accounts by validating their creation, use of specific authentication methods and regular reviews. • Segment information access within network and information systems based on security requirements	• Access control policy including a description of roles, groups, access rights, procedures for granting and revoking access. • Different types of authentication mechanisms for different types of access, e.g. Single-Sign-On, two-factor authentication, multi-factor authentication, etc, (including remote and WiFi mechanisms) • Log of access control policy violations and exceptions, approved by the security officer. • List of authorized users who can access to security functions. • Logs from privileged accounts' usage. • Network isolation and implementation of segmented network security zones that limit the impact of a malware incident

[285] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 27.

		- Segregation of duties control matrix. - Access control matrix.
3	- Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. - Access control policy and access control mechanisms are reviewed and when needed to be revised. - Restrictions in the number of concurrent sessions are defined and implemented by the organization.	- Reports of (security) tests of access control mechanisms - Tools for detection of anomalous usage of systems or an anomalous behaviour of systems (such as intrusion detection/prevention and anomaly detection systems). - Logs of intrusion detection10/prevention and anomaly detection systems. - Updates of the access control policy, review comments or change logs. - Real-time logging and recording of unsuccessful login attempts; - Real-time alerting when the number of defined consecutive invalid access attempts is exceeded.

SO.11: Integrity of network components and information systems

The implementation of specific technology and operational measures for protection from malware threats responsible for altering either the functionality of the systems or the integrity or accessibility of the same information are required and some examples of such security measures are included in table 14.

Table 14: Security measures within sophistication levels[286]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Make sure software of network and information systems is not tampered with or altered, for instance by using input controls. - Protect security-critical data (like passwords, shared secrets, private keys, etc.) from being disclosed or tampered with. - Take measures against malicious software on (internal) network and information systems.	- Software and data in network and information systems are protected using prevention, input controls, firewalls, encryption and signing. - Security-critical data is protected using protection mechanisms like separate storage, encryption, hashing,

[286] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 29.

		etc. • Malware detection systems are present, and up to date. • Records of recent updates of malware protection mechanisms. • Records of periodical scans.
2	• Implement industry standard security measures, providing defence-in-depth and protection against tampering and altering of systems. • The malware protection mechanisms are centrally managed. • There are mechanisms which prevent users from circumventing malware protection capabilities. • Spam protection mechanisms are employed at system entry points such as workstations, servers, or mobile computing devices on the network.	• Documentation about how the protection of software and data in network and information system is implemented. • Documented alternative countermeasures such as: ○ Securing of all physical and logical data interfaces; ○ Network isolation and implementation of segmented network security zones that limit the impact of a malware incident; ○ Comprehensive system hardening measures to minimize the risk of malware incidents. • Tools for detection of anomalous usage of systems or an anomalous behaviour of systems (such as intrusion detection/prevention and anomaly detection systems). • Logs of intrusion detection/prevention and anomaly detection systems. • Documented description of centrally management tools. • Documented spam protection mechanism. • Use of whitelisting solutions, which restrict the execution of non-approved software and code. • Interactive access to critical systems is performed using hardened hosts which have built-in controls to inhibit phishing attacks, lateral movement, and persistent compromise.
3	• Sophisticated controls to protect the integrity of	• Sophisticated controls to

	systems. - Evaluate and review the effectiveness of measures to protect the integrity of systems.	protect the integrity of systems, such as code signing, tripwire, et cetera. - Documentation of the process for checking logs of anomaly and intrusion detection/prevention systems.

SO.12: Operating procedures

These procedures are responsible for the efficient and effective way of operating the key network and information systems by personnel. Examples of security measures are given in table 15.

Table 15: Security measures within sophistication levels[287]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Set up operational procedures and assign responsibilities for the operation of critical systems.	- Documentation of operational procedures and responsibilities for key network and information systems.
2	- Implement a policy for the operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	- Documented policy for the operation of critical systems, including an overview of network and information systems in scope.
3	- Review and update the policy/procedures for the operation of critical systems, taking into account incidents and/or changes.	- Updated policy/procedures for critical systems, review comments and/or change logs.

SO.13: Change management procedures

These procedures are addressing key network and information systems changes (e.g. change and configuration procedures and processes). Examples of security measures are given in table 16.

[287] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 30.

Table 16: Security measures within sophistication levels[288]

1	• Follow predefined procedures when making changes to critical systems, according to licensing agreements • Inform the customer of significant changes to critical systems which affect the offered services.	• Documentation of change management procedures for critical systems. • Documentation of a customer update on significant changes
2	• Implement and test policy/procedures for change management, to make sure that changes in critical systems are always done following a predefined way. • Document change management procedures, and record for each change the steps of the followed procedure.	• Documentation of change management policy/procedures including, systems subject to the policy, objectives, rollback procedures, etc. • For each change, a report is available describing the steps and the result of the change
3	• Review and update change management procedures regularly, taking into account changes and past incidents.	• Up to date change management procedures, review comments and/or change logs.

SO.14: Asset management procedures

These procedures manage the assets under protection and the configuration controls for key network and information systems. Examples of security measures are given in table 17.

Table 17: Security measures within sophistication levels[289]

1	• A secure baseline configuration of components and information systems is developed, documented and maintained. • Manage critical assets e.g. software, hardware, information and configurations of critical systems.	• Documented secure baseline configuration containing at least: ○ Essential capabilities of operation; ○ Restricted use of functions; ○ Security by default; ○ Ports, protocols and/or services allowed.

[288] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, pp. 31-32.

[289] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 33.

		• List of critical assets and critical systems.
2	• Implement policy/procedures for asset management and configuration control.	• Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management • An asset inventory or inventories, containing critical assets, their owners and the dependency between assets. • A configuration control inventory or inventories, containing configurations of critical systems.
3	• Review and update the asset management policy regularly, based on changes and past incidents. • Review regularly the list with configurations and the list with critical assets based, based on changes and past incidents. • A secure baseline configuration for development and test environments is managed separately from the operational baseline configuration.	• Up to date asset management policy/procedures, review comments and/or change logs. • Documented results of the review activities. • Documented and approved exceptions to the configuration baseline containing the alternative controls in place to ensure the confidentiality, availability and integrity of the information system. • Documented secure baseline configuration for development and test environments.

SO.15: Security incident detection & Response procedures

These procedures are addressing the detection and response to security incidents appropriately and should promote the mitigation, recovery and remediation from a security incident providing also an educational indicator. Examples of security measures are given in table 18.

Table 18: Security measures within sophistication levels[290]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set up processes or systems for incident detection and response. • Make sure personnel is available and prepared to manage and handle incidents.	• Past incidents were detected and timely forwarded to the appropriate people, including customers. • Personnel is aware of how to deal with incidents and when to escalate. • Inventory of major incidents and per incident, impact, cause, actions taken, and lessons learnt.
2	• Implement industry standard systems and procedures for incident detection and response. • Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	• Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, security helpdesk for personnel and customers, reports and advisories from Computer Emergency Response Teams (CERTs), tools to spot anomalies, et cetera. • Policy/procedures for incident detection and response, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (CISO e.g.), et cetera. • Management commitment to the incident response program. • Records of individual training activities. • Description of the incident handling capability containing at least the following procedures: o Preparation; o Detection; o Analysis; o Containment; o Mitigation; o Recovery.

[290] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 34.

3	- Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate and reduce time to react to any future occurrence of this type of incident or data breach. - Review systems and processes for incident detection and response regularly and update them taking into account changes and past incidents. - Regular cyber exercises and related results to test the incident response effectiveness are scheduled and documented.	- Individual reports of the handling of major incidents. - Up to date documentation of incident detection and response systems and processes. - Documentation of review of the incident detection and response processes, maximum response times, review comments, and/or change logs. - Records of cyber exercises.

SO.16: Security incident reporting procedures

The DSPs should define these procedures for communicating the security incidents. Examples of such type of security measures are given in table 19.

Table 19: Security measures within sophistication levels[291]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	- Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.
2	- Implement policy and procedures for communicating and reporting about incidents.	- Documented policy and procedures for communicating and reporting about incidents, describing reasons/motivations for communicating or reporting (business reasons, legal reasons etc.), the type of incidents in scope, the required content of communications, notifications or reports, the channels to be used, and the roles responsible for communicating, notifying and reporting. - Templates for incident reporting and communication.

[291] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 35.

	- Evaluate past communications and reporting about incidents. - Review and update the reporting and communication plans, based on changes or past incidents.	- List of incident reports and past communications about incidents - Up to date incident response and communication policy, review comments, and/or change logs.

SO.17: Business continuity

The business continuity plan ensures the continuity of the services offered. Examples of some security measures are given in table 20.

Table 20: Security measures within sophistication levels[292]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Implement a service continuity strategy for the communications networks and/or services provided.	- Documented service continuity strategy, including recovery time objectives for key services and processes. - Management commitment with the continuity strategy.
2	- Implement contingency plans for critical systems. - Monitor activation and execution of contingency plans, registering successful and failed recovery times.	- Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives. - The decision process for activating contingency plans. - Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time.
3	- Review and revise service continuity strategy periodically. - Review and revise contingency plans, based on past incidents and changes. - The continuity of operations plan is tested and updated on a regular basis. - Personnel involved in the continuing operations	- Up to date continuity strategy and contingency plans, review comments, and/or change logs. - Documented results of the continuity of operations test activities.

[292] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 38.

	plan are trained in their roles and responsibilities with respect to the information system and receive refresher training on an organization-defined frequency.	• Records of individual training activities

SO.18: Disaster recovery capabilities

The ability to assist an organization to overcome a natural or/and major disaster should be provided by setting up clear lines of recovery procedures for initiating the established business contingency plan. Examples of such type of security measures are given in table 21.

Table 21: Security measures within sophistication levels[293]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Prepare for recovery and restoration of services following disasters.	• Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, et cetera.
2	• Implement policy/procedures for deploying disaster recovery capabilities. • Implement industry standard disaster recovery capabilities or be assured they are available from third parties (such as national emergency networks).	• Documented policy/procedures for deploying disaster recovery capabilities, including a list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). • Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, et cetera.
	• Advanced implementation controls for disaster recovery capabilities to mitigate natural and/major	• Advanced implementation controls for disaster recov-

[293] ENISA, Technical guidelines for the implementation of minimum security measures for DSPs, pp. 39-40.

3	disasters. • Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	ery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. • Data centre infrastructure/design is designed for availability, auto failover, and resiliency to maintain service to customers. • Updated documentation of disaster recovery capabilities in place, review comments and/or change logs.

SO.19: Monitoring and logging

The organization should establish and maintain procedures and systems responsible for monitoring and logging of the offered services. Examples of security measures are given in table 22.

Table 22: Security measures within sophistication levels[294]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Implement monitoring and logging of critical systems.	• Logs and monitoring reports of critical network and information systems
2	• Implement a policy for logging and monitoring of critical systems. • Set up tools for monitoring critical systems. • Set up tools to collect and store logs critical systems.	• List of auditable events. • Audit records containing at least: • Date and time of the event; ○ Component of the information system where the event concurred; ○ Type of event; ○ User/subject identity; ○ The outcome of the event. • Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. • Tools for monitoring sys-

[294] Technical guidelines for the implementation of minimum security measures for DSPs", pp. 40-41.

		tems and collecting logs. - List of monitoring data and log files, in line with the policy.
3	- Set up tools for automated collection and analysis of monitoring data and logs. - Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	- Tools to facilitate structural recording and analysis of monitoring and logs. - Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

SO.20: *System tests*

The organization should establish and maintain appropriate procedures responsible for testing critical network and information systems. Examples of security measures are provided in table 23.

Table 23: Security measures within sophistication levels[295]

LEVEL	SECURITY MEASURES	EXAMPLES
1	- Test networks and information systems before using them or connecting them to existing systems. - The installation or de-installation of patches is done in an ad hoc manner.	- Test reports of the network and information systems, including tests after big changes or the introduction of new systems. - Checks for latest patches
2	- Implement policy/procedures for testing network and information systems. - Implement tools for automated testing. - The installation or de-installation of patches is done periodically in an organized manner.	- Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates. - Documented testing activities containing at least: ○ Objectives, roles, and responsibilities;

[295] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 42.

		○ The scope of the plan; ○ Detailed results of the execution of the plan; ○ The frequency of the test. • Approved documented actions applying patches.
3	• Review and update the policy/procedures for testing, considering changes and past incidents. • The installation or de-installation of patches is reviewed to ensure the adequate implementation of the defined actions. • Exceptions to defined actions and approved mitigating actions are identified and documented.	• List of test reports. • Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

SO.21: Security assessments

The organization/company should establish and maintain appropriate procedures-methodologies for performing security assessments of critical assets. Examples of security measures are provided in table 24.

Table 24: Security measures within sophistication levels[296]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. • Vulnerabilities are monitored and assessed.	• Reports from past security scans and security tests. • Documented vulnerability scans reports.
2	• Implement policy/procedures for security assessments and security testing. • A single point of contact and communication channels for information security related issues with manufacturers or vendors have been identified.	• Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests, frequency, approved parties (internal or external), confidentiality

[296] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 43.

		levels for assessment and test results and the objectives security assessments and tests. • List of manufactures single point of contact.
3	• Evaluate the effectiveness of policy/procedures for security assessments and security testing. • Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents. • Information obtained from the vulnerability scanning process is shared with designated personnel throughout the organization and authorities to help eliminate similar vulnerabilities in other information systems.	• List of reports about security assessments and security tests. • Reports of follow up actions on assessments and test results. • Up to date policy/procedures for security assessments and security testing, review comments, and/or change log. • Records of vulnerabilities information sharing

SO.22: Compliance

The organization/company should establish and maintain[297] a policy which involves, checking the compliance of the internal policies in contrast with the national and EU legal requirements and industry best practices and standards. Examples of security measures are provided in table 25.

Table 25: Security measures within sophistication levels[298]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Monitor compliance to standards and legal requirements.	• Reports describing the result of compliance monitoring.
2	• Implement policy/procedures for compliance monitoring and auditing	• Documented policy/procedures for monitoring compliance and auditing, including what

[297] Through a formal review process on a regular basis.

[298] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 45.

		(assets, processes, infrastructure), frequency, guidelines who should carry out audits (in- or external), relevant security policies that are subject to compliance monitoring and auditing, the objectives and high level approach of compliance monitoring and auditing, templates for audit reports. - Detailed monitoring and audit plans, including long-term high-level objectives and planning.
3	- Review and update the policy/procedures for testing, taking into account changes and past incidents. - The installation or de-installation of patches is reviewed to ensure the adequate implementation of the defined actions. - Exceptions to defined actions and approved mitigating actions are identified and documented.	- List of all compliance and audit reports ○ Root cause analysis to the compliance and audit reports. - Remediation plans for critical assets. - Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

SO.23: Security of data at rest

The organization/company should establish and maintain appropriate security mechanisms for protecting the data at rest. Examples of security measures are given in table 26.

Table 26: Security measures within sophistication levels[299].

LEVEL	SECURITY MEASURES	EXAMPLES
	- Identify the most critical data taking into account relevant business needs and legal obligations (e.g. with regard to the processing of	- The access control, sharing, copying, transmittal and distribution of confidential and

[299] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 46.

1	personal data). • Retain the critical data for a certain period depending on the type of data and its criticality • Implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas and in transit when moving within and between company data locations. • Implement cryptographic mechanisms such as digital signatures and hashes to detect unauthorized changes to critical data at rest. • Implement mechanisms for the secure disposal of the data after their lawful use.	restricted data are defined • Safeguards to protect the secrecy of secret (private) key(s) are in place • Limited or ad hoc processes exist to protect electronic media • Evidence from regular reviews of devices/storage media to examine that data is removed or securely overwritten prior to disposal.
2	• Classify all data according to a classification scheme which takes into account data's value, legal requirements, sensitivity, and criticality to the organization. • Use of removable media is prohibited unless strictly required. • Ensure the confidentiality and integrity of data at rest according to the classification scheme. • Establish a policy around confidentiality and integrity of data at rest and make all personnel to whom it is relevant, are aware of the policy and procedure and what it implies for their work. • Set detailed cryptographic key establishment and management policies and procedures for data at rest (only if cryptography has been implemented). • A set of best practice procedures are in place for the secure disposal of physical assets.	• Data retention policy exists and is complete • Formal standard to govern the protection of electronic transportable media is in place. Encryption enforced on electronic media identified with confidential information. • Evidence for the existence of mechanisms which support in ensuring confidentiality and integrity of the data at rest such as cryptographic mechanisms, file share scanning, secure offline storage, removal of sensitive data from storage media etc. according to the classification scheme. • Evidence of the existence of a mechanism (either manual or automated) for the establishment and management of cryptographic keys (only if cryptography has been implemented). • Obtain evidence of written authorization to dispose of equipment from Department Head. A disposal form should be completed.
3	• Classify all assets according to the classification scheme. • Implement information labelling and handling procedures in accordance with the classification scheme • The data retention policy considers the value	• Labelling of information of information is reviewed on a regular basis • The data retention policy is supported by a comprehensive data retention schedule, which

	of data over time and the data retention laws the organization may be subject to. • Strong controls are in place surrounding connection of media devices. • Use automated key management mechanisms. • Review of confidentiality and integrity of data at rest policy. • Disposal of assets at the most opportune time in line with company objectives, strategy and the data retention policy, using the most appropriate methods.	contains the retention period for each type of data used by the organization • Reports of the data retention policy and configuration which ensure that they are in line with requirements and good practices • Technology infrastructure automatically encrypts and protects electronic transportable media in the environment. • Portable media standards are reviewed at least annually and on an ad hoc basis for any new technology or threats. • Evidence that the public-key encryption and secret key of user and cypher-text are based on the subject's attributes. • Documentation of the review process, taking into account changes and past incidents. Review the policy on a regular basis • Personnel is aware of the confidentiality and integrity of the data at rest policy and procedures and what it implies for their work (interview). Review comments or change logs for the policy and/or procedure. • Evidence of secure key generation, use, storage and destruction of data. • The rationale for disposal of assets and the methods used is provided. Review of physical asset inventory. All devices leaving the controlled environment must be purged of data using disk wiping utilities or degas-sing methods (reformatting is not enough)

SO.24: Interface security

An appropriate policy should be established and maintained by the organization/company for ensuring the protection of the interfaces of services which use personal data. Examples of such type of security measures are provided in table 27.

Table 27: Security measures within sophistication levels[300]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set a high-level security policy for keeping the cloud and online market interfaces secure • Make key personnel aware of the security policy. • Enable secure channels for data transmission (e.g. TLS2.0) • Use unique identifiers to identify users	• Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. • Key personnel are aware of the security policy and its objectives (interview). • At least one secure channel is enabled. • All customers are assigned to a unique identifier.
2	• Set detailed security policies for data security to include protection of customer administration interfaces (TLS2.0, 2-Factor authentication) etc. • Make all personnel aware of the security policy and what it implies for their work. • Review the security policy following incidents. • Implement 2-Factor authentication	• Documented security policies, approved by management, including applicable law and regulations, accessible to personnel. • Personnel is aware of the security policy and what it implies for their work (interview). • Review comments or change logs for the policy.
3	• Review the security policy periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	• Security policies are up to date and approved by senior management. • Logs of policy exceptions, approved by the relevant roles. • Documentation of the review process, taking into account changes and past incidents.

[300] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 49.

SO.25: Software security

The development of software should be ensured through the designing process[301]. Examples of security measures are given in table 28.

Table 28: Security measures within sophistication levels[302]

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Establish guidelines for maintaining software security	• Documented guidelines, to ensure that software security is maintained. • Key personnel are aware of the guidelines and its objectives (interview).
2	• Implement a defined set of security measures to secure development environments, including measures for protecting test data. • Depending on the type of requirement include software testing methods (e.g. black-box, ad-hoc testing). • Keep separated environments for development purposes, testing purposes and production.	• Evidence of the test results to secure development environments, including measures for protecting test data are maintained. • Evidence of the software testing methods chosen for a particular test scenario and explanation of this. • Evidence of separated environments for development, testing and production.
3	• Security by design is tested at various stages of the SDLC prior to Go-live utilizing independent tools and a self-service testing platform throughout SDLC. • Results of application assessments are used to regularly enhance developer training and the SDLC process.	• Test results of each phase of the SDLC are maintained and are up to date. Test results are maintained and approved by senior management • Documented evidence of the review process of the patch development process, security training for software developments and secure by design software configurations • Evidence that a software

[301] In case that software development is outsourced the DSP should take provisions to include Software Lifecycle Agreements (SLA) as an essential part of the procurement process.

[302] *ENISA*, Technical guidelines for the implementation of minimum security measures for DSPs, p. 50.

		testing method is chosen at each stage of the software development lifecycle

For each of these security objectives, the specifically dedicated security measures (ways) and means listed in the above tables provide also evidence for their implementation, according to international and national security standards. It should be reminded that the Directive is concerned about the theoretical background of the choice of measures and not for the practical issue as such. Each stakeholder may adopt such security measures that follow the NIS Directive's objectives, i.e. a high common level[303] of information systems and networks security within EU.

2.6.4 Notification requirement for digital service providers

The digital service providers, defined by the NIS Directive in Annex III, are required to report any incident having a substantial impact on the provision of their services to the national competent authorities or the CSIRT, only in the following situations:

- The provider has access to all this information required to report an incident so that the reporting can be done properly[304];
- The provider is not considered a micro and small digital service provider[305], otherwise, it will be excluded from implementing the incident notification provisions.

The criteria that are provided by the NISD in case any of the three basic principles of information security has been compromised (confidentiality, integrity and availability) for assessing the type of the impact that the security incident poses on the provision of their services, which are based on the five parameters found in Article 16(4) NIS Directive:

a. "The number of users affected by the incident, in particular users relying on the service for the provision of their own services";

b. "The duration of the incident";

[303] The so-called "state of the art" level of security.
[304] Article 16(4).
[305] Article 16(11).

c. “The geographical spread with regard to the area affected by the incident”;
d. “The extent of the disruption of the functioning of the service”;
e. “The extent of the impact on economic and societal activities”.

For enabling a coherent European implementation of thresholds for the above parameters, by different stakeholders under similar circumstances, the Commission[306] issued the Commission Implementing Regulation 2018/51[307], in which establishes a set of incident notification provisions for adopting common thresholds for common parameters.

According to Article 4 of the Implementing Regulation 2018/51, the thresholds for assessing an incident as substantial are:

a. The incident caused an unavailability of the core service more than 5 000 000 user hours, whereby the term user hour refers to the number of affected users in the EU for a duration of sixty minutes.
b. The incident caused a loss of confidentiality, integrity or authenticity of data or services affecting more than 100 000 users.
c. The incident created risks for public safety, public security or of loss of life.
d. The incident caused damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000000.

So, the digital service providers should consider the above-defined thresholds while assessing and defining the classification process of the impact of any incident. However, it should be noted the Implementing Regulation is silent about the case of an incident to a digital service used in the context of essential services[308].

The DSPs have the right to impose additional measures in case there is a need to ensure national security and to facilitate the investigation, detection and prosecution of criminal offences; if any reported incident is related to criminal activities, it should be reported to law enforcement authorities[309]. In contrast to OESs, DSPs are imposed to a “light-

[306] The Commission was empowered pursuant to Article 16(8).
[307] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.
[308] *Porcedda*, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Computer Law & Security Review 2018, p. 10.
[309] Recital 62: “Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA”.

er-touch" approach concerning their security requirements. More specifically, Member States are not allowed to impose any further security or notification requirements on DSPs; on the contrary, the minimum-security requirements for DSPs should be lighter than those of the OES, and they should remain free to take the measures that they deem appropriate.

Additionally, a light-touch approach is provided to DSPs in case of jurisdiction issues. The DSP must report the incident to the Member State (to the national competent authority or the CSIRT) where it has its main establishment[310]. There is, however, the possibility that the DSP offers services in the EU without having the infrastructure established in the EU territory[311]. In that case, the DSP should designate a representative in the Union. The representative may be chosen between one of those Member States where its services are offered[312].

2.6.4.1 General notification of incident scheme for DSPs

Diagram 3 describes the notification process of an incident. In the case of an incident, the DSPs should assess the impact[313] regarding the provision of the service. If it is about a substantial impact, then the DSP is required to report the incident. But primarily the provider should assess whether the operational status of an operator of essential services is based on its technology infrastructure, so the provision of essential services is affected negatively. In that case, the report of the incident will be performed by the operator of essential services under the defined notifying requirements by the Directive[314]. Otherwise, the digital service provider will - without undue delay - notify the competent authority or the CSIRT, where its main establishment or its designated representative is located[315]. This implies that the startup notifying time of the incident will be the moment that there has been an indication that the provision of the service has been affected[316]. Such an indicator may be e.g. a report from a user or even through a self-check activity by personnel or software.

[310] Article 18(1) and recital 64.

[311] Article 18(2) and recital 65.

[312] *ENISA*, Incident notification for DSPs in the context of the NIS Directive", FEBRUARY 2017, p. 10, This interpretation of the light-touch approach was presented by Commission's representatives, during ENISA's Network and Information Security Workshop in Bratislava, 17-18.10.2016.

[313] The DSP will execute the algorithm used for the classification of impact (the five parameters).

[314] Article 16(5).

[315] Article 17(3).

[316] Without undue delay.

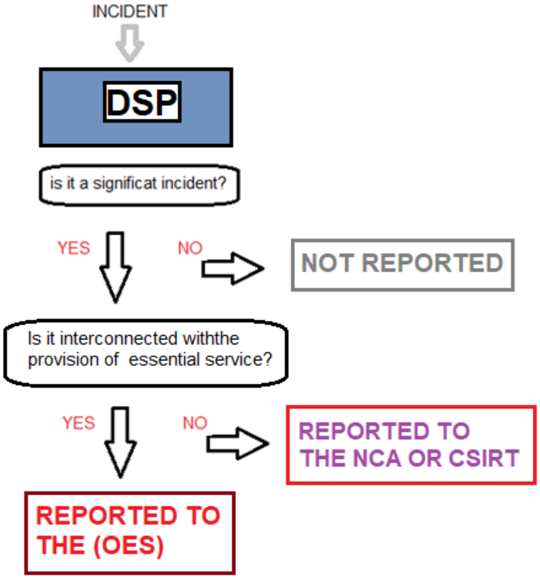

INCIDENT
DSP
is it a significat incident?
YES
NO
NOT REPORTED
Is it interconnected withthe provision of essential service?
YES
NO
REPORTED TO THE NCA OR CSIRT
REPORTED TO THE (OES)

Diagram 3: Incident notification process for DSPs.

The form template of the information data that will be communicated through the notification process should include:

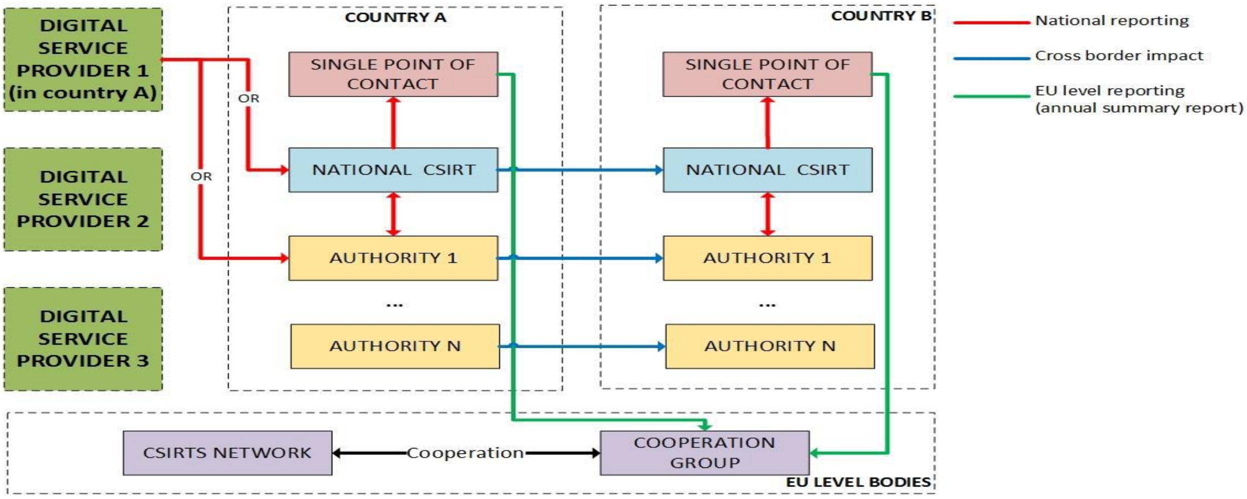
- The starting time;
- The ending time[317];
- The name of the notifying person;
- The description of the incident in terms of what systems and/or services were affected negatively.

All these incident details will help the competent authority to assess which other countries should be informed (in case of cross-border impact affection)[318].

If the nature of the incidents' impact arises public awareness then it is strictly required that the public is informed[319] either from the provider or from the competent authority, within the meaning of preventing or responding to an on-going incident.

[317] In case the incident has been handled successfully, then the duration of the incident may be used e.g. for statistical reasons.
[318] Article 16(6).
[319] Article 16(7) and recital 67.

2.6.4.2 The incident notification as part of the overall incident management process



Picture 10: The overall incident notification process at EU level320.

By examining the picture 10 we may understand the incident notification process for the digital service providers as following:

1. The DSP of country A may come across with a security incident;
2. The DSP performs its defined “classification of incident” process, based on the parameters provided by the Directive in article 16(4), to assess whether the incident should be reported;
3. The digital service provider should assess any probable interconnection with the provision of essential services as defined in article 16(5);
4. The digital service provider of country A reports the incident to the NCA or the CSIRT of its main establishment or that of its representative [321];
5. In case the security incident should be communicated to more Member States, the competent authority or CSIRT forwards the reported incident to the SPOC of country A by requesting to be extended forward to the Member States that were indicated as being affected through the cross-border affection process. Thus, the

[320] Incident notification for DSPs in the context of the NIS Directive FEBRUARY 2017, p. 18.
[321] Article 17(3).

SPOC of country A forwards the reported incident to the SPOC of e.g. country B in order to forward it to the relative competent authority or CSIRT of country B[322];

6. The CSIRT will provide support to the notifying digital service provider for handling the incident;
7. The NCA or the CSIRT or the digital service provider of country A will communicate the incident to the public for raising awareness purposes[323];
8. In the meantime, the SPOC communicates with the Coop-Group for receiving guidance and support from the CSIRT network for receiving the appropriate information for handling the incident in case it is needed.

2.6.5 Requirements for the Member States concerning the DSP notification requirement

The national competent authorities are responsible for ensuring that the digital service providers are compliant with their obligations as they are indicated in Article 16, for taking the appropriate and proportionate security and operational measures, including documented security policies for ensuring the state-of-the-art security level of the networks and information systems used for the provision of their services.

The role of the national competent authorities is to serve as an external "*ex-post* supervisor" - auditor to the DSPs with the responsibility to monitor their compliance with the NIS Directive's notification objectives[324]. Pursuant to the light-touch approach of non-compliance to the requirements of Article 16, the digital service provider would be audited by its national competent authority in case there is evidence provided by the competent authority from a different Member State, where also the service is provided[325].

In this respect, a similar operational policy with the auditing team responsible for supervising the operators of essential services should be established and maintained to support the proper and efficient function of this process, including[326]:

- Educational requirements for the personnel;

[322] Article 16(6).

[323] Article 16(7).

[324] This is an additional element that supports the light-touch approach concerning the DSPs' security requirements.

[325] Article 17(1).

[326] In terms of article 17(2)(a).

- Defined capacities of human resources and facilities;
- Type of assessment;
- Operational procedures with clearly defined:
  - ✓ roles and responsibilities;
  - ✓ the type of the incident for ensuring interaction with relevant legislation;
  - ✓ the identification of documented information required alongside with the purpose of requesting it;
  - ✓ the frequency of the audits alongside with its preventive objectives;
  - ✓ the dedicated communication channels between the relative entities; and,
  - ✓ the provision of a documented report based on the evidence found through the assessment of the implemented security measures.

The documented report should underpin the level of compliance of the digital service provider. In the case of partial compliance or even worse non-compliance, the competent authority should provide guidance to the digital service provider for remediation treatment[327].

2.7 Final provisions,

Chapters VI and VII of the NISD include the last general provisions aiming to facilitate and achieve a coherent implementation approach of the NIS Directive within the EU while promoting the incident notification requirement between voluntary and obliged CI stakeholders. More specifically:

- ➢ The EU intention is to promote the convergent application of cybersecurity measures within identified OESs and certain defined DSPs without imposing specific technological products. For this reason, the use of European or internationally accepted standards and specifications on the security of networks and information systems is supported[328].
- ➢ The rest CI that do not belong into identified OESs and certain defined DSPs may choose to report events with significant operational implications on the continuity of their provided services on a voluntary basis without having the obliga-

[327] Article 17(2)(b).
[328] Article 19.

tion to take additional security measures. However, the competent authorities should give priority to mandatory notifications and then to volunteers without causing disproportionate or unnecessary burdens for the Member States concerned[329].

- The Member States should impose sanctions on a natural and legal person in the event of any breach of the provisions of this law and should have communicated them to the European Commission by 9/5/2018330.
- The Coop-Group and CSIRT network have initiated their tasks as of 9/2/2017.
- The Commission will periodically review the implementation of this Directive at operational and strategic level, by submitting a relevant report including an inventory evaluation taking into account the reports of the cooperation group and the CSIRT network on the experience gained at strategic and operational levels. The first report will be submitted by 9 May 2021[331].
- Until 9/11/2018 important assistance has been provided to the Member States regarding the process of identifying OESs[332].
- Until 9/02/ 2017, Member States should have designated appropriate representation in the cooperation group and the CSIRT network.

[329] Article 20.
[330] Article 21.
[331] Article 23.
[332] Article 24.

3 Evaluation of NIS Directive's context

The implementation of the NIS Directive comes at a significant moment of a global change in the security area of ICT systems against new emerged cyber threats. The technological development in the way information is managed and handled through networked facilities[333], makes it imperative to harmonize the European Union with the two new cyber regimes in the United States: The National Cybersecurity Protection Act of 2014[334] and the National Cybersecurity and Critical Infrastructure Protection Act of 2014[335].

More specifically:

1. The NIS Directive sets up the new conception of security approach[336], the so-called security by design. The security objectives, regarding the networks and information systems, should include:
    A. Management of the security risk;
    B. Protection[337] against cyber-attacks;
    C. Detection of cybersecurity events;
    D. Deterring the impact of cybersecurity incidents.

2. The security measures required for incident handling while notifying the significant security incidents for the identified OESs and DSPs both formalize a revolutionary change in the cybersecurity conception.
3. Concerning the incident handling obligations, the new security conception includes the implementation of a risk assessment process for identifying threats coming from intentional and unintentional actors against the information sys-

[333] The way we create, store and consume data

[334] The National Cybersecurity Protection Act, PUBLIC LAW 113–282—DEC. 18, 2014.

[335]The National Cybersecurity and Critical Infrastructure Protection Act H.R.3696 — 113th Congress (2013-2014).

[336]*Myriam Dunn Cavelty, Victor Mauer, Sai Felicia Krishna-Hensel*, Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.

[337] In terms of responding to threats.

tems and network infrastructures. Through the Risk Assessment, the relevant stakeholders will be able to understand how prepared they are against new emerged threats and decide on what type of additional operational and technical measures they should take for managing the risk.

4. Particularly interesting is the introduction of an incident notification scheme, given the fact that there were no laws requiring incident reporting since the enactment of the NISD.

   For example, in case an attack occurs, traditional ways do not provide for an immediate reaction. This incident handling approach may carry risks of loss of critical data due to intentional or unintentional malicious activities coming from both inside or outside an organization.

   So, the incident notification obligation without undue delay is considered quite revolutionary in the information era; it actually reveals the way the EU is exposed to cyber risks while extending its knowledge on the actual cyber-threat landscape and promoting an effective handling of them.

5. The tougher obligations imposed to organizations[338] in case of not being compliant to NIS Directive's obligations, the more positive dynamism is added in updating and upgrading their cybersecurity capabilities at the national level.

6. The establishment of general provisions on key operational issues seems to be quite strategic in handling any jurisdiction and responsibility issue[339]. More specifically, the legislator focuses on achieving a coherent approach[340] within EU, without leaving any margin of misunderstanding and overlaps between the relevant stakeholders. Given the complexity of the issue, since many responsible actors are involved, there is a need for a simple but quite strategic plan for counterfeiting the cybersecurity risks posed on networks and information systems and providing the standards on achieving preparedness, resilience and deterring of such threats. The simpler a system is the more effective approach we may follow.

[338] Performed by establishing binding laws to serve as a penalty measure.

[339]Such as between Member States, relevant Stakeholders of CI and relevant issued legislation at national level.

[340] *Helena Carrapico and Andree Barrinha,* The EU as a Coherent (Cyber)Security Actor?

7. The adoption of a National Cyber Security Strategy (NCSS) serves as a tool for strengthening the role of the State in forcing the establishment of an advanced security level on the CI of both public and the private sector.
8. The issues that harden the strategy making the decision are distinguished into three categories:
   1. The globally interconnected information systems demonstrate the limitations and ineffectiveness of previous security fragmented and with significant differences in maturity level approaches taken by individual countries;
   2. The proposed responses by the strategy[341] to control or regulate the risks would impact the freedom of expression value that underlies the cyber revolution
   3. The constant appearance of new and more sophisticated threats that may be identified yet at the time of the incident.
9. Taking into consideration the complexity hidden into the new dynamics of the strategy[342] field, a need for a metadata hands-on approach by promoting a governance rationale for all owners of critical infrastructure is required[343].
10. The proposed security approach focuses on both of the following views:
    - system and
    - people[344].

    As mentioned in Chapter 1 of the thesis, an information system consists of the following elements: procedures, software; data[345], people and hardware utilities.

    The fact that human errors are considered as key factors on causing security problems either intentionally or unintentionally, introduces the need to monitor and record the behaviour of the system from two different aspects, aiming to achieve better and holistic strategy on cybersecurity of the networked ICT infrastructures. In this sense, Critical Infrastructure stakeholders are required to develop, implement and maintain a Cyber Security System Management (CSSM)

[341] The action framework activities included in the content of the strategy.
[342] *C. F. Kurtz D. J. Snowden,* The new dynamics of strategy: Sense-making in a complex and complicated world.
[343]*George Christou,* Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,
[344] User, personnel.
[345] In terms of information and services.

including a range of policies and procedures taken by organizations for systematically managing organization's sensitive data aiming to minimize and ensure business continuity, by pro-actively addressing not only risks evolving from particular implemented technological products but also risks originated from physical and environmental threats (e.g. a physical threat may be an employee’s behavior to not follow the defined security process for data in transit or at rest). The efficient and effective protection of networks and information systems requires a balanced handling between security measures and residual risk[346] in order to satisfy each of the above-mentioned objectives.

11. Information-sharing among private and public stakeholders is a powerful mechanism to better understand the constantly changing environment. In this sense, owners of critical infrastructures could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of national security[347]. Combining both views gives a very powerful insight into how the threat landscape evolves.

12. The purpose of having a CSIRT is an effective operational security measure and involves:

    - Centralized and specialized[348] handling of IT security incidents reported from various types of CSIRTs[349],
    - "Dealing with legal issues and preserving evidence in the event of a lawsuit”[350];
    - Consistent awareness and knowledge gained on technical and organizational security approaches;
    - Encouraging cooperation[351] within the different entities on IT security issues.

[346] The threat that remains after all efforts done to identify and mitigate risk, such as: to reduce it, to avoid it or to transfer it (e.g. to an insurance company).

[347] Based on their implemented network security tools.

[348] By providing expertise in assisting the relevant stakeholders to quickly recover and return to normal operations.

[349] There are many types of CSIRT, such as: Academic Sector CSIRT, Commercial CSIRT, CIP/CIIP Sector CSIRT, Governmental Sector CSIRT, Internal CSIRT, Military Sector CSIRT, National CSIRT, Small & Medium Enterprises (SME) Sector CSIRT, Vendor CSIRT; see further details in *ENISA*, A Step-by-step Approach on how to set up a CSIRT, p. 9.

[350] *ENISA*, A Step-by-step Approach on how to set up a CSIRT, p. 8.

More specifically, in case of an incident handling, at least two or more security analysts typically collaborate such as:

- Within a CSIRT;
- Between teams within an organization;
- Between different organizations.

For example, a national CSIRT collaborates with CSIRTs from other countries to handle incidents. Although software and hardware security products are considered as critical components for cyber defence purposes, so are the social processes followed between related entities during the incident handling procedure. In other words, cybersecurity incident failures may occur not only due to technological breakdowns[352] but also due to poor coordination and collaboration[353].

13. Hardware and software-based network security tools[354] are required to be implemented by CI stakeholders including:
    - Firewall;
    - Encryption tools;
    - Traffic monitoring tools;
    - Rootkit detection tools[355];
    - Application-specific scanner;
    - Vulnerability scanner;
    - Port scanner;
    - Intrusion detection system;
    - Packet crafting tools[356];

[351] By building awareness.

[352] *Abrams, M., & Weiss, J.,* Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia. National Institute of Standards and Technology, Computer Security Division (2008)

[353] Organizational scientists have noted, "failures of team leadership, coordination, and communication are well documented causes of the majority of air crashes, medical errors, and industrial disasters", *Kozlowski &Ilgen*, Enhancing the Effectiveness of Work Groups and Teams, p. 78, 2006.

[354] As defined by, *William J. Caelli,* Security in Open and Distributed Systems: Information Management & Computer Security, Vol. 2, pp. 18-24.

[355] A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. Therefore, these tools are essential tools for deterring hackers from inserting a preferably hidden rootkit (e.g. Trojan) on the victim's machine.

[356] This tool is used from network administrators for manually generating packets to test network devices, such as firewalls, IDSs, and for auditing network protocols (e.g. TCP/IP Stack) for detecting vulnerabilities, http://www.scs.ryerson.ca/~zereneh/cn8822/PacketCrafting.pdf

- ❖ Antivirus;
- ❖ Spyware detector tools[357];
- ❖ Security-oriented Operating systems (OS);
- ❖ Packet sniffing tools.

14. Until recently, the lowest number of adoptions of security tools came from small-sized companies, followed by medium-sized companies due to limited resources in financial and technical resources[358]. However, they are all obliged to adopt basic security tools that at least protect the confidentiality, integrity, availability of the information flows through the networked communication environment.

15. ISO 27001 (2018) is considered a globally recognized standard that provides a best-practices framework for address the entire range of cyber risks, by encompassing personnel, procedures and use of technology for establishing, implementing and maintaining the protection of businesses' objectives.

16. It is quite interesting that most EU Member States missed NIS Directive deadline[359]; until 10/8/2018 (three months past the transposition deadline) only 11 nations have complied, i.e. Cyprus, Czech Republic, Estonia, Finland, Germany, Italy, Malta, Slovakia, Slovenia, Sweden and UK[360].

    This fact, however, entails significant lack of advice implemented for each Member State. More specifically, had the organizations implemented had transposed the NIS Directive into national law more promptly, the accessibility of advice from regulators and consultancy would have advocate the adoption of security tools for the rest of the EU Member States[361].

[357] Such as keyloggers.

[358] *N. Darmawan***,** *A. Yee-Loong Chong***,** *Keng-Boon Ooi and V. A/L Venggadasallam N. Darmawan***,** *A. Yee-Loong Chong***,** *Keng-Boon Ooi and V. A/L Venggadasallam,* Security Mechanism in Computer Network Environment: A Study of Adoption Status in Malaysian Company (a research article), available at: http://docsdrive.com/pdfs/ansinet/jas/2009/2735-2743.pdf

[359] Probably being in the shadow of the EU GDPR (General Data Protection Regulation) that came into force on 25/5/2018.

[360] Available at: https://www.itgovernance.eu/blog/en/majority-of-eu-member-states-missed-nis-directive-deadline

[361] In the sense that if member states haven't integrated the transposition of the directive, no one can be quite sure on the best way to prepare.

17. The establishment of a “European Cybersecurity Certification Framework for ICT products and services is recommended for addressing the multiple certifications risks promoted by various companies. More specifically, these companies certify ICT products, but they do not always follow the same procedures and standards. Considering the interoperability issues entailed due to the networked communication of ICT products (e.g. Internet of Things - IoT) the EC proposed the implementation of the voluntary “Framework” making use of existing Union and international technical standards for replacing all existing national cybersecurity certification schemes or procedures for ICT products and services which will be prepared by ENISA[362].

    According to the Commission’s belief, the proposed Framework and European cybersecurity certification schemes will make certification less expensive, more effective, and more commercially attractive, thus helping to spread better cybersecurity practices throughout the EU[363].

18. Although the light-touch approach aims at avoiding overburdening the DSPs, special concern should be imposed on ensuring the swift and efficient way of incident reporting while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner, by setting up the types of incidents and parameters to that will be used.

[362] The new proposed Regulation will be known as the EU “Cybersecurity Act, available at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

[363]*Kurt Wimmer* Covington, The EU Gets Serious About Cyber: The EU Cybersecurity Act and Other Elements of the “Cyber Package, available at: https://www.cov.com/-/media/files/corporate/publications/2017/09/the_eu_gets_serious_about_cyber.pdf

4 Analysis of the current situation in Greece

In Greece, cybersecurity policy concerns several Ministries due to previous relevant actions, which however have created overlaps and ambiguities. For this purpose, the General Secretariat of Digital Policy (GSDP) [364] was established for maintaining the leading role in the governance of cybersecurity in the country, taking into consideration the contribution of all involved entities.

4.1 The GSDP's mission

The GSDP's mission is to develop the national cybersecurity strategy which deals with the security of networked information systems including both public and private sector critical infrastructures, taking into consideration the increased development of ICT and the evolving interdependences between the interconnected digital infrastructures in daily social and economic activities of the country.

4.1.1 The GSDP's objectives

The GSDP was established having the following strategic objectives[365]:

a) The development and maintaining of a National Cybersecurity Strategy (NCSS) demonstrates the national action plan for strengthening the cyber protection of Information and Communication Technologies (ICT), using in infrastructures that support the development of the digital single European market.

b) Monitoring the implementation of the NCSS while providing coordination between the involved Ministries about the individual actions to implement the NCSS.

[364] Part of the Ministry of Digital Policy, N. 4389/2016.

[365] http://mindigital.gr/index.php/announcments-ggdp/1109-systasi-tis-genikis-grammateias-psifiakis-politikis

c) The assessment of the implementation of the NCSS while submitting an additional relative proposal to engaged Ministries and entities, such as competent authorities and institutional and educational bodies.

d) The international representation of Greece on matters concerning the NCSS.

4.1.2 The governance framework of cybersecurity in Greece

The governance structure of the General Secretariat for Digital Policy (GSDP) is depicted in table 29.

Table 29: The governance structure of GSDP.

GENERAL SECRETARIAT FOR DIGITAL POLICY		
Department of Information Security and Networks	Department of Security Control	Department of Coordination and Domain Names

4.1.2.1 **Department of information security and networks**

The department of information security and networks is responsible for providing support and guidance to all relevant stakeholders on the establishment of appropriate and proportionate security measures, in order to be compliant to the requirements of the NIS Directive and any other relative EU Directive.

4.1.2.2 **Tasks of the department of information security and networks**

The role of this department is strategic in[366]:

a) Developing the Cybersecurity Strategy for Greek CI;

b) Developing and maintaining the information security policy for the public sector infrastructures;

c) Supporting the development of a security by design approach in the public sector's ICT infrastructures by defining rules and procedures;

[366] Department of information security and networks ,Άρθρο 05-Αρμοδιότητες Οργανικών Μονάδων της Γενικής Γραμματείας Ψηφιακής Πολιτικής. Available at: http://www.opengov.gr/ypes/?p=3408

d) Promoting cooperation and building of trust among relevant authorities, regulatory, institutional and educational bodies.

e) Establishing cooperation with the National CERT and any other established CSIRT at national CI sector.

f) Promoting culture, training and raising public awareness of the public sector.

4.2 The Hellenic Cybersecurity Strategy (HCSS)[367]

The Cybersecurity Strategy of Greece was published recently[368] and depicts the Greek society needs and interests.

4.2.1 Principles of the Hellenic Cybersecurity Strategy (HCSS)

The Hellenic cybersecurity strategy protects the interconnected operational environment of digital infrastructures (public and private sector) by ensuring the integrity, availability, confidentiality and availability of information flows through the networked installation while supporting the principle of open society along with constitutional freedoms and individual rights.

4.2.2 The governance structure of the Hellenic cybersecurity approach

According to the content of Greece's cybersecurity strategy, the centralized independent governance structure has been selected for assigning both roles of National Competent Authority (NCA)[369] and Single Point of Contact (SPOC) to the National Cyber Security Authority - General Secretariat of Digital Policy (GSDP).

Additionally, the National Authority Against Electronic Attacks - National Cert of the National Intelligence Service (EYP) has been designated as the responsible authority for the handling of risks and incidents based on a precisely defined procedure[370]. Table 30 illustrates this governance structure.

[367] Presidential Degree of 82/2017.

[368] On March of 2018.

[369] For both DSPS and OES.

[370] It is worth mentioning that on the 12th of November 2018 the Greek draft law for the transposition of the NISD into Greek law by rearranging this role to the Cyber-defense Directorate of the Ministry of De-

Table 30: The governance structure of the Hellenic cyber-security approach

NCA	GSDP	Representative in Coop-Group
NATIONAL CSIRT	National Cert	Representative in CSIRT network

4.2.2.1 Involved entities[371]

The involved entities with the HCSS are coming from both of authorized and regulatory communities.

A. Authorized entities

The cybersecurity activities in Greece require the participation and cooperation of several ministries. The following authorized entities are designated for serving the ministries' individual actions and concerns:

1. Center for Safety Studies[372] (CSS)**;**

2. National Intelligence Services (EYP), Technical Department INFOSEC;

3. Cyber-defense Directorate **[373];**

4. Computer Development Authority **[374]**

5. Cyber Crime Division **[375]**

6. Hellenic Police **[376]**

B. Regulatory bodies

Additional regulatory authorities have been established for various CI such as:

1. Regulatory Authority for Energy (RAE);

2. Hellenic Authority for Communication Security and Privacy

3. Hellenic Data Protection Authority

4. Hellenic Telecommunications & Post Commission - EETT

5. Stakeholders from the Transport sector:

fense. Available at: https://www.e-nomothesia.gr/law-news/ste-boule-skhedio-nomou-gia-ten-kubernoasphaleia.html

[371] As it is required in 3.1 State's obligation under the NCSS.

[372] It was created so as to identify the Critical Infrastructures of Greece (abbreviation in Greek:KEMEA)

[373] Ministry of Defense.

[374] Ministry of Administrative Reform and eGovernment.

[375] Ministry of Citizen Protection.

[376] Ministry of Citizen Protection.

- Regulatory Authority for Railways;
- National Regulatory Authority for Land Transport;
- Regulatory Authority for ports;
- Hellenic Civil Aviation Authority[377] (HCAA);
- Air navigation supervising authority (ANSA).

4.3 Evaluation of the HCSS

1. Greece until today has not transposed the NIS Directive into the national legislation; however recently Greece took a step forward, by forwarding the relevant draft law in the Greek Parliament[378]. Greece has integrated essentially but not formally the transposition of NIS Directive into national legislation by designating the roles and responsibilities of relevant entities complemented by identifying the CI sectors and defining incident handling procedures and binding penalty rules. But these requirements should have been addressed by 9 November 2018[379].

2. The protection of Critical Infrastructures in our country is far from the desirable level; although Greece has formally incorporated the relevant European Directive (114/2008 / EC) on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection into its legislation, subsequently now after 10 years, there is a mandatory accountability that must be applied avoiding be mistaken with the emphasis given on the funded programmes in the past.

3. Additionally, the content of HCSS applies to networks and information systems within the whole public sector and not being implemented in fragmented areas. However, the absence of explicit references to critical infrastructure protection issues resulting in not demonstrating the positive dynamic that should have. The ef-

[377] Hellenic Ministry of Infrastructure, Transport and Networks.

[378] https://www.e-nomothesia.gr/law-news/ste-boule-skhedio-nomou-gia-ten-kubernoasphaleia.html

[379] *Maglaras/Drivas/Noou/Rallis*, NIS directive: The case of Greece, ICST Trans. Security Safety 4(14), 2018, p. 3.

fective cooperation between the public and private sector is fundamental for the recognition and protection of critical ICT infrastructures and related services[380].

4. Although in the HCSS there is a specific reference to cultural interests, cultural interests are not explicitly included among the tasks[381] of Department of information security and networks (4.1.2.1). This is crucial because the National Competent Authority (GSDP) lacks the dynamism it should have in accordance with the NIS Directives requirements for achieving a coherent approach and for that reason a redefinition of its responsibilities is required.

5 Conclusions

1. Cybersecurity is not a concern that we can avoid or ignore any more and the cyber threat is integrated into security conception.
2. Although a lot of financial resources can be made available to tackle cybersecurity at the national level the lack of an appropriate coordination and competence between organizations is of paramount importance.
3. Cybersecurity initiatives should not be limited to economically advanced countries. Instead, it is necessary to be addressed as a key priority ensuring the support of allied countries within EU.
4. Each Member State will decide on which CI sector, from both of public and private sector, the NIS Directive will be implemented on.
5. The spread of internet use, which includes the use of networks and information systems alongside our day-to-day activities offers us an absolute freedom of ac-

[380] According to analysis and research institute “Dianeosis” study on “Holistic Critical Protection Infrastructure”, pp. 119-120. Available at: https://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo3_version_020616_2.pdf

[381] Άρθρο 160 Αρμοδιότητες της Γενικής Γραμματείας Ψηφιακής Πολιτικής, ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ Τεύχος Α’ 94/27.05.2016. available at: http://mindigital.gr/attachments/article/1109/N_4389_2016_%CE%93%CE%93%CE%A8%CE%A0.pdf

cess, but it can also put us with the involved information systems at very high risk unless we introduce the required prevention and protection rules.

6. Network security demands a collective effort, at the local level, between all parts of an organization and the creation of strong cooperation between private and public bodies while building trust on them.
7. The mistaken perception that security was synonymous with the choice of specific technology solutions[382], does not exist anymore. Instead, the new security conception requires security to be provided by design.
8. The NISD identifies the need for a cyber-security capability model to focus on the entire organization and in the particular domains of:
   - ✓ Risk Management;
   - ✓ Asset, Change, and Configuration Management;
   - ✓ Identity and Access Management;
   - ✓ Threat and Vulnerability Management;
   - ✓ Situational Awareness;
   - ✓ Information Sharing and Communications;
   - ✓ Event and Incident Response, Continuity of Operations;
   - ✓ Supply Chain and External Dependencies Management;
   - ✓ Workforce Management;
   - ✓ Cybersecurity Program Management.

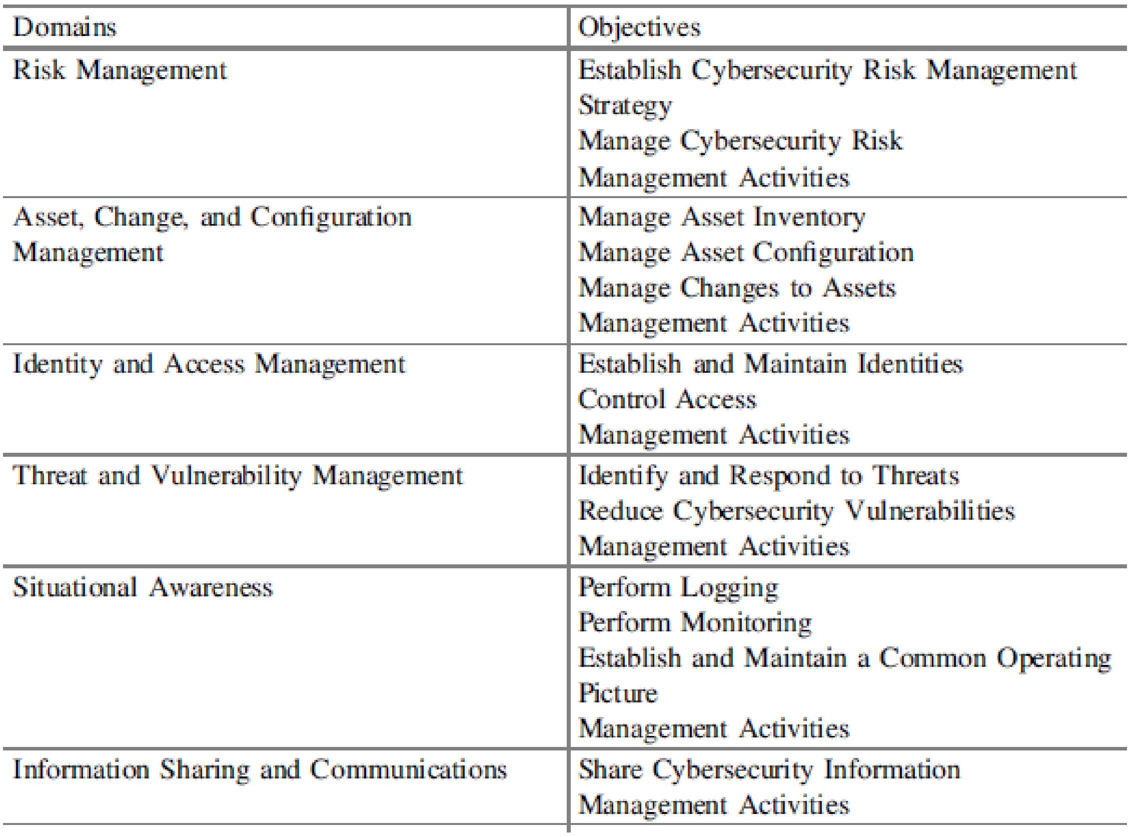
In that sense, NIS Directive regulates the creation of baseline security rules concerning network and information systems used from the public and private sector stakeholders while setting up requirements for education, awareness[383] and training programs for involved entities.

The cybersecurity capability maturity model that satisfies the NISD requirements is the C2M2 model, which is updated and focused on the entire organization, while implements a certain risk management measurement system. In table 31 are depicted the security domains and objectives of the C2M2 model.

[382] E.g. the best firewall.

[383] Both on a member-state level and an organizational level.

Table 31: Domains and objectives of the C2M2 model[384].



Domains	Objectives
Risk Management	Establish Cybersecurity Risk Management Strategy Manage Cybersecurity Risk Management Activities
Asset, Change, and Configuration Management	Manage Asset Inventory Manage Asset Configuration Manage Changes to Assets Management Activities
Identity and Access Management	Establish and Maintain Identities Control Access Management Activities
Threat and Vulnerability Management	Identify and Respond to Threats Reduce Cybersecurity Vulnerabilities Management Activities
Situational Awareness	Perform Logging Perform Monitoring Establish and Maintain a Common Operating Picture Management Activities
Information Sharing and Communications	Share Cybersecurity Information Management Activities

[384] *Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano and Isaac Daniel Sanchez-Garcia*, Comparative Study of Cybersecurity Capability Maturity Models, p. 9. Available at: https://www.researchgate.net/profile/Jose_Calvo-Manzano/publication/319640924_Comparative_Study_of_Cybersecurity_Capability_Maturity_Models/links/5a0d707da6fdcc39e9bfe110/Comparative-Study-of-Cybersecurity-Capability-Maturity-Models.pdf?origin=publication_detail

Event and Incident Response, Continuity of Operations	Detect Cybersecurity Events Escalate Cybersecurity Events and Declare Incidents Respond to Incidents and Escalated Cybersecurity Events Plan for Continuity Management Activities
Supply Chain and External Dependencies Management	Identify Dependencies Manage Dependency Risk Management Activities
Workforce Management	Assign Cybersecurity Responsibilities Control the Workforce Life Cycle Develop Cybersecurity Workforce Increase Cybersecurity Awareness Management Activities
Cybersecurity Program Management	Establish Cybersecurity Program Strategy Sponsor Cybersecurity Program Establish and Maintain Cybersecurity Architecture Perform Secure Software Development Management Activities

6 An example of the NIS Directive’s implementation into Aviation subsector in Greece

6.1 Introduction

In sections 6 and 7 (recommendations on developing an aviation cybersecurity strategy) I will present the possible way the NIS Directive could be implemented in the aviation subsector. The content of this presentation is based on the method proposed by ENISA[385]and a study conducted by a research and analysis company ‘Dianeosis’, for identifying the Critical Infrastructures[386] in Greece. While advising the aviation cybersecurity strategy of UK, for understanding which recommendations should be proposed to Hellenic Civil Aviation Authority for implementing the NIS Directive’s requirements into air transport subsector.

The quantity of the information collected and processed was based on publicly accessible rights and personal expertise due to my participation in a relative training course[387] and the quality is ensured by appropriate scientific methods used from ENISA, ‘DIANEOSIS’ and information sources provided by EUROCONTROL and Hellenic Civil Aviation Authority.

[385] Rossella Mattioli, 2014.

[386] Public and private.

[387] The cyber security in ATM, by EUROCONTROL.

6.2 Transport sector

The transport sector provides services in many areas and supports relative economic activities, such as trade, tourism, farming, and industrial development.

The provided services are subdivided into sectors as depicted in table 32.

Table32: The transport sector in Greece.

TRANSPORT SECTOR			
Rail transport sector	Road transport sector	Shipping transport sector	Air transport sector

6.2.1 The case of Air transport sector services

When we refer to air transport sector the following services are included:

- Airport services;
- Aeronautical services.

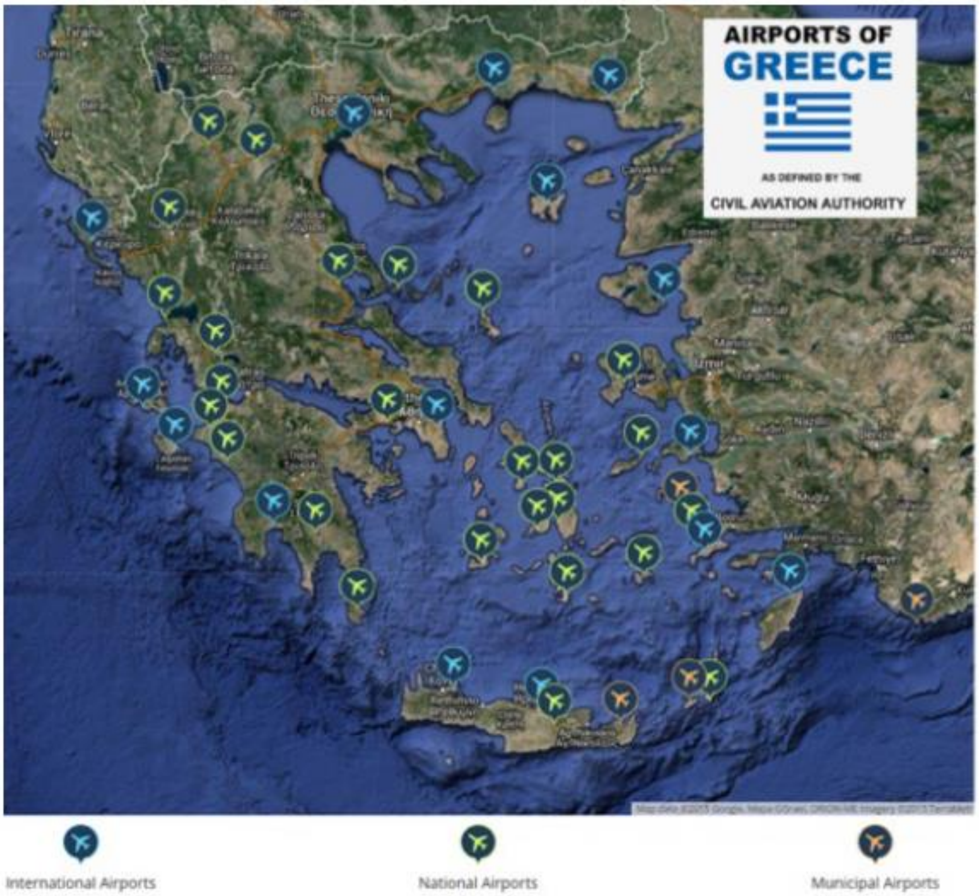
6.2.1.1 Airport services

The airport services include services related to air transport (including aircraft) and airport infrastructures. Table 33 presents schematically the airport services.

Table 33: Airport services.

Airport services	
Air-transport services (including aircraft services)	Airport infrastructures Services

The Air transport services are critical for Greece due to its geographical location and its soil morphology; in the meantime, operate 41 airports (picture 11) in Greece.



Picture 11: Airport network in Greece[388].

Despite the increased demand for air travel, the lack of significant investment in infrastructure limits the development of the air traffic management system in Greece, which in its turn makes the risk of saturation evident.

As a response to the increased demand on air travelling, the European Commission adopted the Single European Sky, in 2008, in order to create a legislative framework for European aviation for improving the quality of the civil aviation in terms of ensuring the provision of safer, more efficient and more environmentally friendly services[389].

It is worth mentioning that, "El. Venizelos'[390], was founded at the 30th position of the top 30 airports in Europe, with the second highest growth rate, by welcoming a total of 18,073,940 travellers in 2015 in the medium-sized airport's category[391]. An additional discrimination concerns the airport of Santorini[392] with the fast-

[388] Provided by *Civil Aviation Authority*, available at: http://www.ypa.gr/our-airports

[389] It is estimated that Air Passengers will be increased by 50% within EU by 2020 while the cargo services by 125%.

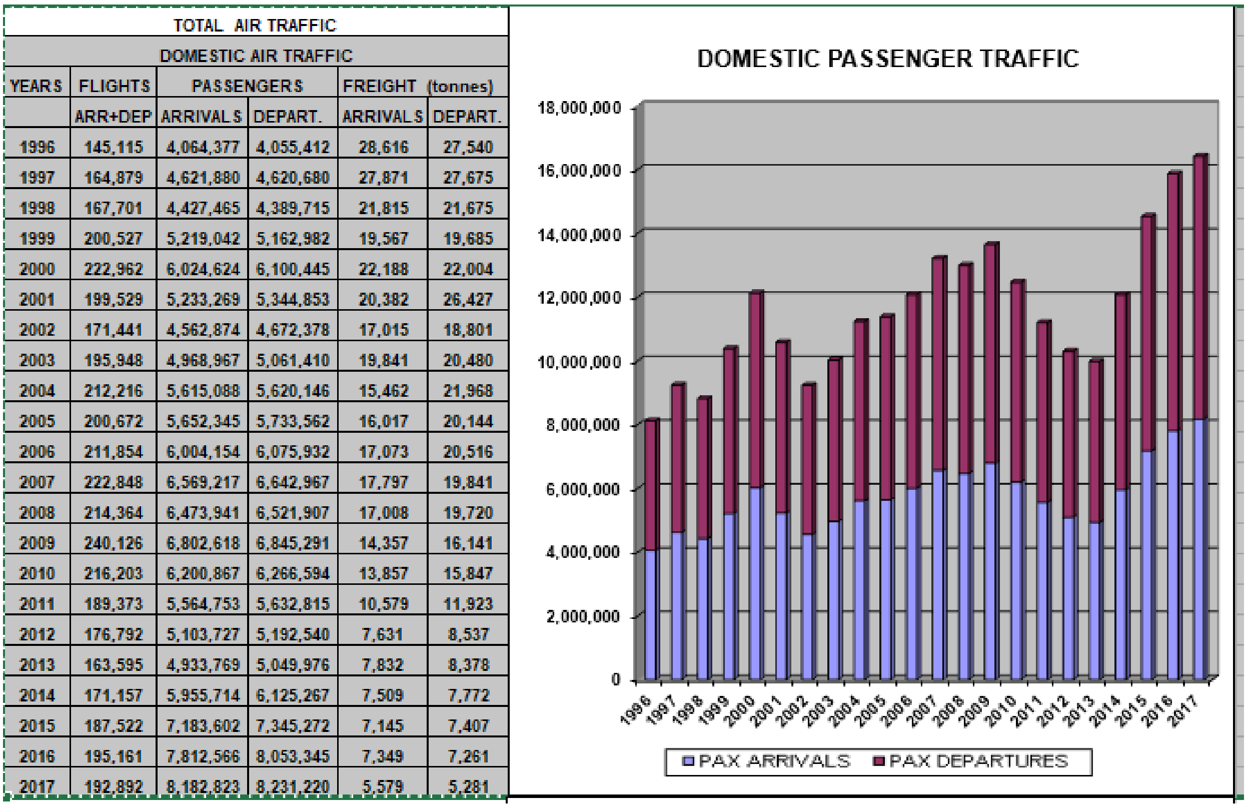
[390] Athens airport

[391] The airports that receive 10-25 million passengers per year.

est growing one since it recorded an impressive 87.6% increase in passenger numbers for 2015[393].

Indicatively, the following table in tables 34 and 35 depict the increase in the movement of the air passenger community during 1996-2017[394].

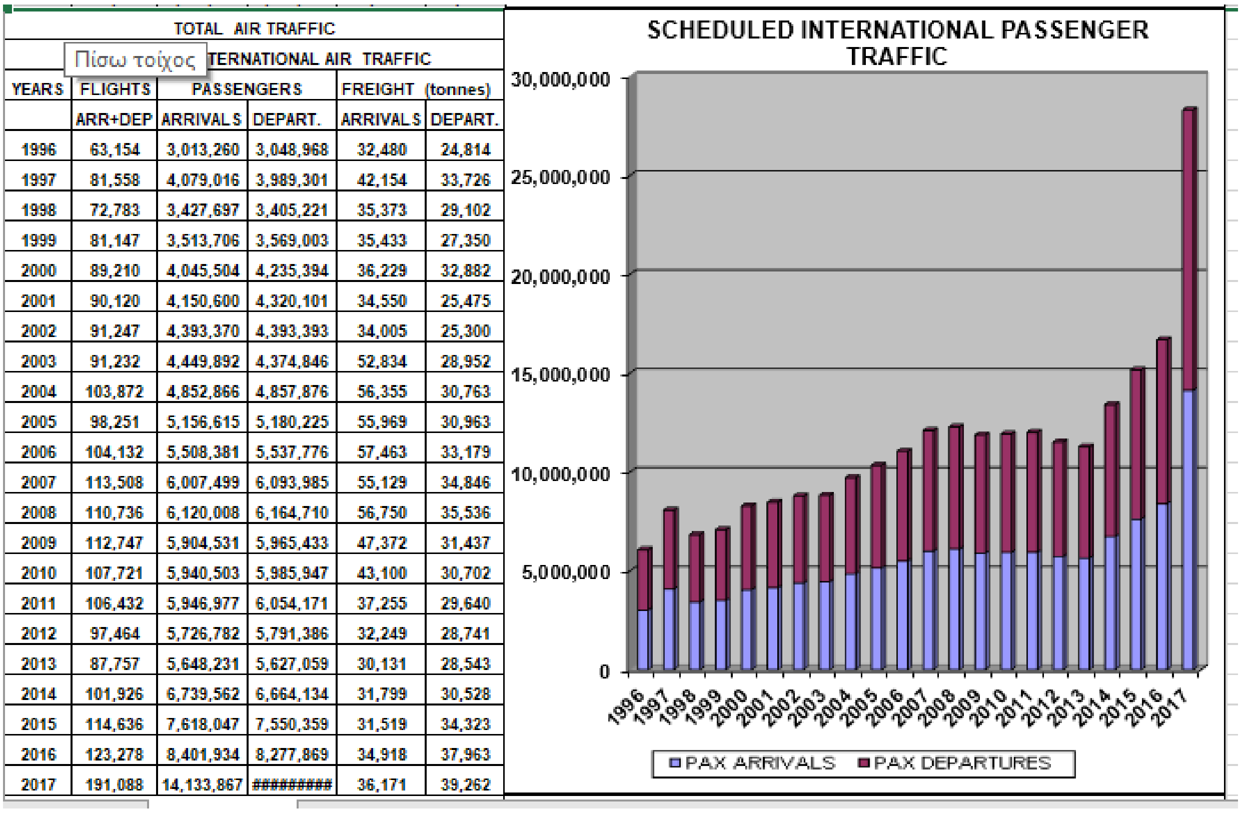
Table 34: Domestic passenger traffic for 1996-2017.



TOTAL AIR TRAFFIC					
DOMESTIC AIR TRAFFIC					
YEARS	FLIGHTS	PASSENGERS		FREIGHT (tonnes)	
	ARR+DEP	ARRIVALS	DEPART.	ARRIVALS	DEPART.
1996	145,115	4,064,377	4,055,412	28,616	27,540
1997	164,879	4,621,880	4,620,680	27,871	27,675
1998	167,701	4,427,465	4,389,715	21,815	21,675
1999	200,527	5,219,042	5,162,982	19,567	19,685
2000	222,962	6,024,624	6,100,445	22,188	22,004
2001	199,529	5,233,269	5,344,853	20,382	26,427
2002	171,441	4,562,874	4,672,378	17,015	18,801
2003	195,948	4,968,967	5,061,410	19,841	20,480
2004	212,216	5,615,088	5,620,146	15,462	21,968
2005	200,672	5,652,345	5,733,562	16,017	20,144
2006	211,854	6,004,154	6,075,932	17,073	20,516
2007	222,848	6,569,217	6,642,967	17,797	19,841
2008	214,364	6,473,941	6,521,907	17,008	19,720
2009	240,126	6,802,618	6,845,291	14,357	16,141
2010	216,203	6,200,867	6,266,594	13,857	15,847
2011	189,373	5,564,753	5,632,815	10,579	11,923
2012	176,792	5,103,727	5,192,540	7,631	8,537
2013	163,595	4,933,769	5,049,976	7,832	8,378
2014	171,157	5,955,714	6,125,267	7,509	7,772
2015	187,522	7,183,602	7,345,272	7,145	7,407
2016	195,161	7,812,566	8,053,345	7,349	7,261
2017	192,892	8,182,823	8,231,220	5,579	5,281

[392] It belongs to category 4, which receives less than 5 million passengers per year.
[393] According to the ACI-European Airport Trade Association communication.
[394] Available at: http://www.ypa.gr/profile/statistics/yearstatistics/

Table 35: Scheduled International passenger traffic for 1996-2017.



TOTAL AIR TRAFFIC

TERNATIONAL AIR TRAFFIC

YEARS	FLIGHTS	PASSENGERS		FREIGHT (tonnes)	
	ARR+DEP	ARRIVALS	DEPART.	ARRIVALS	DEPART.
1996	63,154	3,013,260	3,048,968	32,480	24,814
1997	81,558	4,079,016	3,989,301	42,154	33,726
1998	72,783	3,427,697	3,405,221	35,373	29,102
1999	81,147	3,513,706	3,569,003	35,433	27,350
2000	89,210	4,045,504	4,235,394	36,229	32,882
2001	90,120	4,150,600	4,320,101	34,550	25,475
2002	91,247	4,393,370	4,393,393	34,005	25,300
2003	91,232	4,449,892	4,374,846	52,834	28,952
2004	103,872	4,852,866	4,857,876	56,355	30,763
2005	98,251	5,156,615	5,180,225	55,969	30,963
2006	104,132	5,508,381	5,537,776	57,463	33,179
2007	113,508	6,007,499	6,093,985	55,129	34,846
2008	110,736	6,120,008	6,164,710	56,750	35,536
2009	112,747	5,904,531	5,965,433	47,372	31,437
2010	107,721	5,940,503	5,985,947	43,100	30,702
2011	106,432	5,946,977	6,054,171	37,255	29,640
2012	97,464	5,726,782	5,791,386	32,249	28,741
2013	87,757	5,648,231	5,627,059	30,131	28,543
2014	101,926	6,739,562	6,664,134	31,799	30,528
2015	114,636	7,618,047	7,550,359	31,519	34,323
2016	123,278	8,401,934	8,277,869	34,918	37,963
2017	191,088	14,133,867	#########	36,171	39,262

6.2.1.2 Aeronautical services

The aeronautical services include the Air Traffic Management (ATM) services and the Airspace services (table 36).

Table 36: Aeronautical services.

Aeronautical services	
ATM services	Airspace services (AIS)

6.2.1.3 Air transport sector interdependencies.

The CI of the air transport sector, through the networks and information systems that are used for providing their critical services, create dependencies on a variety of ICT systems and services.

In table 37 I have included the identified interdependencies and the main providers of air transport sector services.

Table 37: Air transport services and identified interdependencies

CI	Relative sub-sector	Interdependences		Main providers
		Dependency on	Affects	
Airport services	-Airport[395] infra-structures -Air transport – airline network (including aircraft services)	-Energy supply; -ICT systems; -internet provision; -Interoperability of infrastructures; - X-Ray scanners; -Metal detectors; -flight management system; -CCTV[396] system etc -Meteo services	-Air transport sector -Tourist & Economic development	-HCAA[397] -AIA[398] -FRAPORT[399]
Aeronautical services	-ATM services -AIS[400] services (flight plan, NOTAM[401] etc.)	-Energy supply; -Air navigation systems[402] (COM-NAV-RADAR system)	All sectors[403]. Indicatively mentioning: -Tourism -Trade	-HCAA -ICAO[404]

[395] National, international, municipal or private airports.
[396] Closed-circuit television system.
[397] Hellenic civil aviation authority
[398] Athens international airport
[399] More information available at: https://www.fraport-greece.com/www.mjt-airport.gr
[400] Aeronautical information services supported by international civil aviation organization (ICAO) for ensuring the flow of information necessary for the safety, regularity, and efficiency of international air navigation.
[401] A Notice to Airmen (NOTAM) in order to notify aircraft pilots of any potential hazards along a flight route or at a location that could affect the safety of the flight.
[402] The air navigation systems include the ICT systems used for communicating the aircraft to ground and the opposite, such as: Communication systems with transponders and receivers, Air navigation systems (ILS, VOR, DME) and radar system (air traffic control and navigation, and space and range instrumentation radar system).
[403] According to "Dianeosis" study, available at: page 117.
[404] International civil aviation authority

		-ICT infrastructure; - Interoperability of infrastructures; -Meteo services -Aircraft ICT infrastructure.	-Industry -Public administrations	

7 Recommendations on establishing an Aviation cybersecurity strategy.

7.1 Introduction

The Aviation subsector (air transport sector) is responsible for developing an Aviation cybersecurity strategy for ensuring that it remains safe, secure and resilient into possible cyber threats due to the increasingly interconnected digital infrastructures.

The Hellenic Civil Aviation Authority (HCAA) is the competent authority under the Ministry of Infrastructures and Transport with the responsibility to design, develop, monitor, and maintain a National aviation cybersecurity strategy for air transport sector services. Although a national aviation security strategy has been developed in 2016, for ensuring the proper operation of the sector, providing protection against certain defined risks, such as physical threats, terrorist attacks, mechanical failures and human errors, the cybersecurity risk is a new entry into the security area. Taking into consideration that in modern times, the operation of the aviation sector relies heavily on complex and networked information systems, there is a need for developing a new security approach including the cybersecurity threats and impacts on aviation sector due to the existing dependencies between cyber, physical and personnel security conception. The content of this strategy is set up in a way that involved parties from government, regulators and aviation industry, tackle in order to ensure a robust approach to risk management.

7.2 Scope

The aviation cybersecurity strategy applies to the whole Greek aviation sector and includes:

- ✓ Airports, including operators of passenger and cargo services and manufacturers and other ancillary service providers (airport infrastructures and facilities);
- ✓ Air navigation service providers;

Although the airlines and airports have robust systems in place in order to protect their services against common hacking threats, there is a need for implementing a rather holistic approach than a fragmented used till recently, by forcing them and IT providers to work towards a common security framework.

Additionally, the ATM systems used are closed and mainly consisted of proprietary systems well-isolated from cyber-attacks. However, there are factors that may increase the possibility of being compromised by cyber-attacks, such as[405]:

- Increasing automation and dependence on digital systems;
- Growing need for interoperability for facilitating the ground to air communication;
- Moving to a network-centric architecture;
- Increasing use of COTS[406] products and open standards;
- Mixing legacy and modern equipment;
- Adding more and more new end users; and
- Increasing the capabilities of threat actors.

Taking into consideration the increased interconnectivity between ATM systems alongside the shared used of COTS products it is common knowledge that the Member States and operators will be more reliant on each other regarding their cyber protection. For example, an attack on a week point in the network before propagating across it may lead to cascade failures. In that case, security concerns should be placed on ensuring trust and assurance between operators of ATM systems.

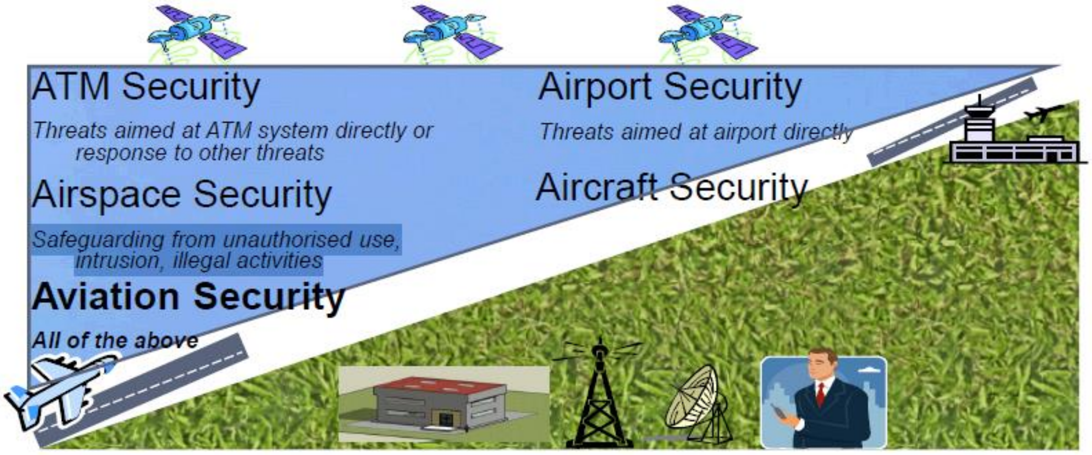
Therefore, the Aviation cybersecurity strategy provides guidance to secure the following sectors:

- **Air Traffic Management (ATM) interface systems and aircraft**: includes threats aimed at ATM system directly (such as attacks on ATM assets) or to other parts of the aviation system where ATM plays a key role in the prevention or response to such threats.
- **Airport systems**: includes threats aimed at airport infrastructures directly.

[405] Based on a position paper by ICB (Industry Consultation Body): “ Regulatory Response to ATM Cyber-Security”, p. 2.
[406] Commercial off the shelf products

- **Airspace**: includes threats related to unauthorized use, intrusion, illegal activities.
- **Other aircraft systems**: include threats that compromise potential vulnerabilities of used SCADA and ICT products in the aircraft's communication and entertainment systems.

In picture 12 is illustrated accordingly the ATM security conception with regards to general aviation security approach.


ATM Security
Threats aimed at ATM system directly or response to other threats
Airport Security
Threats aimed at airport directly
Airspace Security
Safeguarding from unauthorised use, intrusion, illegal activities
Aircraft Security
Aviation Security
All of the above

Picture 12: The Aviation security and its components under the ATM conception[407].

7.3 Objectives

The aviation cybersecurity strategy aims to:

- **Understand**:

    i. the risks posed by cyber threats to the aviation industry infrastructures;

    ii. their vulnerabilities and

    iii. their potential impacts.

- **Manage** cyber risks and take appropriate and proportionate actions to protect key assets;
- **Respond to and recover** from cyber events and incidents effectively and

[407] Provided by EUROCONTROL.

ensure that lessons are learnt;

- **Promote** cultural change, raise awareness and build cyber capability in the sector.

7.4 Principles

The development of the aviation cybersecurity strategy must be aligned with:

- the Hellenic Cyber Security Strategy and
- the Hellenic Aviation Security Strategy[408].

The aviation cyber-security strategy must be also focused on ensuring the following priorities for:

a) Helping the aviation industry to operate for its customers;

b) Ensuring a safe and secure way of travelling;

c) Building a global and connected Greece;

d) Encouraging competitive markets;

e) Supporting growth while tackling environmental impacts; and

f) Developing innovation, technology and skills.

7.5 Strategic Context

7.5.1 Definitions

Clear definitions should be provided for establishing a common language within relevant stakeholders.

7.5.1.1 Definitions for:

- cyber threats into Greece and in alignment with the HCSS;
- cyber threats into civil aviation;
- cybersecurity into civil aviation for protecting the confidentiality, integrity and availability of digital infrastructures and services;
- cyber resilience into civil aviation for ensuring the recovery of digital infrastructures and services to normal operation following a cyber-attack, taking

[408] Αριθ. Δ15/Α/18070/1501 Εθνικός Κανονισμός Ασφάλειας Πολιτικής Αεροπορίας.

into consideration that there is a significant possibility that a cyber-attack cannot be prevented.

7.5.1.2 Identification of threat sources, such as:

- Risk of espionage;
- Terrorism;
- Criminals;
- Extreme activists / Hacktivists;
- Disgruntled staff.

7.5.1.3 Identification of Actors source by using physical and/or electronic means, such as:

- Outsiders
- Insiders
- Insiders in collusion with outsiders

7.5.1.4 Identification of vulnerabilities

7.5.1.5 Identification of impacts by setting up the appropriate criteria needed to be taken into consideration for determining the types of significant impacts, such as:

- loss of life;
- disruption of aviation services; and
- reputation damage.

7.5.2 International Context

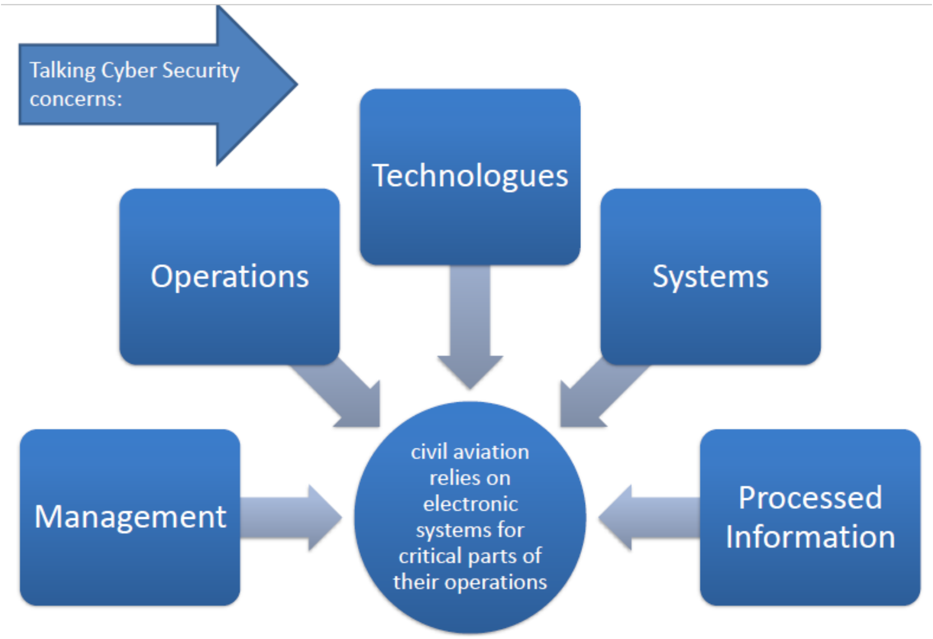
The Cybersecurity Strategy for the European Union alongside the EU Cyber Defense policy framework[409] set up the baseline for informing a regulatory framework to air transport sector operators and services. More specifically, Annex 17 from ICAO (chapter 4) adopts a holistic approach to cyber-security and recommends the Member States to develop functions to protect systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation, as well as implement procedures to share threat information.

[409] European Commission (2014) EU Cyber Defense Policy Framework.

The ICAO Aviation Security Manual (Doc 8973) assists in Annex 17 implementation and has been revised to contain minimum measures to protect critical information systems.

Additional to ICAO, it should be defined all the organizations at European and international levels each of which has a role to play in shaping the global approach to cybersecurity issue, such as:

- The European Aviation Safety Agency (EASA);
- The European Civil Aviation Conference (ECAC); and
- The European Organization for Civil Aviation Equipment (EUROCAE).


Talking Cyber Security concerns:
Technologues
Operations
Systems
Management
civil aviation relies on electronic systems for critical parts of their operations
Processed Information

Picture: Aviation cyber-security affected entities[410].

7.5.3 Emerging Technologies

Special interest should be focused on emerging technologies for ensuring that cyber resilience of innovations will be provided by their conception[411] in the future. For example, the Unmanned Aerial Systems (UAS) since they are increasingly used in improving and delivering our everyday life.

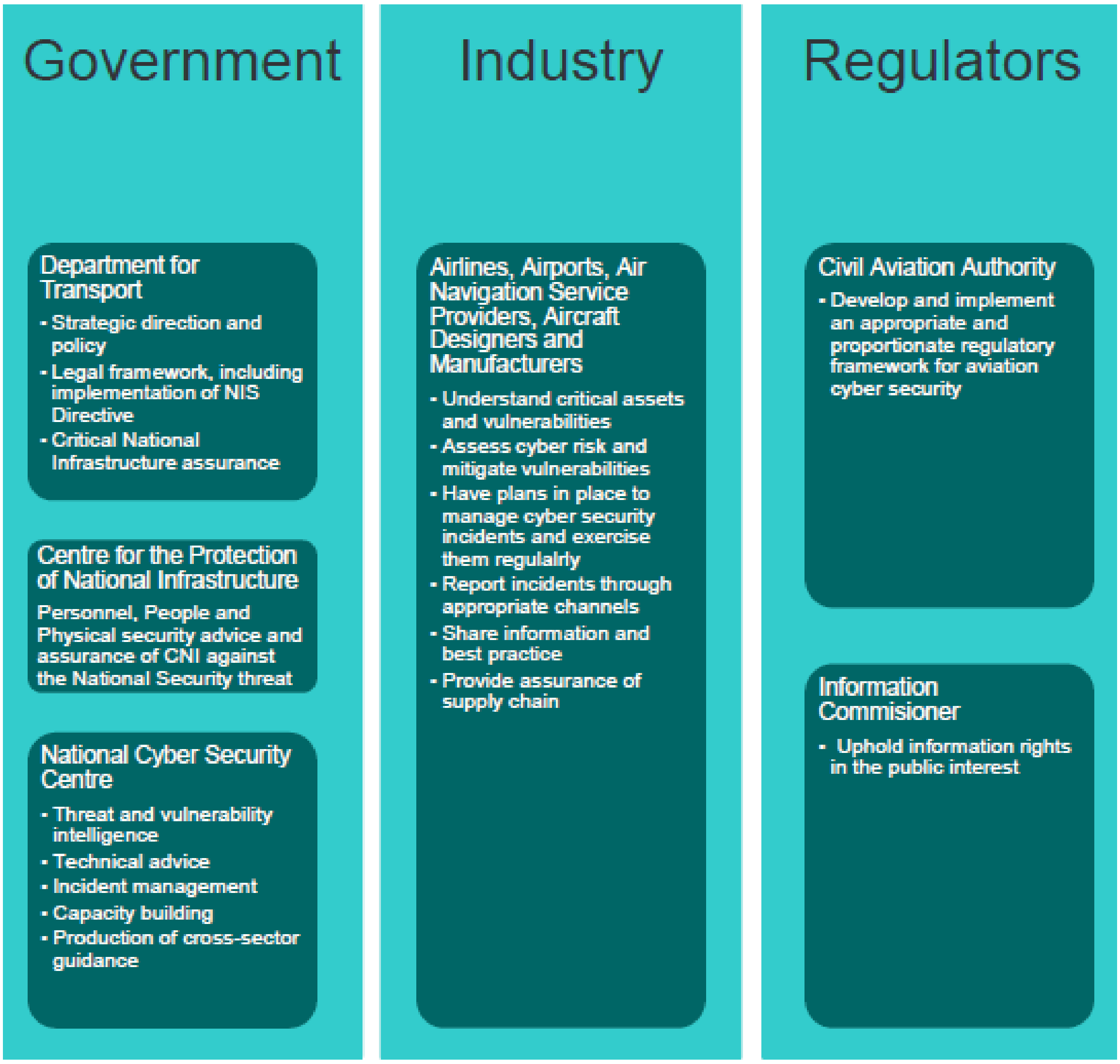
[410] Provided by: Mona Achkar Jabbour presentation at ICAO/UNOOSA Symposium, 2017 for Cyb-Air Security in Civil Aviation, p. 7,. Available at: http://www.unoosa.org/documents/pdf/spacelaw/workshops/2017/ICAOUNOOSA2017/0503_AL-Achkar_Jabbour_Lebanese_Univ_rev.pdf

[411] Security by design.

7.6 Roles and Responsibilities

A holistic approach should be taken by examining dependencies between cybersecurity, physical security and personnel security dependencies.

The key roles of each of the partners in delivering aviation security are presented schematically in picture 13.



Government

Department for Transport
- Strategic direction and policy
- Legal framework, including implementation of NIS Directive
- Critical National Infrastructure assurance

Centre for the Protection of National Infrastructure

Personnel, People and Physical security advice and assurance of CNI against the National Security threat

National Cyber Security Centre
- Threat and vulnerability intelligence
- Technical advice
- Incident management
- Capacity building
- Production of cross-sector guidance

Industry

Airlines, Airports, Air Navigation Service Providers, Aircraft Designers and Manufacturers
- Understand critical assets and vulnerabilities
- Assess cyber risk and mitigate vulnerabilities
- Have plans in place to manage cyber security incidents and exercise them regulalrly
- Report incidents through appropriate channels
- Share information and best practice
- Provide assurance of supply chain

Regulators

Civil Aviation Authority
- Develop and implement an appropriate and proportionate regulatory framework for aviation cyber security

Information Commisioner
- Uphold information rights in the public interest

Picture 13: Key partners participating in aviation cyber-security strategy[412].

7.6.1 Government

The Ministry of Infrastructures and Transport is responsible for developing the strategic objectives of aviation cyber-security strategy and regulation in Greek air transport sec-

[412] Provided by: The UK aviation cyber-security strategy, from Department for Transport, p.13.

tor, based on a robust assessment of the identified threats and vulnerabilities from paragraph 7.5.1

The Ministry of Infrastructures and Transport is also responsible for setting up the baseline security measures for Critical National Infrastructure in the transport sector, which ensures their appropriate and proportionate protection against potential cyber-attacks.

The government's tasks are performed through the Hellenic Civil Aviation Authority (HCAA) for providing advice, guidance and regulation to help operators and owners to mitigate the risks on assets, facilities, and ICT systems, platforms, networks, processes and people largely owned and managed.

7.6.2 The GSDP

The role of the GSDP in this strategy is defined in alignment to the HCSS since it reflects the single, central body for cybersecurity at a national level. The involved entities additional to the ministry of Infrastructure and Transport while being under the GSDP's side are the following:

- The ministry of foreign affairs in the context of the exchange of information between the Member States.
- The HNDGS Chief;
- The ministry of citizen protection;
- EYP (the technical department-INFOSEC) as considered the national CERT.

7.6.3 The Center for Safety Studies (KEMEA)

KEMEA is appointed as the "National Contact Point" for the protection of European Critical infrastructures (ECIs)[413] with the responsibility to provide protective security advice relating to national security threats in the physical and personnel/people security areas.

[413] Following the implementation of the 2008/114/EC Directive of the European Council of December 8th 2008 "regarding the definition and designation of the European Critical infrastructures and the assessment of the need to improve the protection of such infrastructures".

7.7 Regulators

7.7.1 The Civil Aviation Authority (CAA)

The CAA is responsible for the regulation of aviation security in Greece and monitors the aviation industry’s compliance with the aviation security requirements by determining safety and security strategy for the use of airspace.

7.7.2 The Information Commissioner’s Office (ICO) of HCAA

The role of the ICO is to provide communication to the public interest of security incidents, which are applied under the GDPR regulation regarding the protection of personal data.

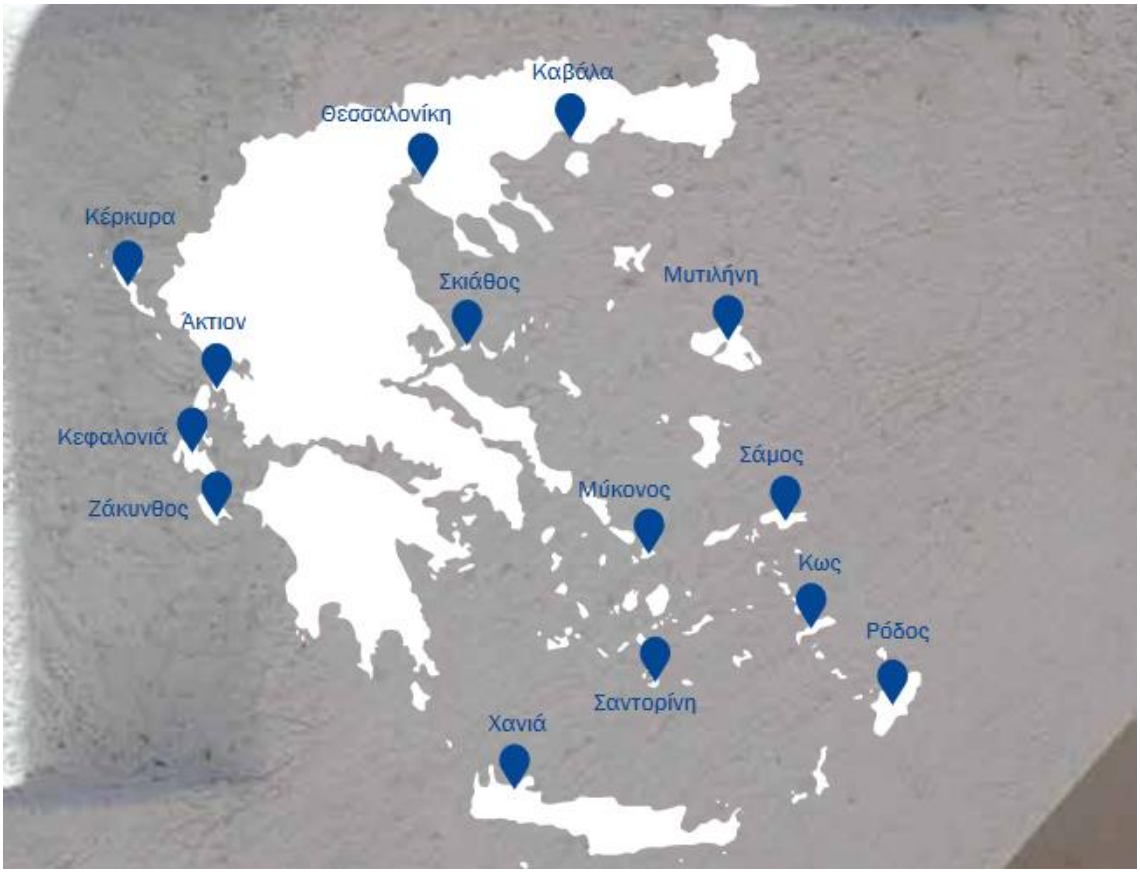
7.8 The Aviation Industry

The Greek Aviation Industry includes:

- The airport services (air transport services and airport infrastructures); and
- The aeronautical services.

The key aviation authorities for state and non-state airports are the following:

- Civil Aviation Authority (CAA);
- Athens International Airport (AIA);
- FRAPORT: the responsible authority for the 14 Greek airports depicted in picture 14;
- Hellenic Police Department;
- Customs; and
- Airline representatives.



Picture 14: The 14 airports of Greece under the FRAPORT's authority[414].

Each key partner (government and regulators performs the strategic part and aviation industry performs the operational part) must define what they aim to deliver and when, in accordance with the objectives of the aviation cybersecurity strategy, defined in paragraph 7.2.

7.9 ACTIONS

Each of the strategic partner (government-regulator-aviation industry) should define their goals and in accordance with the aviation cyber-security strategy's objectives from paragraph 7.2. Additionally, an activity framework should be provided for determining the way each of the strategic partners' defined goals will be fulfilled.

[414] https://www.fraport-greece.com/uploads/page_art/0/34//fraport_entypo%20A4_GR.pdf p. 8

7.9.1 1st security objective: UNDERSTAND.

The activity framework for enabling the 1st security objective includes security measures concerning:

i. the risks posed by cyber-threats to the air transport sector;
ii. the vulnerabilities within the transport sector; and
iii. the potential impacts of these identified cyber-risks and vulnerabilities within the air transport sector.

7.9.1.1 Required outcome

The provision of a mature understanding between and within government, the regulators and the aviation industry by matching specific vulnerabilities in Critical National Infrastructure sites and other critical assets, with common vulnerabilities across the air transport sector.

7.9.1.2 Actions for government partner

The government’s side will deliver:

1. A continuous risk assessment process for identifying all the Critical National Infrastructure sites of air transport sector and all defined critical assets, including data and information systems;
2. A documented report for providing evidence on the founding of the risk assessment process, including common vulnerabilities and the way these can be mitigated.

7.9.1.3 The Greek aviation industry partner

The Greek Aviation Industry will:

1. Prepare and maintain a list of all their critical digital, IT and Operational Technology systems, and platforms within their organization and supply chain, helping them have a clear understanding of why these assets are considered critical to their provided services and how they can be affected by potential compromised vulnerabilities.

7.9.1.4 Security measure- Risk Assessment

The aviation industry must implement a scientific Risk Assessment method for identifying the critical assets that need protection against cyber threats, physical risks and personnel harmful activities in order to assess whether the achieved or perceived risk is acceptable or tolerable; otherwise appropriate and proportionate preventive security measures should be adopted.

The Standards and Recommended Practices (SARPs) used for the aviation industry is based on Annex 17 from International Civil Aviation Organization (ICAO)[415]

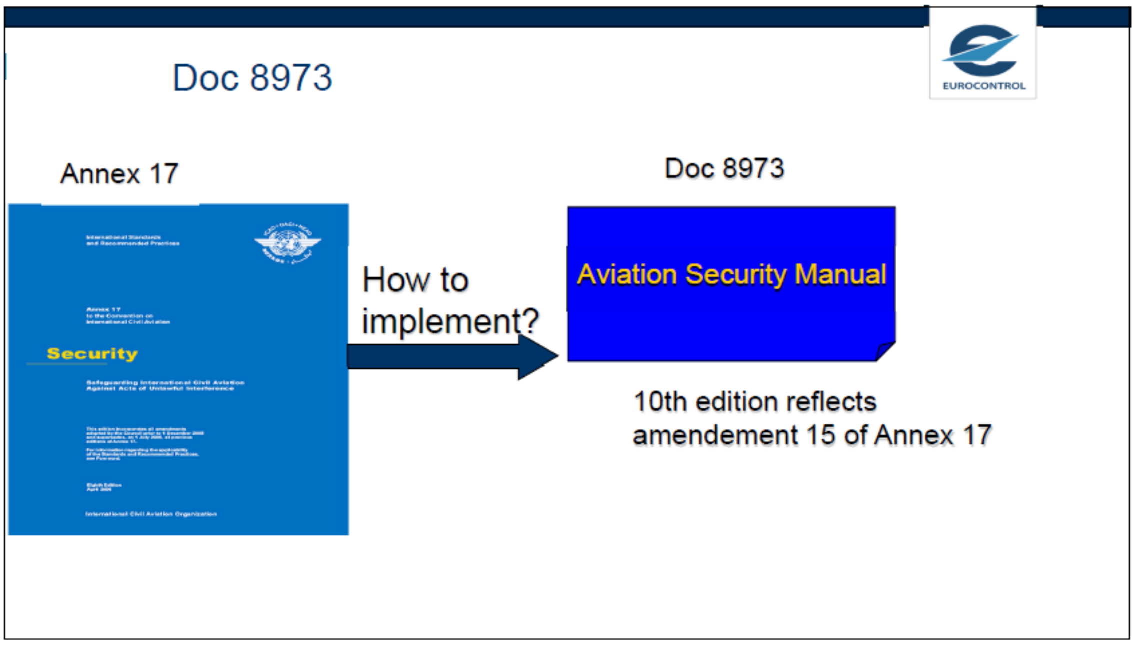
7.9.2 2nd security objective: MANAGE.

The activity framework for enabling the 2nd security objective includes:

i. Taking appropriate and proportionate security measures for protecting key assets;
ii. Selecting security measures for continuously managing the cyber risks

The security mechanisms that should be implemented by the aviation industry for satisfying the security objectives and requirements of national aviation cyber-security strategy are based on the security manual Doc. 8973 of Annex 17 from ICAO. Particularly for ATM security the security manual Doc 9985 should be implemented (pictures 15 and 16).

[415] The ICAO Council adopts standards and recommended practices concerning air navigation, its infrastructure, flight inspection, prevention of unlawful interference, and facilitation of border-crossing procedures for international civil aviation. ICAO defines the protocols for air accident investigation followed by transport safety authorities in countries signatory to the Chicago Convention on International Civil Aviation.



Doc 8973

Annex 17

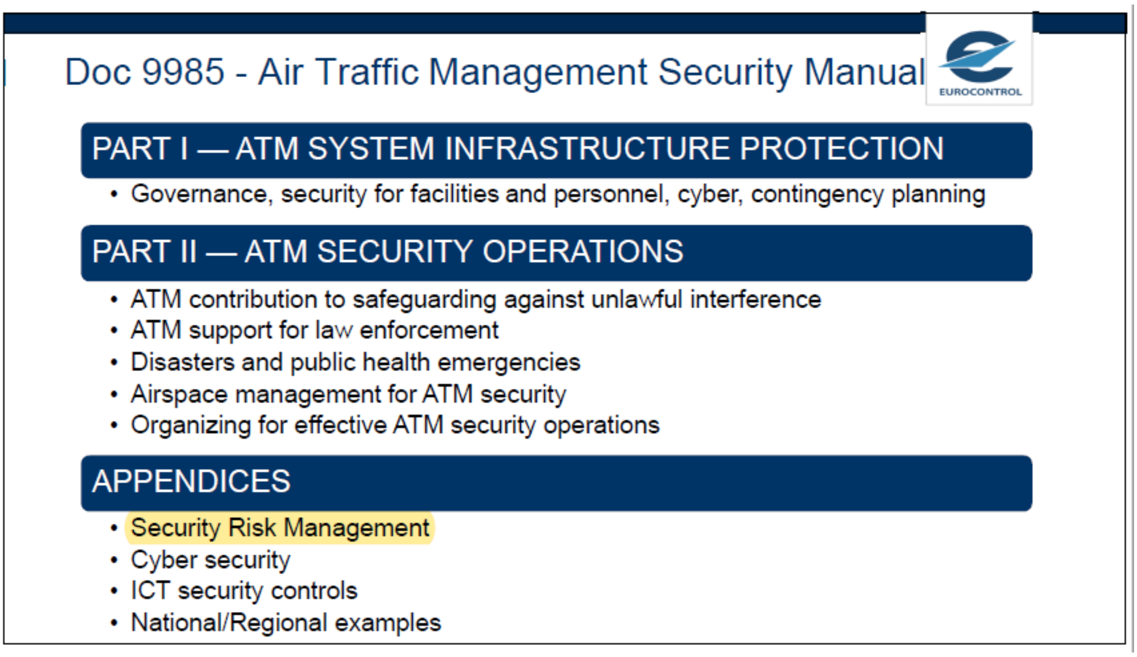
How to implement?

Doc 8973

Aviation Security Manual

10th edition reflects amendement 15 of Annex 17

Picture 15: Doc 8973 Aviation security manual[416].



Doc 9985 - Air Traffic Management Security Manual

PART I — ATM SYSTEM INFRASTRUCTURE PROTECTION

- Governance, security for facilities and personnel, cyber, contingency planning

PART II — ATM SECURITY OPERATIONS

- ATM contribution to safeguarding against unlawful interference
- ATM support for law enforcement
- Disasters and public health emergencies
- Airspace management for ATM security
- Organizing for effective ATM security operations

APPENDICES

- Security Risk Management
- Cyber security
- ICT security controls
- National/Regional examples

Picture 16: Doc 9985- ATM security manual[417].

Table 38 provides security measures alongside the roles and responsibilities for key partners.

[416] Provided by: EUROCONTROL.
[417] Provided by: EUROCONTROL.

Table 38: security measures for continuously managing cyber risks

Security requirement	Security mechanism	Implementation plan	
		GOVERNMENT	AVIATION INDUSTRY
Continuously managing cyber risks	**Risk management**	-Targeted support and advice to the aviation industry on developing risk treatment plans; - National level cyber risk assessment; -communication of the results through documented reports to Boards and aviation industry groups to raise awareness about the approach and specific activities industry can take to protect itself against specific threats, by understanding the potential cost to business in case of a cyber-attack or system compromise; -comprehensive guidance on the implementation o NIS Directive within stakeholders of the aviation industry.	- implement a Risk Management Method with the following features: i. continuous identification and assessment of cyber risks; ii. vulnerabilities treatment iii.robust governance structures and risk ownership - Ensure that cyber risks are managed throughout the lifespan of any new and developing systems, platforms and technologies.
	OUTCOME	***The support to the Aviation industry with advice and guidance for managing cyber-risks effectively and efficiently.***	

7.9.3 3rd security objective: RESPOND and RECOVER.

The aviation industry should be sufficiently prepared to deal with security incidents and events the moment they do occur. For that purpose, it is essential that there is a clear procedure for reporting the security incidents with corresponding business recovery plans related to critical assets for ensuring the effective and on time handling of them while promoting that lessons are across the industry. Therefore, the security requirements should include documented processes for:

i. Reporting incidents;
ii. Managing incidents; and
iii. Sharing of information within the aviation industry.

In table 39 are included the security measures- mechanisms for satisfying the abovementioned security requirements.

Table 39: Security measures for achieving the objective of responding to cyber-threats.

Security requirement	**Security mechanism**	**Implementation plan by:**	
		GOVERNMENT	**AVIATION INDUSTRY**

Respond to and recover from security incidents and events	**i. reporting incidents;**
	ii. managing incidents;
	iii. sharing information
		-preparing a report for assessing aviation industry's capability to respond to a cyber-attack, carried out repeatedly periodically to monitor progress;
		- Clearly defined procedures for determining the types of reporting incident alongside the content of required data (name, time)
		-create a **cyber-security information platform** for communicating the vulnerabilities and lessons learnt through incident handling procedures.
		- Develop cyber-exercises for gov., regulators and aviation industry;
		-create PPP[418] for sharing information and threat intelligence;
		- Support to the aviation industry in setting up aviation cyber security-CSIRTs for each stakeholder and meetings for the purpose of information exchange and sharing of best practice.
			- Develop, implement and review business continuity plans for recovering the sooner from a cyber-attack or system failure;
			- Report incidents to CSIRT of CAA through defined channels as outlined in NIS Directive.

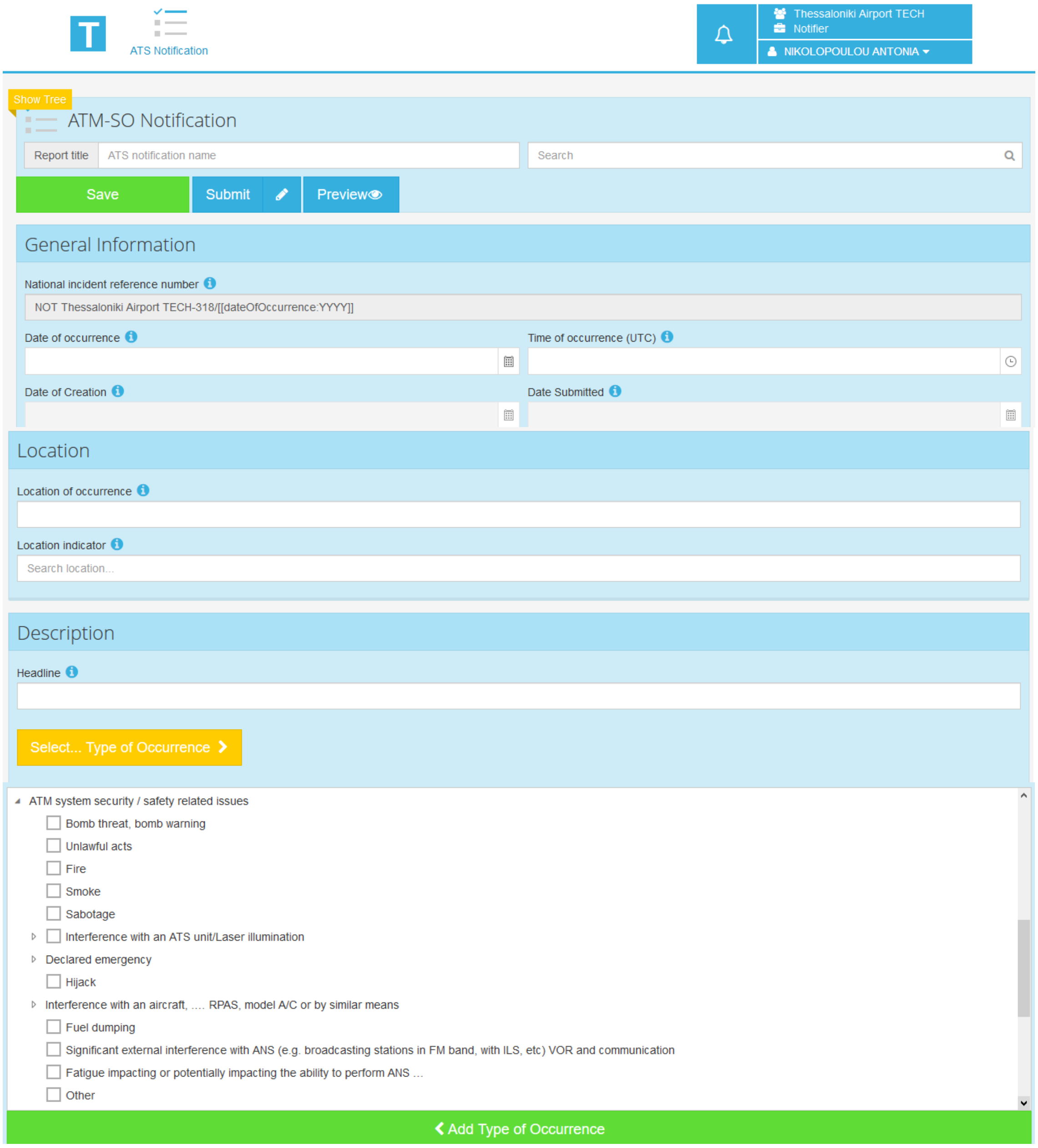
	OUTCOME	**The establishment of an incident response mechanism including clear lines of reporting and processes for implementing lessons learned.**	

[418] Public and private partnership

In case of ATM security area, the established reporting platform used for security incidents caused by physical and terrorist threats (e-tokai.net, produced by Eurocontrol) should be enhanced by adding cybersecurity indicators in the list provided for selecting the type of security incident.

Additionally, the platform should be extended in providing support and shared information to all notifier personnel for communicating the vulnerabilities and lessons learnt through incident handling procedures.

The following pictures illustrate the application used from Hellenic Civil Aviation for reporting security incidents related to physical and terrorist threats.



ATM-SO Notification

Report title: ATS notification name

Search

General Information

National incident reference number: NOT Thessaloniki Airport TECH-318/[[dateOfOccurrence:YYYY]]

Date of occurrence

Time of occurrence (UTC)

Date of Creation

Date Submitted

Location

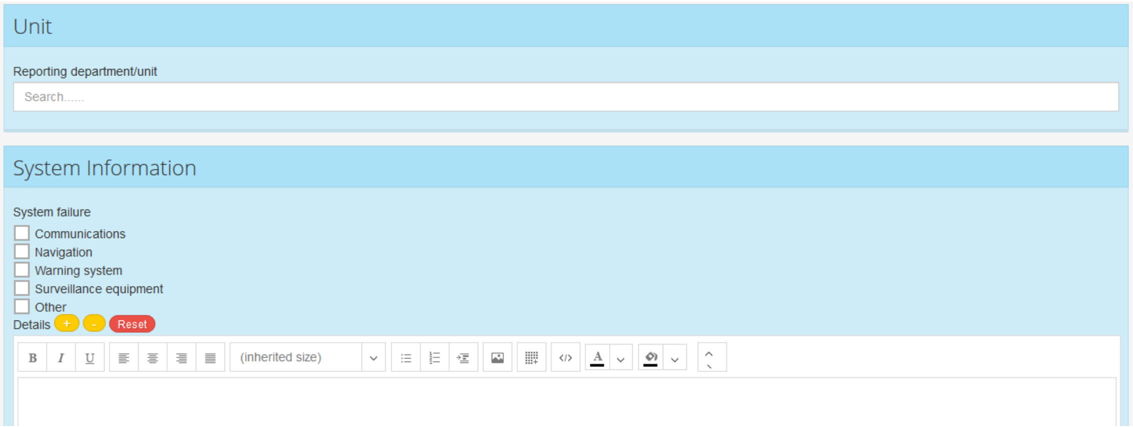
Location of occurrence

Location indicator: Search location...

Description

Headline

- ATM system security / safety related issues
  - □ Bomb threat, bomb warning
  - □ Unlawful acts
  - □ Fire
  - □ Smoke
  - □ Sabotage
  - □ Interference with an ATS unit/Laser illumination
  - Declared emergency
  - □ Hijack
  - Interference with an aircraft, ... RPAS, model A/C or by similar means
  - □ Fuel dumping
  - □ Significant external interference with ANS (e.g. broadcasting stations in FM band, with ILS, etc) VOR and communication
  - □ Fatigue impacting or potentially impacting the ability to perform ANS ...
  - □ Other



Unit

Reporting department/unit

Search......

System Information

System failure

□ Communications
□ Navigation
□ Warning system
□ Surveillance equipment
□ Other

Details

Picture 18: Example of the incident reporting platform[419]

7.9.4 4th security objective: PROMOTE CULTURE

It is essential for the Greek aviation industry to be capable of managing its risks. For that purpose, there is a need for establishing and maintaining an advance minimum common level of cyber-security skills and knowledge for the personnel, while training people entering the profession of a cyber-security specialist.

In order to satisfy the promotion of cultural change, raising awareness and building cyber capability the aviation industry should adopt security measures for:

i. Working collaboratively at an international level; and

ii. Providing Skills, training and resources.

In table 40 are included proposed security measures for satisfying the 4th security objective of the aviation cyber-security strategy.

Table 40: Security measures for achieving the objective of promoting culture, raising awareness and building cyber-capability.

Security requirement	**Security mechanism**	Implementation plan by:	
		GOVERNMENT	**AVIATION INDUSTRY**
Promote cultural change, raise awareness and build cyber capability.	i. Working collaboratively at a global and European level.	- will follow the ICAO's Working Group initiatives on Threat and Risk defence; - will work alongside other partners to help develop global approaches to tackling cyber	

[419] Source: the UK aviation cyber-security strategy, annex D, page 31.

		vulnerabilities, and will continue to press for ICAO leadership in this area; - will seek to support and input to an appropriate pan-European forum for exchanging information and incident response; - will continue to support the work of the ECAC Study Group on the Cyber Threat to Aviation, and help to update and maintain ECAC guidance to states on cybersecurity; - will continue to support and input to the development of appropriate and proportionate aviation cybersecurity standards for industry through EUROCAE.	
	ii. Providing Skills, training and resources	The NCSC Industry 100 secondments initiative which invites organizations of all sizes to work with the NCSC by embedding staff into the organization to provide the industry with a greater understanding of the cybersecurity environment, and the NCSC with new perspectives and knowledge of different sectors; - Access to certified training and professional schemes through the GCHQ Certified Training (GCT) scheme3 and the NCSC Certified Professional (CCP) scheme4.	- adopt clearly defined career development paths and further development opportunities for cybersecurity professionals in the civil aviation sector. -develop and provide regular education programmes in collaboration with ENISA for ensuring the participation of all personnel for achieving a common security level in identifying the risks posed in the aviation industry and responding effectively. This will grow both the pool of suitably qualified and experienced cybersecurity personnel

			in the sector, as well as raising existing personnel’s cybersecurity capability. -organize annually refresh courses (e.g. by organizing on the job training exercises) based on reported cyber-security incidents per stakeholder in the industry for sharing knowledge between personnel; -communicate the mitigation treatment established for all the significant security incidents providing evidence that all personnel have been informed.
	OUTCOMES	**1. Enhances Greece’s capability to shape the global evolution of cyberspace regarding the civil aviation strengthening the principle of national defence and proliferating national economic interests.** 2. **Building on self -security capabilities by creating expertise to meet national needs and interests within the aviation sector for overcoming future threats and challenges.**	

Bibliography

BOOKS

- *Cavelty Myriam Dunn*, Cyber-Security and Threat Politics: US efforts to secure the information age, p. 14, Routledge, New York (2008).

- *Cavelty Myriam Dunn, Mauer Victor and Krishna-Hensel Sai Felicia*, Power and security in the Information Age: Investigating the Role of the State in Cyberspace. Ashgate (2007).

- *Christou George*, Cyber security in the European Union: Resilience and Adaptability in Governance Policy, PALGRAVE MACMILLAN (2016).

- *Grabosky Peter*, Electronic Crime. Upper Saddle River. New Jersey, Pearson/Prentice Hall (2007).

- *Valacich Joseph, Schneider Christoph* , Information Systems Today: Managing in the Digital World 7th edition, Pearson (2016).

- *Webster Frank*, Theories of the Information Society. Third edition, Routledge, Taylor & Francis Group (2006).

- *Whitman /Mattord*, Principles of Information Security, 4th edition (2012), p. 120

PAPERS

- *Abrams, M., & Weiss, J.,* Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia. National Institute of Standards and Technology, Computer Security Division (2008).

- *Helena Carrapico/ Andree Barrinha*, The EU as a Coherent (Cyber)Security Actor?, JCMLS 2017 Volume 55. Number 6. pp. 1254- 1272

- *N. Darmawan, A. Yee-Loong Chong, Keng-Boon Ooi and V. A/L Venggadasallam N. Darmawan, A. Yee-Loong Chong, Keng-Boon Ooi and V. A/L Venggadasallam,* Security Mechanism in Computer Network Environment: A Study of Adoption Status in Malaysian Company. Also, available at: http://docsdrive.com/pdfs/ansinet/jas/2009/2735-2743.pdf

- "*Dianeosis"* (*ΔιαΝΕΟσις, ΟΡΓΑΝΙΣΜΟΣ ΕΡΕΥΝΑΣ ΚΑΙ ΑΝΑΛΥΣΗΣ*: Ολιστική Προστασία Κρίσιμων Υποδομών) 2016, Δ. Γκρίτζαλης, Π. Κοτζανικολάου, Μ. Μάγκος, Γ. Στεργιόπουλος, Γ. Λύκου, Ν. Πετράκος. Also available at: https://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo3_version_020616_2.pdf

- ICB (Industry Consultation Body): "Regulatory Response to ATM Cyber-Security", p. 2. Also available at: https://ec.europa.eu/transport/sites/transport/files/modes/air/single_european_sky/doc/20150910_icb_position_on_regulatory_response_to_atm_cybersecurity.pdf

- *Kozlowski & Ilgen*, Enhancing the Effectiveness of Work Groups and Teams, p. 78, Michigan State University, 2006. Also available at: https://pdfs.semanticscholar.org/c55c/7907b0ab68954460f087a3d8d76d1da17200.pdf

- *Kurtz C. F., Snowden D. J.,* The new dynamics of strategy: Sense-making in a complex and complicated world.

- *Maglaras/Drivas/Noou/Rallis*, NIS directive: The case of Greece, ICST Trans. Security Safety 4(14), 2018.

- *Motsko Michele, Oberndorf Patricia, Pairo Ellen-Jane, Smith James*, Rules of Thumb for the Use of COTS Products, TECHNICAL REPORT CMU/SEI-2002-TR-032 ESC-TR-2002-032 Carnegie Mellon University (Software Engineering Institute – 2002). Also, available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14078.pdf

- *RAMBOL*, Evaluation of the EU decentralized agencies in 2009, Final Report Volume III, Agency level findings (2009). Also available at: http://www.statewatch.org/news/2012/apr/evaluation-eu-agencies-vol-III.pdf

- *Wimmer Kurt* Covington, The EU Gets Serious About Cyber: The EU Cybersecurity Act and Other Elements of the "Cyber Package" (2017). Also, available at: https://www.cov.com/-/media/files/corporate/publications/2017/09/the_eu_gets_serious_about_cyber.pdf

MSc THESIS

Liis Peedu, Implementation of Network and Information Systems Security Directive 2016/1148 in Republic of Estonia: Balancing Transparency and Secrecy, TALLINN UNIVERSITY OF TECHNOLOGY, School of Business and Governance, Department of Law (2018)

JOURNAL ARTICLES

- *Caelli William J.*, Security in Open and Distributed Systems: Information Management & Computer Security, Vol. 2, pp. 18-24.

- *Cormack Cf., Andrew,* Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTED A Journal of Law, Technology & Society 2016, Volume 13, Issue 3, pp. 259-282.

- *Esays*, Breach notification requirements under the European Union legal framework: Convergence, Conflicts, and Complexity in Compliance, The John Marshall Journal of Information Technology & Privacy Law 2014, Vol. 31, Issue 3, Article 2, pp. 317-368, specifically pp. 329 et seq.

- *Fahey*, The EU’s Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security, European Journal of Risk Regulation 2014, Vol. 5, Issue 1.

- *Holzleitner/Reichl*, European provisions for cyber security in smart grid – an overview of the NIS-directive, Elektrotechnik & Informationstechnik 2017, Vol. 134, No. 1, p. 16.

- *Kemp*, Legal aspects of cloud security, Computer Law and Security Review, 2018, pp. 22 et seq.

- *Marion Nancy E.*, The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010.

- *Porcedda, Maria Grazia*, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Computer Law & Security Review 2018.

LEGAL INSTUMENTS

- A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”, COM (2006), {SEC(2006) aaa}. Also available at: http://ec.europa.eu/information_society/doc/com2006251.pdf

- COMMISSION IMPLEMENTING REGULATION (EU) 2018/151, 30 January 2017. Also available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG

- Commission Recommendation 2003/361/EC. Also available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF

- Communication on Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM (2016) 410. Also available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

- Council conclusions on Critical Information Infrastructure Protection-Achievements and next steps: towards global cybersecurity. 3093rd TRANSPORT, TELECOMMUNICATIONS and ENERGY Council meeting – telecommunication items only – Brussels, 27 May 2011. Also available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybersecurity_/sede150611cccybersecurity_en.pdf

- Council conclusions on Digital Agenda for Europe, 3017th TRANSPORT, TELECOMMUNICATIONS AND ENERGY Council meeting Brussels, 31 May 2010. Also available at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/114710.pdf

- Cybersecurity Act: Proposal for a REGULATION on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification COM (2017) 477. Also available at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)1. Also available at:

https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

- Department of information security and networks, Άρθρο 05-Αρμοδιότητες Οργανικών Μονάδων της Γενικής Γραμματείας Ψηφιακής Πολιτικής, available at:
- http://www.opengov.gr/ypes/?p=3408 (in Greek)

- Digital Agenda for Europe, COM(2010)245. Also available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

- Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 12 August 2013. Also available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

- Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008) p. 75.

- Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, 15 May 2014. Also available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014L0065

- Directive (EU)2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015. Also available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015L2366

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 6

July 2016. Also available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=

- OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

- European Commission - Fact Sheet “Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cyber security, also available at: http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm

- ENISA, A step-by-step approach on how to set a CSIRT, Deliverable WP2006/5.1(CERT-D1/D2).

- ________ Cyber exercises platform, available at: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform
- __________ Guideline on Threats and Assets, available at: https://www.enisa.europa.eu/publications#c5=2008&c5=2018&c5=false&c2=
- publicationDate&reversed=on&b_start=0&c10=Critical+Infrastructures+and+Services

- ___________ Incident notification for DSPs in the context of the NIS Directive”, FEBRUARY 2017, available at: https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

- ___________ Mattioli Rossella methodology, 2014, available at: https://publications.europa.eu/en/publication-detail/-/publication/e8b32529-fae9-495c-8494-e7e6cf6e014e/language-en

- ____________ NCSS Good Practice Guide, available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

- ________ Strategy 2016–2020 - Europa EU, available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

- ________ Technical guidelines for the implementation of minimum security measures for DSPs, December 2016, available at: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

- _________ Technical guidelines on the security measures in Article 13a, available at: https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

- ___________ The European Public-Private Partnership for Resilience", EP3R 2010-2013, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps

- _________ Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

- EU cyber security initiatives –working towards a more secure online environment, January 2017, p. 2. Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

- EU cyber security Strategy http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf, p. 2.

- European Commission (2014) EU Cyber Defense Policy Framework

- Evaluation in the Commission Reporting on Results Annual Evaluation Review 2006: Conclusions and findings from evaluations in the Commission. Also available at: http://ec.europa.eu/smart-regulation/evaluation/docs/eval_review_2006_en.pdf

- Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM (2017) 476 final. Also available at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-MAIN-PART-1.PDF

- NIS Coop-Group, Reference document on Incident Notification for Operators of Essential Services. Also available at: <https://circabc.europa.eu/sd/a/ac46021f-bccf-4970-80ba-a2c7d40fd29b/reference_document_incident_notification_OES.pdf >

- Proposal for A European Policy Approach, COM (2001) 298. Available at: https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf

- Proposal for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 2018/0328 (COD), COM (2018) 630. Also available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf

- Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009)149,{SEC(2009) 399} {SEC(2009) 400. Also available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

- The European Agenda on Security, COM(2015)185. Also available at https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf.

- The National Cybersecurity and Critical Infrastructure Protection Act H.R.3696 — 113th Congress (2013-2014) available at: https://www.congress.gov/bill/113th-congress/house-bill/3696

- The National Cybersecurity Protection Act, PUBLIC LAW 113–282—DEC. 18, 2014. Available at: https://www.gpo.gov/fdsys/pkg/PLAW-113publ282/pdf/PLAW-113publ282.pdf

CONFERENCE PAPERS

Jabbour Mona Achkar, ICAO/UNOOSA Symposium, 2017 for Cyb-Air Security in Civil Aviation 28-31 August 2017, p. 7,. Available at: http://www.unoosa.org/documents/pdf/spacelaw/workshops/2017/ICAOUNOOSA2017/0503_AL-Achkar_Jabbour_Lebanese_Univ_rev.pdf

WEB SITES

- Budapest Convention, available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

- *Civil Aviation Authority (CAA)*, available at: http://www.ypa.gr/our-airports

- ______________________________http://www.ypa.gr/profile/statistics/yearstatistics/

- *ENISA*, National Cyber Security Strategies Training Tool available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool%3E

- EU Computer Emergency Response Team (CERT-EU), available at: https://cert.europa.eu/cert/plainedition/en/cert_about.html

- EUROCONTROL, available at: https://www.eurocontrol.int/articles/who-we-are

- Europol's Cybercrime Centre (EC3), available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- Fraport, available at: https://www.fraport-greece.com/www.mjt-airport.gr

- General Secretariat of Digital Policy (GSDP) http://mindigital.gr/index.php/announcments-ggdp/1109-systasi-tis-genikis-grammateias-psifiakis-politikis

- Global Forum on Cyber Expertise (GFCE) News, available at: https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime

- International Civil Aviation Organization (ICAO), available at: https://www.icao.int/Pages/default.aspx

- IT Governance European Blog, available at: https://www.itgovernance.eu/blog/en/majority-of-eu-member-states-missed-nis-directive-deadline

- IT-Sicherheitsgesetz, available at: http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

- Νόμος 4389/2016. Available at: http://www.publicrevenue.gr/elib/view?d=/gr/act/2016/4389/art/14

- Packet crafting tools http://www.scs.ryerson.ca/~zereneh/cn8822/PacketCrafting.pdf

- Presidential Degree of 82/2017, available at: https://www.e-nomothesia.gr/enemerose-tupos-radiophono-teleorase/proedriko-diatagma-82-2017-fek-117a-10-8-2017.html

- The Greek draft law for cybersecurity, available at: https://www.e-nomothesia.gr/law-news/ste-boule-skhedio-nomou-gia-ten-kubernoasphaleia.html

- The Horizon 2020 https://ec.europa.eu/programmes/horizon2020/en/

- The 7th Framework Programme https://ec.europa.eu/research/fp7/index_en.cfm

- The UK aviation cyber-security strategy, from Department for Transport, p. 13.
- https://www.fraport-greece.com/uploads/page_art/0/34//fraport_entypo%20A4_GR.pdf p. 8