Good practices on interdependencies between OES and DSPs

NOVEMBER 2018

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Konstantinos Moulinos, Dr. Athanasios Drougkas, Dr. Kleanthis Dellios, Paraskevi Kasse

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For providing valuable information that helped shape the report (in alphabetical order):

Gitte Bergknut, Information Security Officer, Uniper Sweden
Aurelio Blanquet, Digital Director of Networks Platform, EDP Distribuição
Fredrik Blix, Associate Professor Cybersecurity, Stockholm university
Claudio Caimi, Program Manager, hpe Italiana.
Francesco Di Maio, Head of Security Dept., ENAV SpA Italy
Dr. Georgios Giannopoulos, Scientific Officer, European Commission - DG Joint Research Centre (JRC)
Caroline Greer, Head of European Public Policy, Cloudflare.
Mick Haynes, Technical Director, Hitrail BV
Dr. Marieke Klaver, programme manager, TNO
Aris Lambrianidis, Information Security Manager, AMS-IX
David Lecarpentier, GRTgaz
Antonio E. Lopez, General Manager, Hit Rail BV
Eric Luiijf, Principal Consultant, Luiijf Consultancy
Nuno Medeiros, Head of OT Cyber Security, EDP Distribuição
Jos Menting, Chief Technologist Cybersecurity, ENGIE Laborelec
Jan Neutze, Director of Cybersecurity Policy, Microsoft
Massimo Rocca, Chairman of EE-ISAC
"Jean-François SIMONS, Chief Information Security Officer – Data Privacy Officer, Brussels Airlines
Dr. Marianthi Theocharidou, Project Officer, European Commission - DG Joint Research Centre (JRC)
Philip Westbroek, OT Security Officer, Enexis Netbeheer

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-265-3, DOI 10.2824/124305

Table of Contents

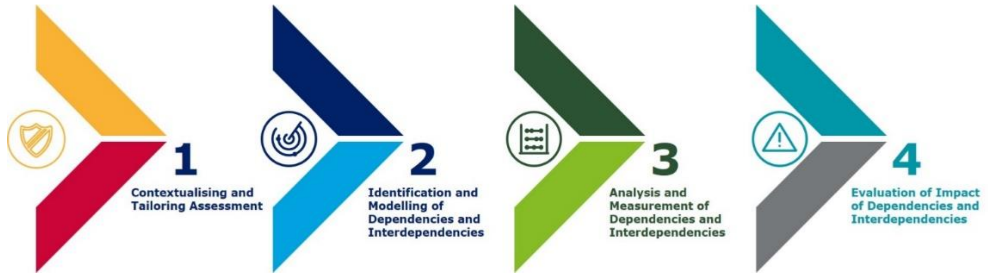
Executive Summary

The Network and Information Security (NIS) Directive[1] entered into force in 2016, becoming the first piece of European legislation dealing with cybersecurity. The directive was created with the objective of boosting the overall level of cybersecurity in the European Union. It does so by increasing the cybersecurity capabilities in the Member States, by enhancing cooperation on cybersecurity among the Member States, and by requiring Operators of Essential Services (OES) and Digital Services Providers (DSPs) to manage their risks. In relation to the latter, an important element of the risk to be assessed is the one of the dependencies of the services offered on other services of either OES or DSPs. These dependencies might be of either national or cross-border nature.

A glance at the interdependency landscape reveals a number of emerging interdependencies between OES/DSPs at both system and service level. There is an increasing number of cybersecurity incidents that, due to these interdependencies, either propagated across organisations, often across borders, or had a cascading effect at the level of essential services.

Yet, despite the clear need to address interdependencies as part of their overall cybersecurity risk management, organisations and National Competent Authorities (NCAs) face difficulties due to the lack of suitable methods, tools, available data and expertise.

In order for OES, DSPs and National Competent Authorities (NCAs) to effectively identify and assess interdependencies, a framework based on a 4-phase approach appears to be a suitable way forward. Existing methods, tools and good practices for interdependencies can easily be mapped to these 4 phases based on the respective individual or sectorial specificities and needs. The development of indicators for the interdependencies' assessment, which are mapped to well-known and widely used industry standards and frameworks would also constitute a practical approach.


1
Contextualising and Tailoring Assessment
2
Identification and Modelling of Dependencies and Interdependencies
3
Analysis and Measurement of Dependencies and Interdependencies
4
Evaluation of Impact of Dependencies and Interdependencies

This report includes a set of recommendations for OES, DSPs and NCAs to effectively address interdependencies in their risk assessments, including:

- OES and DSPs should conduct **empirical investigations** to collect data
- OES, DSPs and NCAs should develop and integrate **methodologies and tools**
- OES and DSPs should develop expertise via **awareness and training**
- NCAs should work towards developing a **common taxonomy** of incident impact assessment
- OES and DSPs should address interdependencies at **operational level**
- NCAs should facilitate **information sharing**.

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

1. Introduction

The European Commission has adopted a series of measures to enhance Europe's capabilities addressing the increasing risks of cyber attacks and incidents in terms of frequency of occurrence and severity of impact. These measures aim at making the online environment more trustworthy and therefore supporting the functioning of the European Union's Digital Single Market[2]. Among such measures, the European Parliament and the Council reached an agreement about the Directive[3] on the security of network and information Systems (NIS Directive). The NIS Directive represents the first step of an EU-wide strategy and legislation on cybersecurity. This report is part of a series of ENISA activities supporting the implementation of the NIS Directive.

1.1 Scope and objectives

This study is concerned with dependencies and interdependencies among Operators of Essential Services (OES) and Digital Service Providers (DSPs) as defined in the NIS Directive and addresses emerging dependencies and interdependencies across sectors. Figure 1 depicts different dependencies and interdependencies within the scope of this report as the result of combined dependencies:

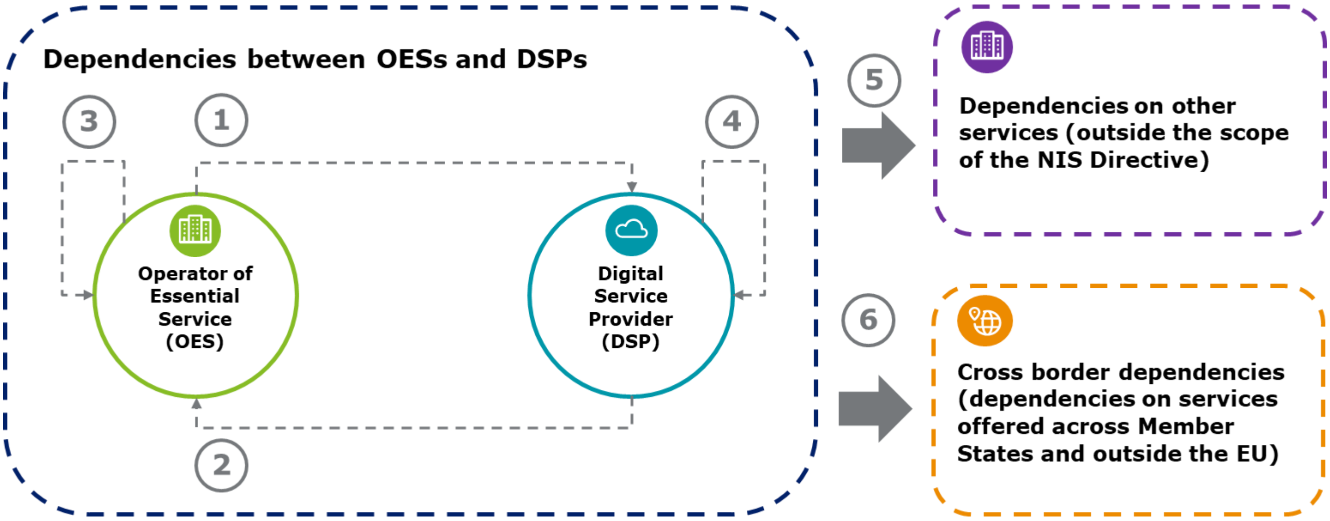

Dependencies between OESs and DSPs
3
1
4
Operator of Essential Service (OES)
Digital Service Provider (DSP)
2
5
Dependencies on other services (outside the scope of the NIS Directive)
6
Cross border dependencies (dependencies on services offered across Member States and outside the EU)

Figure 1 Dependencies (and Interdependencies) among OES and DSPs

The main objectives of the study are:

1. To provide a description of interdependencies among OES and DSP
2. To highlight risk assessment practices for the evaluation of the potential impact of interdependencies
3. To propose a framework for assessing interdependencies
4. To define good practices for assessing interdependencies.

[2] European Commission (2015): A Digital Single Market Strategy for Europe, COM/2015/0192.
[3] European Parliament and the Council (2016): Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30. ELI: http://data.europa.eu/eli/dir/2016/1148/oj

These objectives would support relevant NIS stakeholders, in particular OES, DSP and National Competent Authorities (NCAs) with addressing the risks associated with emerging dependencies and interdependencies. Analysing emerging dependencies and interdependencies would also support decision makers in defining mitigation measures reducing risks, thus enhancing the security of network and information systems.

1.2 Definitions

Guidelines concerning the security and resilience of critical infrastructures[4] provide definitions for dependency as *"the one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly"* – and for interdependency as *"mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions"*.

Taking into consideration the scope of this report, these definitions emphasise the directional aspects of dependency and interdependency and highlight the directional relationships between services (OES and DSPs), rather than simply on the underlying infrastructures. This characterisation is necessary in order to take into account subtle interactions among services in operations and simultaneously aligns with the definitions provided by the NIS Directive:

Dependency: *A linkage or connection between two services (or underlying infrastructures), through which the state of one service (infrastructure) influences or is correlated to the state of the other*

Interdependency: *A bidirectional relationship between two services (or underlying infrastructures) through which the state of each service (infrastructure) influences or is correlated to the state of the other. More generally, two services (infrastructures) are interdependent when each is dependent on the other.*

Nevertheless there are additional characteristics highlighting the nature of (inter)dependencies and their potential impact on services, classifying the relationships (and the related impact on services) into cross-border, cross-sectorial, spatial and functional interconnectedness and dependency[5].

- **Cross-border (inter)dependencies** refers to services' (inter)dependencies between OES themselves, between DSPs themselves, and between OES and DSPs operating in two or more different Member States.
- **Cross-sector (inter)dependencies** refers to services' (inter)dependencies between OES, between DSPs, and between OES and DSPs operating in different sectors (without excluding the case of OES and DSPs stationed in different Member States).
- **Functional interconnectedness** refers to a situation in which an infrastructure is necessary for the operations of another infrastructure.
- **Spatial interconnectedness** refers to a situation where two infrastructures are in close proximity to each other.

There are also cases with both types of interconnectedness. Three factors influence the results of these (inter)dependencies:

[4] US Department of Homeland Security (2013): National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience.

[5] Zimmerman, R. (2001): Social implications of infrastructure network interactions. Journal of Urban Technology 8(3):97–119. DOI: https://doi.org/10.1080/106307301753430764

- **Interconnectedness and coupling** (which affect how failures propagate through systems);
- **Redundancy** (affecting alternative ways of restoring systems);
- **System knowledge** (for example, which enables identification of threats).

How incidents propagate through (inter)dependencies of services can be described in four different classes: *Physical*, *Cyber*, *Geographic* and *Logical*[6] [7]. Figure 2 provides the graphical representation of these classes of (inter)dependencies among OES and DSPs.

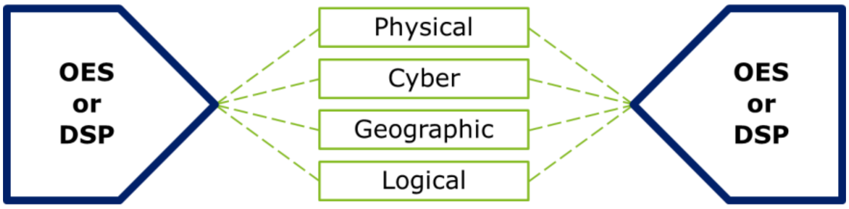


Figure 2 Classes of dependencies and interdependencies among OES and DSPs

- **Physical:** A service (or an infrastructure) is physically dependent if the state of its operations is dependent on the material output(s) of another service (infrastructure) through a functional and structural linkage between the inputs and outputs of two assets.
- **Cyber:** A service (or an infrastructure) is cyber dependent if its state of operation depends on information and data transmitted through the information service (infrastructure) via electronic or informational links.
- **Geographic:** A service (or infrastructure) is geographically dependent if a local environmental event can create changes in the state of operations in all of them. A geographic dependency occurs when elements of service (infrastructure) assets are in close spatial proximity (e.g. a joint utility right-of-way).
- **Logical:** A service (or an infrastructure) is logically dependent if its state of operations depends on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes; for instance, demand for services may shift from an infrastructure that does not function properly to another infrastructure that provides similar services.

This formulation suggests that (inter)dependencies transcend individual infrastructure sectors. As such, they vary in scale and complexity, ranging from local linkages to international linkages. Their differences create a variety of spatial, temporal, and system complexities that are difficult to identify, represent and analyse. Therefore, based on the impact of dependencies and interdependencies, infrastructure (inter)dependencies classified in three general categories:

- **Cascading failure:** how disruption in one infrastructure causes a disruption in the second
- **Escalating failure:** how a disruption in one infrastructure exacerbates an independent disruption of a second
- **Common cause failure:** disruptions of two or more infrastructures is due to a common cause.

1.3 Methodology

This report was developed using information deriving from the following streams:

[6] https://publications.anl.gov/anlpubs/2015/06/111906.pdf
[7] https://www.sciencedirect.com/science/article/pii/S1874548214000262

- **Desk research** of public documents and research papers focusing on the dependencies and interdependencies among OES across sectors and types of digital services;
- **Online survey** to collect feedback from relevant stakeholders; and
- **Interviews** with experts from different sectors of OES, DSPs and researchers and experts in different related areas (e.g. information security, risk assessment, modelling, etc.);

Interviews were conducted with a total of **25 experts** from **11 Member States**. Experts from different OES and DSPs provided feedback for the challenges of the respective sectors covering several sectors and sub-sectors of the NIS Directive, including **Energy** (Electricity and Gas), **Digital Infrastructure** (DNS and IXP), **Transport** (Rail and Air) and **DSP** (Online Marketplace and Cloud Computing). Experts from Research & Academia, Security Consulting and IT Security Services were interviewed to provide a different point of view.

1.4 Target audience

The target audience of this study is:

- **OES** across all sectors and **DSPs** who have to assess the risks associated with emerging dependencies and interdependencies in their operations.
- **Policy makers and NCAs** who are concerned with the implementation of the NIS Directive or for conducting national risk assessments and the adoption of relevant good practices.

1.5 Structure of the document

The rest of the document is structured as follows:

- Dependencies and Interdependencies: providing a characterisation of emerging dependencies and interdependencies, including a sectorial analysis (Section 2).
- Framework for Assessing Dependencies and Interdependencies: proposing a methodological framework for assessing dependencies and interdependencies and reviewing practices and methodologies supporting this assessment. It also highlights experiences drawn from National Risk Assessments (Section 3).
- Indicators for interdependencies: presenting a list of indicators as part of the framework for the assessment of dependencies and interdependencies (Section 5)
- Good Practices for Dependencies and Interdependencies: discussing challenges and good practices for OES/DSPs and NCAs when assessing dependencies and interdependencies (Section 4).
- Conclusions and Recommendations: highlighting key conclusions and providing recommendations for future initiatives concerned with emerging dependencies and interdependencies (Section 7).

2. Dependencies and Interdependencies

2.1 Examples of cyber incidents with a cross-sector or cross-border impact

Recent cyber incidents (e.g. WannaCry, Petya, NotPetya, Stuxnet, etc.) provide instances of the potential impact on different sectors and countries. Table 1 provides a schematic analysis of the impact of different recent cyber incidents. It highlights the type of threat, the affected sectors, users, countries and systems[8].

Table 1 Examples of cyber incidents and their potential impact

CYBER INCIDENT	TYPE OF THREAT	AFFECTED SECTORS	AFFECTED USERS	AFFECTED COUNTRIES	AFFECTED SYSTEMS
WannaCry	Ransomware	Cross-sector propagations (e.g. Telecom and Health)	Multiple users (more than 250 victims paid a ransom)	Cross-border propagations affecting multiple countries (more than 150 countries)	Operating Systems (more than 230.000 systems)
Petya	Ransomware	Multiple Sectors	Multiple users	Multiple Countries (e.g. Ukraine, USA, Russia, France, UK, Germany, India, China, etc.)	Operating Systems
NotPetya	Malware	Multiple Sectors (e.g. Finance, Transportation, Energy, Commercial facilities, and Healthcare)	Multiple users	Multiple Countries (e.g. Ukraine, Russia, Denmark, France, UK, Belgium, USA, etc.)	Software Application (i.e. the MEDoc Tax and accounting software package)
SamSam	Ransomware	Multiple Sectors (including Transport and Health)	Multiple users (of the attacked services)	Multiple Countries	Targeted infrastructures
VPNFilter	Malware	Multiple Sectors	Multiple users	Multiple Countries	Infect certain routers and network attached-storage (NAS) devices
Stuxnet	Malware	Energy	Multiple users	Multiple Countries (mainly Iran but also Indonesia, India, etc.)	Industrial Control Systems (ICS), Programmable Logic Controllers (PLCs), SCADA systems
BlackEnergy	Trojan	Energy	Multiple users	Multiple Countries	SCADA distribution management systems

[8] Note that the table refers to the affected countries, because cyber incidents can propagate beyond regional areas and beyond Member States. Moreover, it reports the impact of incidents based on reports that may rely on partial and incomplete analyses. It is often difficult to have final accurate assessments due to the different reporting channels that highlight partial assessments.

- **WannaCry (Ransomware) – Incident description:** WannaCry was a global (worldwide) ransomware cryptoworm cyber attack, which targeted computers running Microsoft Windows operating system. It encrypted data and demanded ransom payments in Bitcoin cryptocurrency; **Impact:** The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230.000 systems. The economic impact of the WannaCry incident is estimated in the order of hundreds of million euros with some cyber risk modelling analysts placing the losses in the order of billions[9]. **Insights:** The attack started just before the weekend (on Friday). This made it very difficult for companies and organisations to quickly react and resolve the crisis. Although security patches were available, most systems still had unpatched vulnerabilities. The attack presented an increasing complexity (in terms of speed of spreading and sophistication).
- **NotPetya (Malware) – Incident description:** A fake Ukrainian tax software update (in June 2017) spread laterally through infected networks like a worm, using attack vectors Supply Chain ME.doc and the EternalBlue and EternalRomance exploits; **Impact:** NotPetya, a variant of the older Petya attack, charged $300 in ransom from victims in more than 100 countries; NotPetya had significant economic impact for a number of companies whose estimated losses in revenue alone are estimated at over 800 million euros[10]. **Insights:** Although the attack channel may be similar to other cyber attacks, NotPetya seemed targeting specifically Ukranian government and organisations – suggesting the involvement of organised crime or coordinated hacker groups (e.g. State-sponsored attacks).
- **SamSam (Ransomware) – Incident description:** SamSam ransomeware attacks affected different organisations across sectors, the ransomware encrypts data and demand a huge ransom payment in Bitcoin in exchange for the decryption keys.; **Impact:** SamSam has attacked different large organisations across sectors, including Transport (e.g. COSCO attack) and Health; SamSam has earned its creator(s) more than 5 million euros since late 2015, a figure that does not take into account revenue losses and system restore costs[11]. **Insights:** Differently from other ransomware attacks, SamSam targets specific organisations' infrastructures rather than spreading accidentally over the Internet.

Figure 3 depicts one example of how cross sector and cross border propagation of incidents may occur.

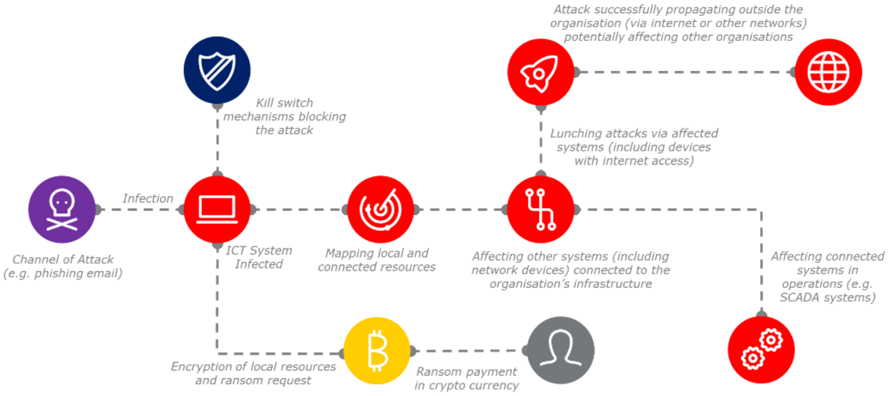

Attack successfully propagating outside the organisation (via internet or other networks) potentially affecting other organisations
Kill switch mechanisms blocking the attack
Lunching attacks via affected systems (including devices with internet access)
Infection
Channel of Attack (e.g. phishing email)
ICT System Infected
Mapping local and connected resources
Affecting other systems (including network devices) connected to the organisation's infrastructure
Affecting connected systems in operations (e.g. SCADA systems)
Encryption of local resources and ransom request
Ransom payment in crypto currency

Figure 3 Chain of events resulting in cross border / sector propagations

[9] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

[10] https://www.cybereason.com/blog/blog-notpetyas-fiscal-impact-revised-892-5-million-and-growing

[11] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

EUROPOL's cybercrime report[12] highlights how such type of attack (having cross sector and cross border impact) is becoming common and further sophisticated. The incidents' review points out the complexity of different types of attacks and their potential impact cross sector and cross border.

This also suggests that risk assessments need to take into account realistic scenarios in order to provide insights on emerging dependencies and interdependencies.

2.2 Landscape of cyber (inter)dependencies

In this section, the landscape of cyber (inter)dependencies among different sectors and types of OES and DSPs, as well as potentially sectors beyond the scope of the NIS Directive (e.g. telco or mobile communications) is identified. Taking into account relevant studies in Critical Infrastructure Protection (CIP) [13], the resulting landscape reveals a complexity of the relationships[14] across sectors and their related services. Any disruption on their operations may affect the cyber-security of these sectors and have either a cross-sector (or even a cross-border) impact on the provided services. However, the examples (as presented in the following sub-sections) acknowledge cross-sector (inter)dependencies as sources of vulnerabilities and often point out mutual functional relationships among almost all sectors of critical infrastructures (although in general terms).

The semantics of these cyber security incidents/attacks also suggest that the energy and telecommunication sectors often drive cascade effects of critical infrastructure failures, whereas, other sectors rather are victims of emerging dependencies and interdependencies[15].

Due to the digitalisation of services, all major sectors[16] have an increasing level of cyber (inter)dependencies on digital infrastructures and DSPs. By analysing current and best practices within different industrial sectors in the ways OES adopt the digital services, the identified key (inter)dependencies of OES on DSPs as confirmed by means of interviews[17] with involved stakeholders (representatives of OES and DSPs) are highlighted in Figure 4. It should be clarified that these are the identified (inter)dependencies and the list should not be considered exhaustive.

The variation among the degrees of dependencies (i.e. low, medium, high) is defined by using the qualitative information as collected from the professional opinion of interviewed experts while taking into consideration the cross-sector factor, as follows:

- **LOW** = the OES capability to successfully carry out core mission/business functions has a limited dependency on a DSP (for operational, security, risk management, compliance purposes)
- **MEDIUM** = the OES capability to successfully carry out its core mission/business functions has an average dependency on a DSP (for operational, security, risk management, compliance purposes)

[12] EUROPOL (2018): Internet Organised Crime Threat Assessment (IOCTA), European Cybercrime Centre (EC3).

[13] European Commission, Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure, 28.8.2013, SWD(2013) 318 final.

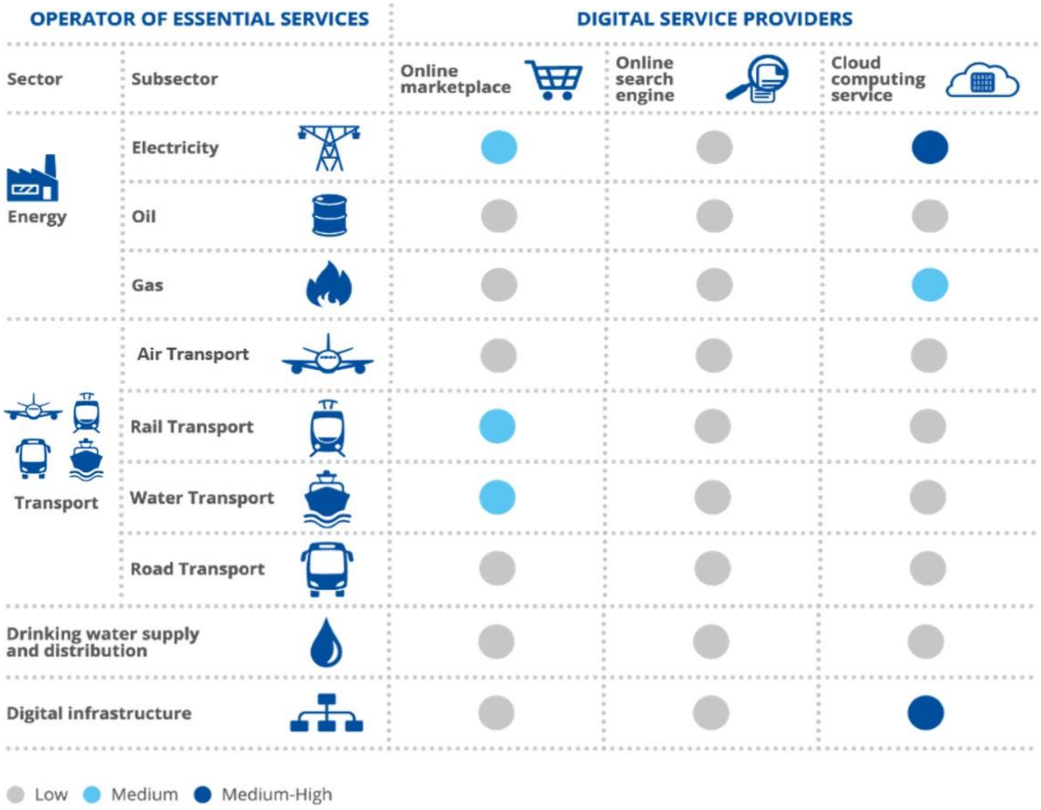
[14] Note that there are not only complex relationships across sectors, but also within sectors. For example, charging service providers and producers of invertors for solar panels (who offer internet access to production figures) control large amounts of power and cyber incidents might affect the stability of grid operators' stability.

[15] European Commission, Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), 22.6.2012, SWD(2012) 190 final.

[16] Without excluding the telecom operators (although the NIS Directive does not directly cover them).

[17] note that not all categories of OES use or are depending, to the same extent, on the services provided by DSPs

- **HIGH** = the OES capability to successfully carry out its core mission/business functions has critical dependency on a DSP (for operational, security, risk management, compliance purposes).



OPERATOR OF ESSENTIAL SERVICES		DIGITAL SERVICE PROVIDERS		
Sector	Subsector	Online marketplace	Online search engine	Cloud computing service
Energy	Electricity	◉	○	●
	Oil	○	○	○
	Gas	○	○	◉
Transport	Air Transport	○	○	○
	Rail Transport	◉	○	○
	Water Transport	◉	○	○
	Road Transport	○	○	○
Drinking water supply and distribution		○	○	○
Digital infrastructure		○	○	●

○ Low ◉ Medium ● Medium-High

Figure 4: Dependencies of Operators of Essential Services on Digital Service Providers (overview)

Despite the efforts of OES in dealing with external parties (e.g. DSPs), it is challenging and difficult to measure and assess the effectiveness of managing dependencies due to the complexity. Moreover, OES need to verify effectively the trustworthiness of DSPs with respect to their security practices and processes in operations. Typically, in order to address risks, common practices involve specifying security requirements into contracts, Service Level Agreements (SLAs), Operational Level Agreements (OLAs) and other formal agreements. However, such contracts and agreements can still leave some uncertainties about (shared) duties, responsibilities and obligations in operations. Moreover, it can be difficult to clarify such uncertainties in case of cybersecurity incidents (e.g. data breaches) affecting complex ICT systems and services. Nevertheless, organisations in some cases may have limited ability to negotiate security requirements. Sometimes, it is simply unrealistic to expect DSPs meeting stringent security requirements in operations.

Of course, key cyber (inter)dependencies for OES and DSPs extend beyond the scope of the NIS Directive. For instance, trust certificates at the infrastructure/service level are necessary in order to support transactions with parties (e.g. for e-government, a high level of trust between the different systems is needed).

In the following paragraphs, a brief overview of the respective cross-sector and of OES on DSPs (inter)dependencies are provided. The reason the examples are provided is for emphasizing the necessity to provide methodologies for identifying and understanding cyber (inter)dependencies in order to mitigate any risk associated with security incidents as the impact of cyber-security incidents may propagate across sectors.

2.2.1 Emerging (inter)dependencies in energy

Energy operations are possible thanks to a combination of goods and services that include digital services, finance, digital infrastructure and transport. The **energy sector** also has dependencies with **financial market infrastructures**. In economic terms, energy (i.e. electricity, oil and gas) is a commodity that can be bought, sold and marketed. In the past, monopoly-based organisational structures were the common ways of selling and exchanging energy[18].

Nowadays the digitalisation of the energy sector has also transformed related financial market infrastructures[19] that support the negotiation of energy in real time in order to make the market efficient. This highlights the increasing cyber dependencies with **digital infrastructures** and digital services such as cloud computing becoming key elements supporting daily activities in the energy sector.

Moreover, within the energy subsectors of the NIS directive (Electricity, Oil and Gas), the distribution and supply phases (or the activities concentrated in the downstream for the Oil and Gas sectors) in the value chains present the most interest of the emerging (inter)dependencies on DSPs. This is due to the fact that **distribution** and **supply** phases are the ones that have stronger market drivers (than other phases such as production and transmission) targeting at innovation and competition.[20] Cloud services enable data usages regardless of the data storage location while connecting different teams from around the world, enabling them to share information instantly and expedite the development process[21].

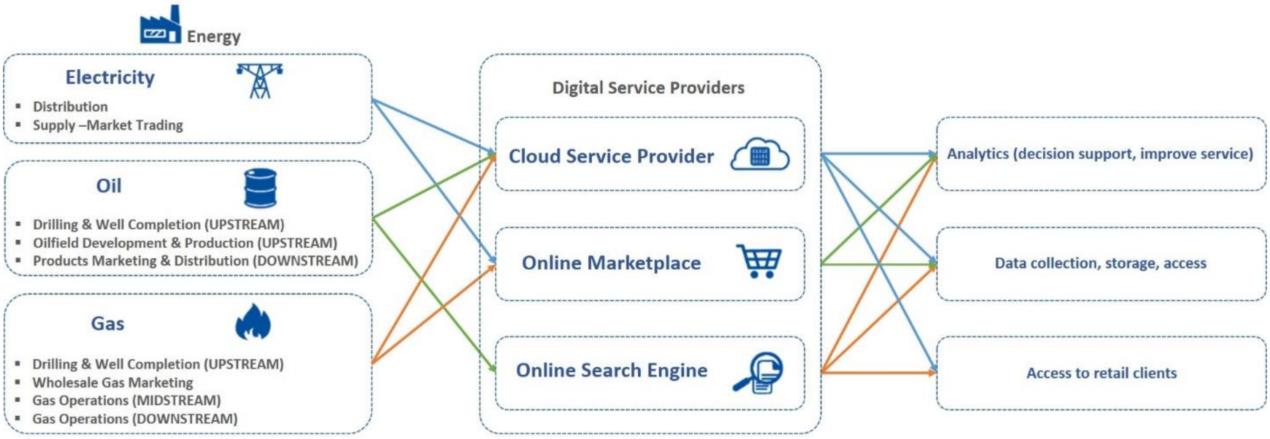

Energy
Electricity
Distribution
Supply –Market Trading
Oil
Drilling & Well Completion (UPSTREAM)
Oilfield Development & Production (UPSTREAM)
Products Marketing & Distribution (DOWNSTREAM)
Gas
Drilling & Well Completion (UPSTREAM)
Wholesale Gas Marketing
Gas Operations (MIDSTREAM)
Gas Operations (DOWNSTREAM)
Digital Service Providers
Cloud Service Provider
Online Marketplace
Online Search Engine
Analytics (decision support, improve service)
Data collection, storage, access
Access to retail clients

Figure 5: Elements of the Energy value chain that depend most on DSPs

[18] Barton, B., et al. (2004): Energy Security: Managing Risk in a Dynamic Legal and Regulatory Environment. Oxford University Press.

[19] Note also that the energy transition requires a lot of effort from especially regional grid operators.

[20] This applies mainly to centralised production; as decentralised production becomes more prominent, dependencies on digital services grow as well.

[21] Saputelli, L. A., Bravo C., Moricca, G., Cramer R., Nikolaou, M., Lopez, C., Mochizuki S. (2013): Best Practices And Lessons Learned After 10 Years Of Digital Oilfield (DOF) Implementations, SPE Paper 167269, Presented at the SPE Kuwait Oil and Gas Show and Conference, 8-10 October, Kuwait City, Kuwait. DOI: http://dx.doi.org/10.2118/167269-MS

In the **electricity** sub-sector, there will be new roles due to the digital transformation of electricity systems across the value chain. Digital technologies and services (e.g. smart meters, IoT, cloud services) increasingly enable information flows across the grid and the different value chain phases in order to communicate and provide (real-time and updated) data for operations and customers. In the **distribution** phase, many electricity operators are strategically investing in and acquiring advanced capabilities, which allow customers to choose their energy supply mix in order to address their demands.

One example is EnergySage[22], an online marketplace that enables comparison-shopping among pre-screened solar installers and financiers and a number of utilities. Another example, in the electricity subsector where demand and offer of electricity are traded through specialised online marketplaces is Nord Pool - a specialised online marketplace for the energy market in northern Europe[23].

The **supply** phase involves different stakeholders ranging from infrastructure providers, utility retailers and customers (both commercial and private end users). In the supply phase, cloud computing and IoT (e.g. smart metering) have the greatest impact and involve customers' interaction. Some of the digital technologies currently employed by electricity involve **cloud** computing services, IoT and services such as big data and analytics, impacting the interactions with and offering new digital capabilities to end users and customers.

In the **oil** subsector, there is an emerging dependency on massive data connectivity, on **cloud** services and infrastructures. The oil industry is prototyping new and connected technologies to reduce well completion time, maintenance time, etc. through real-time monitoring and advanced analytical software, especially in the areas of fracturing fluids, sand, and logistics management. **Oil-specialised search engines** is another interesting illustrative example of digital services utilised by the oil subsector. More specifically, these specialised search engines (e.g. Datafari) allow oil (and gas) geoscientists to get very quickly an overview of all the data that are necessary for them to decide whether to drill an oilrig.

In the **gas** sub-sector, a forecast from the UK-based Oil and Gas Council[24] indicates that the gas industry stands to benefit particularly from **cloud computing** services. Cloud adoption is one of the main IT trends for oil and gas in 2017, alongside with the Internet of Things (IoT), drones, intelligent rigs, and leak-detection software.

2.2.2 Emerging (inter)dependencies in transport

The increasing digitalisation of the **transport sector** makes it highly dependent on **digital infrastructure** and **DSPs**. The transport sector is highly reliant on digital services such as online marketplaces, online search engine and cloud computing services for their daily operations. For instance, unavailability of such services would severely impact automated airport processes such as online check-in, self-service luggage, ticketing, etc., resulting in flight delays, financial and reputational losses.

The cyber (inter)dependencies of the transport sector are likely to increase due to the digitalisation and integration of transport services (e.g. multimodal transport).

[22] EnergySage: https://www.energysage.com/
[23] Nord Pool Market: http://www.nordpoolspot.com/
[24] UK Oil Gas Council (2017): The forecast for oil & gas IT.

The digitalisation of transport services (including the adoption of autonomous cars) will likely increase the cyber dependencies and interdependencies of the transport sectors (e.g. dependencies on digital services, interdependencies among transport services, dependencies on energy sector, etc.).

Another dependency of the **transport sector** is on the **energy sector**. A study[25] on the energy sector highlights the potential effects of energy disruptions on other essential services. In particular, the transport sector may be exposed to energy disruptions on the Electricity and Oil/Gas sectors.

- ***Disruptions to electricity will potentially have an impact on electric public transportations, signal and control systems, transport of fuel and shipping of goods and materials as well as transport information systems (arrival times, platforms, etc.) and may affect ticket machines and turnstiles***
- ***Disruptions to oil/gas will potentially have an impact on fuel and lubricants for vehicles and facilities, transport of fuel and shipping of goods and materials.***

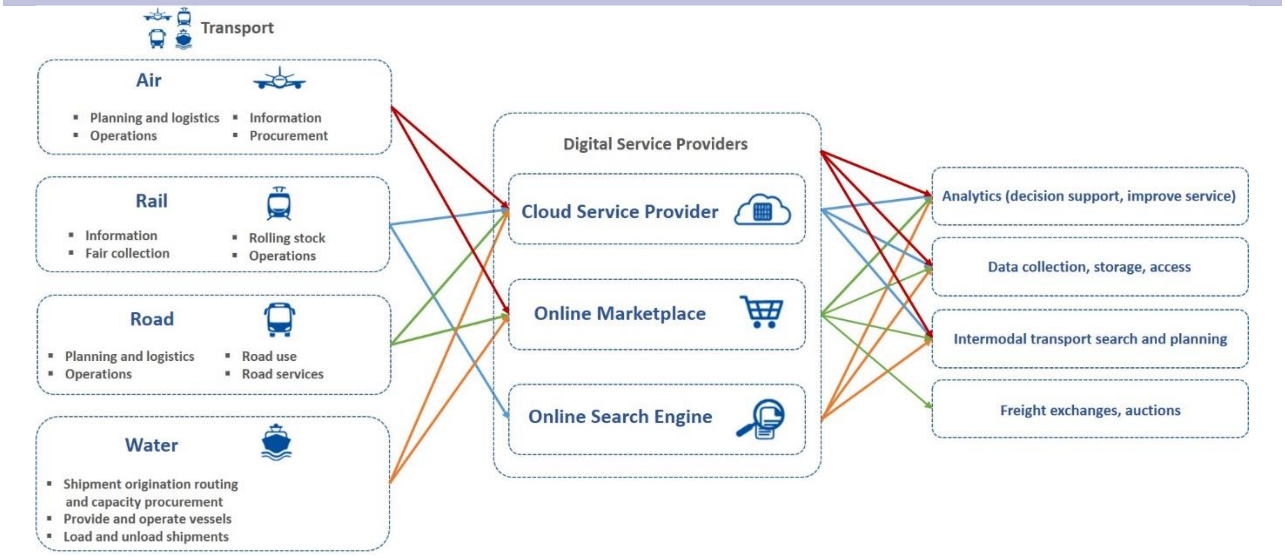

Transport
Air
Planning and logistics
Operations
Information
Procurement
Rail
Information
Fair collection
Rolling stock
Operations
Road
Planning and logistics
Operations
Road use
Road services
Water
Shipment origination routing and capacity procurement
Provide and operate vessels
Load and unload shipments
Digital Service Providers
Cloud Service Provider
Online Marketplace
Online Search Engine
Analytics (decision support, improve service)
Data collection, storage, access
Intermodal transport search and planning
Freight exchanges, auctions

Figure 6: Elements of the Transport value chain that depend most on DSPs

The **rail** sub-sector exhibits increasing dependencies on DSPs, particularly in the operations due to the increasing adoption of **online marketplaces** (e.g. for ticketing), online search engines (e.g. for marketing), cloud computing services (e.g. for information sharing). Illustrative cases of **cloud** services applied to support the business of rail companies may include sharing of information and services of public importance, such as the train timetables, scheduling information, seats reservations, monitoring of freight cars, e-ticketing and public procurement. Higher level of rail transport traffic safety can be achieved with support of **cloud** computing services that facilitate cooperation of the autonomous traffic and transportation systems (especially in the area of distributed information systems, web user interface, integrated database available on the Internet, effective reporting, etc.). Moreover, interoperability of rail transport data and better information sharing between operators is also facilitated by the use of services provided by the **cloud** DSPs.

[25] NIST (2016): Guide Brief 5 – Assessing Energy System Dependencies, NIST Special Publication 1190GB-5. DOI: http://doi.org/10.6028/NIST.SP.1190GB-5

In the **road** sub-sector, online road transport marketplaces are portals where transportation capacity is bought and sold - typically, these can be categorized as vertical marketplaces as they deal specifically with road transportation and sometimes with other added-value services for transportation management. There is an increasing number of transport operators (whether for rail, road or water) that are adopting **cloud computing technologies and services** to streamline their business, operations, to improve workflows and to allow data sharing among a broader audience in their supply chain. Moreover, **transport OES make use of cloud computing services for geospatial applications**. **Cloud based GIS systems and applications** can also compile information from a wider array of sources via the web, encouraging data sharing among stakeholders to support the interdisciplinary nature of transportation services (inter-modality). Collaboration through cloud based applications or systems can increase efficiency by allowing access to the same data set and eliminate duplicated data collection activities.

The **air** sub-sector has typically been a closed environment that exhibits low dependency regarding the feasibility of the adoption of **cloud computing** in order to support the exchange of information among[26] Air Navigation Service Providers (ANSPs), though cloud is being used especially for office automation, while **online marketplace** are used for procurement. Although, broader adoption of cloud computing is under consideration in order to reduce operational costs and to improve the overall system resilience and continuity, no DSPs are involved in core operational services.

In **water transport,** typical applications involving cloud services for water transport operators are related to[27] ship/ fleet management, maintenance management, document management and reporting.

2.2.3 Emerging (inter)dependencies in banking and financial market infrastructures

The sectors of banking and financial market infrastructures show a high level of dependency on the **digital infrastructure** and **DSPs**. This is because the activities of these sectors involve electronic transactions that rely on digital infrastructures and services. For example, banking and financial market infrastructures' operators depend on digital infrastructure operators managing Top-Level Domain (TLD) name registries.

Another example is the sector's dependency on Society for Worldwide Interbank Financial Telecommunication (SWIFT), the world's leading provider of secure financial messaging services, which as of 2015 linked more than 11,000 financial institutions in more than 200 countries and territories

Another example is the sector's dependency on Society for Worldwide Interbank Financial Telecommunication (SWIFT), the world's leading provider of secure financial messaging services, which as of 2015 linked more than 11,000 financial institutions in more than 200 countries and territories. Due to the dependencies of banking and financial market infrastructures on digital infrastructures, there are also secondary dependencies on the energy sector. For example, energy disruptions may have different impacts:

- Disruptions to electricity will potentially have an impact on financial transactions and HVAC (Heating, Ventilation, and Air Conditioning) systems

[26] Currently, considering the IT domain for ENAV, only a raw 20% is weighted as common office activity. Strong commitment and expectations are posed on the SWIM activities, considered an enabler for the civil aviation worldwide and SESAR JU consortium funds are available. There are similar programmes in the USA and other international pan-European air transport services and, worth of note, ICAO is actively working for standardisation.

[27] Pančo Ristov, M. P. V. T. (2014): The implementation of cloud computing in shipping companies. Scientific Journal of Maritime Research.

- Disruptions to oil/gas will potentially have an impact on fuel for heat, generators and facilities.

Indeed, disruptions to energy supplies could potentially trigger a cascade effect on the normal functioning of digital infrastructures and then consequently to banking and financial market infrastructures.

2.2.4 Emerging (inter)dependencies in health

As the health sector is currently undergoing a process of digitalisation, the dependency on the **electricity sector** is essentially the most critical for health services. The case of a power outage is just a practical example that highlights the dependency of health operators on the energy sector for maintaining their services (e.g. on-line prescription, appointment booking, etc.) that depend on networks and information systems (e.g. laboratory information systems, radiology information systems, etc.). In turn, the power generators requiring fossil fuels (mainly, oil and gas) in order to provide electricity to facilities of health operators create a dependency with the rest of the energy sector.

Moreover, the sector is becoming more and more dependent on the **digital infrastructure**.

For example, incidents affecting Domain Name System (DNS) operators may affect health services such as eHealth services relying on online websites (e.g. on-line prescription, appointment booking, telemedicine, etc.).

The dependency with the **drinking water supply and distribution** sector is another critical dependency for the health sector. Water supplies are necessary for cooling systems of operation environments in health services such as data centres (e.g. servers in data rooms, routers, etc.). Healthcare also depends on banking sector services in order to perform several financial transactions (e.g. payroll web applications) to medical staff, suppliers, vendors and other third parties (e.g. electricity suppliers, digital services, etc.).

2.2.5 Emerging (inter)dependencies in drinking water supply and distribution

Services of drinking water supply and distribution depend on different SCADA systems, which need to operate constantly in order to provide the necessary operational information creating a dependency on the **electricity** sector. New digital technologies in the drinking water sector have introduced detailed measurement and near real-time monitoring of water extraction, treatment, distribution, use and reuse, with the potential to distinguish between different water qualities, sources, quantities and users[28].

Among the most relevant categories of data[29] handled by the drinking water sector, the following that produce a large volume can be enlisted: Flow, chemical concentration and laboratory data; Water supply metering and customer usage data; Engineering and construction data; and Water asset performance and maintenance data.

Growth in the variety of data processed by the water supply and distribution operators, particularly unstructured data, is changing the landscape of water data and the manner the use, storage and protection of this data is more and more dependent on the DSPs. For example, the open source

[28] Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks. OJ L 288, 6.11.2007, p. 27–34. ELI: http://data.europa.eu/eli/dir/2007/60/oj
[29] Deloitte (2016): Water Tight 2.0 - Top trends in the global water sector.

unstructured data - web content, social content and crowdsourcing[30] – is changing the landscape of water data.

The information systems that support the ordering, planning and monitoring of chemical supplies create indirectly cyber dependencies on the **transport** sector. However, due to the low level maturity concerning the integration and standardisation of ICT solutions in the respective business processes[31], incidents related to digital infrastructure would have in principle a limited impact on the sector as a whole.

One of the most relevant and obvious opportunities – at the same time, dependencies – that the drinking water supply and distribution operators have is on the **cloud computing services providers**. Drinking water OES are benefitting from the availability of a broad variety of cloud services. In particular, data-related services such as storage and analytics support the digitalisation of several services in the water value chain (hence, the digital water process).

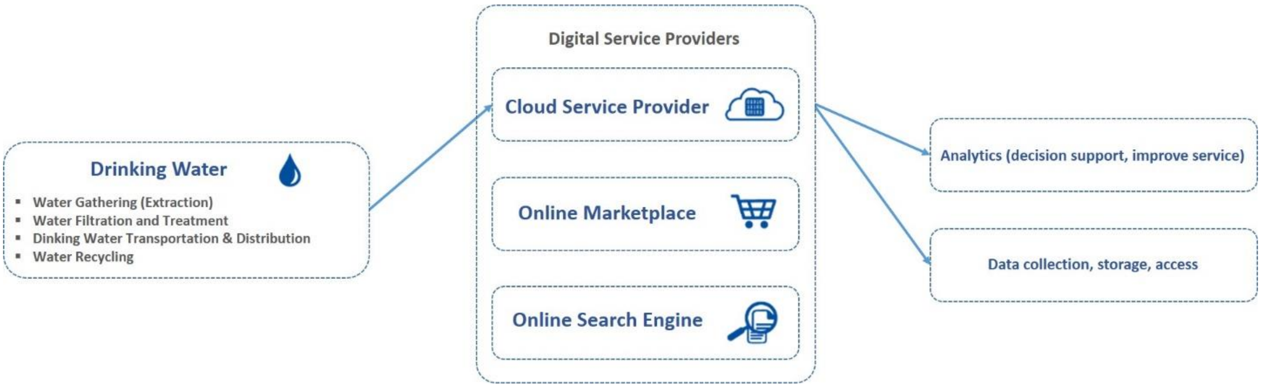

Digital Service Providers
Cloud Service Provider
Online Marketplace
Online Search Engine
Drinking Water
Water Gathering (Extraction)
Water Filtration and Treatment
Dinking Water Transportation & Distribution
Water Recycling
Analytics (decision support, improve service)
Data collection, storage, access

Figure 7 Drinking water value chain elements that depend the most on the DSPs

Moreover, the increasing digitalisation of SCADA systems and reliance on information networks expose the operators of drinking water supply and distribution to potential cyber attacks[32]. Networked, intelligent sensors and decision support systems in real time facilitate data acquisition, monitoring and reporting to make better use of energy, avoid unnecessary water losses and minimize the consumption of resources.

2.2.6 Emerging (inter)dependencies in digital infrastructures

Most sectors are developing an increasing dependency on digital infrastructure services. This is due to the progressive digitalisation of services across sectors. On the other hand, digital infrastructure services also depend on other sectors. For example, a clear dependency relates to how the digital infrastructure relies on servers, storage devices, network switches and data centre infrastructure, as well as a shift to much greater shares of cloud and hyper scale data centres.

[30] One definition of the crowdsourcing is the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers.

[31] European Commission (2018). Report on the Action Plan to foster Digital Single Market for Water Services (ICT4Water).

[32] Birkett, D.M., (2017): Water Critical Infrastructure Security and Its Dependencies. Journal of Terrorism Research. 8(2), pp.1–21. DOI: http://doi.org/10.15664/jtr.1289

Big quantities of energy are needed in order to power this infrastructure. In this regard, Data centres worldwide consumed around 194 terawatt hours (TWh) of electricity in 2014, or about 1% of total demand[33].

Another dependency relates to the water sector. Indeed, cold water is needed in many cases by the datacentre cooling systems for maintaining the system from overheating (e.g. servers in data rooms, routers, UPSs etc.). Moreover, in some cases where the electric energy is produced from dumps, the digital infrastructures has a secondary dependency with the water sector.

2.3 Cross-border (inter)dependencies

In order to have a comprehensive account of (inter)dependencies, it is necessary to discuss and analyse them also from a cross-border perspective, that is, how security incidents affecting services in a Member State may propagate cross-border to services in other Member States.

Cross-border impact provides another dimension for assessing the impact of security incidents and significant incidents may have a cascading effect on different sectors as well as on services across Member States.

In general, it is possible to distinguish three situations, as depicted in Figure 8.

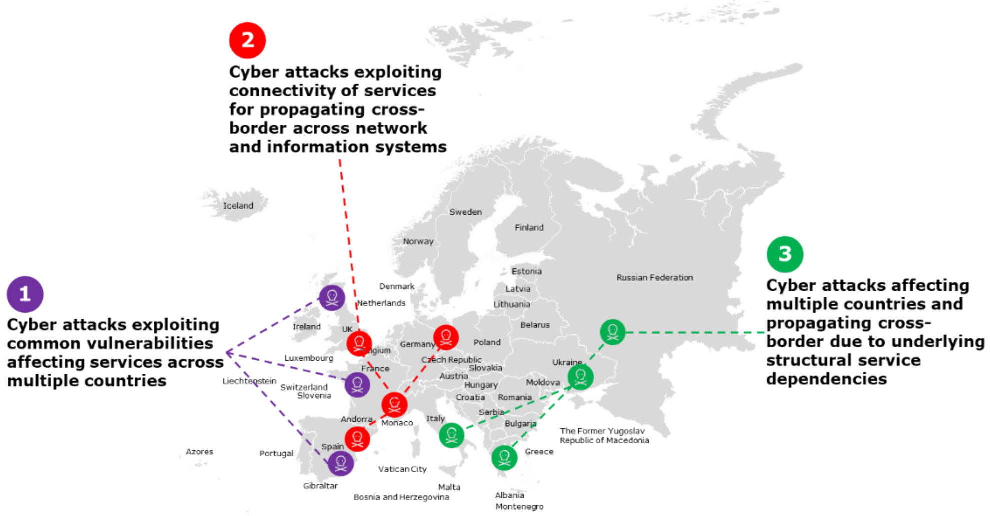

2
Cyber attacks exploiting connectivity of services for propagating cross-border across network and information systems
1
Cyber attacks exploiting common vulnerabilities affecting services across multiple countries
3
Cyber attacks affecting multiple countries and propagating cross-border due to underlying structural service dependencies
Iceland
Sweden
Finland
Norway
Estonia
Russian Federation
Denmark
Latvia
Netherlands
Lithuania
Ireland
UK
Belarus
Belgium
Germany
Poland
Luxembourg
Czech Republic
France
Slovakia
Ukraine
Liechtenstein
Switzerland
Slovenia
Austria
Hungary
Moldova
Croatia
Romania
Serbia
Andorra
Monaco
Italy
Bulgaria
The Former Yugoslav Republic of Macedonia
Azores
Portugal
Spain
Greece
Vatican City
Gibraltar
Malta
Bosnia and Herzegovina
Albania
Montenegro

Figure 8 Cyber attacks with cross-border impact

1. **Common Vulnerabilities.** In such cases, cyber incidents are due to the exploitations of common vulnerabilities and may have an impact in multiple countries as the result of such vulnerabilities, rather than cross border propagation. This type of attack may involve sophisticated technologies or services and often suggests that cyber-attacks target specific services (e.g. large organisations providing services or critical infrastructures) rather than citizens.
2. **Connectivity of Services.** In such cases, security incidents propagate due to the underlying connectivity of sectors operating in different countries. For instance, this is the case of attacks infecting ICT systems and propagating by infecting connected resources or systems. At the sectorial level, essential services may be exposed to cyber-attacks affecting (inter)interdependencies. For example, banking and

[33] IEA (International Energy Agency) (2017). Digitalisation and Energy 2017.

financial market infrastructures depend on service connectivity for financial transactions. Cyber-attacks targeting highly connected banking and financial market infrastructures can have significant propagation effects that cascade into related and neighbouring financial services (e.g. payment and other banking transactions) operating in other countries.

3. **Service Structures.** In such cases, security incidents have a cross-border impact due to structural service dependencies, i.e., security incidents may affect multiple countries, because there exist underlying structural dependencies among services. An example of this might be the case of energy production services that may operate in multiple countries. A security incident affecting energy production would affect the countries that depend on such energy supplies. Other examples involve security incidents affecting Air Transport services (e.g. National Air Traffic Management services) that may also have a cross-border impact due to underlying service structures.

3. Framework for Assessing Dependencies and Interdependencies

An extensive review of the relevant literature regarding good practices, methodologies, approaches and tools revealed significant commonalities as regards the phases for (inter)dependencies risk assessment. This chapter builds on these commonalities to propose a framework for assessing (inter)dependencies, based on a phased approach. For each phase, the relevant **state of the art** in terms of methodologies, practices and tools is presented to allow customised implementation of the framework based on the individual requirements, sectorial specificities, maturity and resources of the different stakeholders who may wish to implement it in practice.

3.1 Introduction to the framework

Integrating the assessment of (inter)dependencies in an overall risk management process is a complex process, particularly in the case of cross-sector or cross-border dependencies and interdependencies. This section provides a framework for assessing (inter)dependencies, which follows common principles of risk management[34, 35] and defines a process consisting of four different phases (Figure 9).

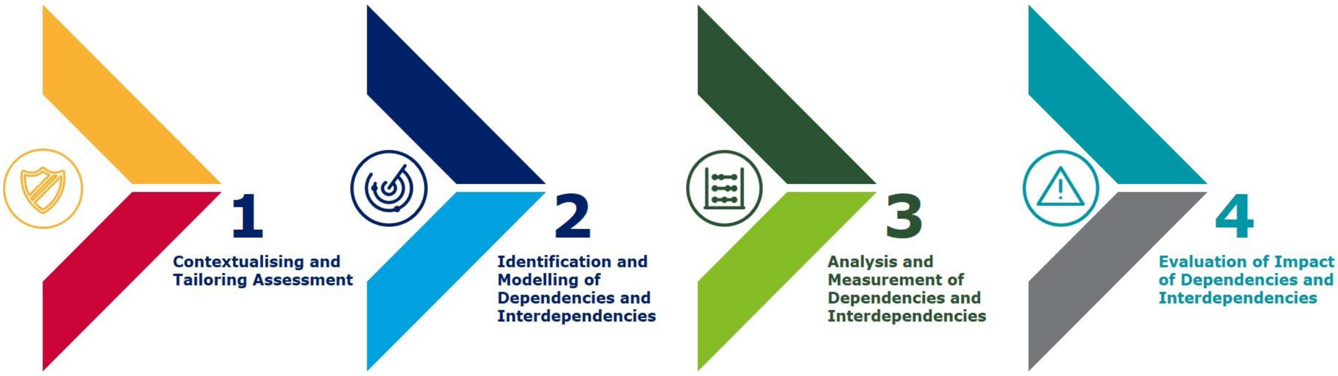

1
Contextualising and Tailoring Assessment
2
Identification and Modelling of Dependencies and Interdependencies
3
Analysis and Measurement of Dependencies and Interdependencies
4
Evaluation of Impact of Dependencies and Interdependencies

Figure 9 Dependency and Interdependency Assessment

1. **Contextualising and Tailoring Assessment:** involves defining the key elements of the (inter)dependencies risk assessment
2. **Identification and Modelling of Dependencies and Interdependencies:** involves diverse methodological approaches, including the analysis of historical data, for the identification and modelling of dependencies and interdependencies among OES and DSPs.
3. **Analysis and Measurement of Dependencies and Interdependencies:** involves analyses, including quantitative analyses, based on different scenarios or simulations of the dependencies and interdependencies among OES and DSPs.
4. **Evaluation of Impact of Dependencies and Interdependencies:** involves the impact assessment, based on the performed analyses and measurements, for the identified and modelled dependencies and interdependencies among OES and DSPs.

For each phase, the following sections provide an overview of different methodologies that take into account such (inter)dependencies between OES and DSPs highlighting the main types of methodological

[34] ISO 31000:2018, Risk management – Guidelines.
[35] ISO 31010:2009 – Risk Management – Risk assessment techniques

approaches, the common risk assessment steps, approaches to metrics and impact assessments, as well as key aspects of National Risk Assessment approaches.

The framework is applicable for:

- **OES/DSPs** for supporting their (inter)dependencies risk assessment
- **NCAs** for integrating (inter)dependencies in their National Risk Assessments (NRAs)

3.2 Contextualising and tailoring assessment

Prior to any methodological approach or tool adopted for conducting any aspects of (inter)dependencies risk assessment, it is necessary to define the assessment's key elements:

- **Scope:** The scope and the scale of risk assessments depend on various factors including the involved critical infrastructures, OES or DSPs taken into account as well as to what extent Member States are vulnerable to security attacks affecting deliveries of services.
- **Cross Border and Regional Dimensions:** Risk assessments highlight that incidents or hazardous conditions may have origins beyond organisational and national boundaries. The nature of cyber threats and the continuous evolution of threat landscape require understanding how cyber incidents may propagate across organisations[36] such as OES and DSPs, and across Member States.
- **Previous Incidents and Lessons Learnt:** The availability of relevant data affects the overall risk assessment (e.g. in terms of accuracy). The most common sources of information supporting risk assessments are, for instance, historical records and databases of events, impacts and recorded losses and damages. Although the sources of information, the ownership and the responsibility may belong to different organisations (e.g. OES and DSPs as well as governmental bodies and authorities such as CSIRTs and NCAs), data on previous incidents provide evidence and understanding of past events, their occurrences and impact (e.g. in terms of damages and consequences).
- **Multi-stakeholder Involvement:** (Inter)dependencies risk assessments typically involve different stakeholders, who may have different responsibilities as well as different risk perceptions and who position themselves differently with respect to emerging risks. It is necessary to involve all relevant stakeholders, who may affect the outcomes of risk assessments.
- **Timeframe:** (Inter)dependencies risk assessments are often conducted at specific time and are constrained by budget; for instance, national risk assessments are conducted with a timeframe of three to five years. Therefore, it is necessary to understand the timeframe of a risk assessment and its validity with respect to emerging threats.

3.3 Identification and modelling of dependencies and interdependencies

The overall objective of this phase is to identify and model relationships, that is, (inter)dependencies among OES and DSP, capturing domain-specific knowledge based on historical data and experts or data insights.

The ISO 31010 standard identifies various techniques that can support risk identification. Such techniques may support different types of activities for gathering stakeholder knowledge (e.g. brainstorming, structured and semi-structured interviews, etc.).

[36] Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., Cruz, E. (2011): The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Administration 89(2):381-400. DOI: https://doi.org/10.1111/j.1467-9299.2011.01926.x

*Among the various techniques for identifying and modelling (inter)dependencies, **risk scenarios** capture contextual knowledge and support the identification of risks for specific environments.*

National Risk Assessments (NRAs) often develop specific risk-based scenarios[37] in order to assess the exposure of critical infrastructures to critical events such as cyber-attacks. In order to develop a comprehensive account of risk, it is necessary to take into account two different aspects of the risk scenarios:

- **Scenario severity and impact:** risk scenarios may capture a single incident differently. Therefore, it is necessary to develop multiple scenarios covering different magnitudes (e.g. in terms of criticality or expected impact) and different interactions among threats or hazards. High-risk scenarios may be associated to highly improbable events having catastrophic impacts. Although these risk scenarios are unlikely, they are required in order to assess the potential impact of critical events.
- **Scenario timeline and scope:** risk scenarios need to have a validity in alignment with foreseen developments (e.g. increasing number of data breaches in the next five years, expected adoption of digital services in the next five years, etc.) This information is necessary in order to clarify the scope (in terms of time and space) of risk scenarios. Risk scenarios may also involve a scope beyond the organisational or national boundaries. For example, severe events may have a cross-border impact affecting services across multiple Member States. Moreover, it is necessary to underpin the main relevant causes or trends.

In order to limit their complexity, risk scenarios may capture individual risks rather than multiple risks. Unfortunately, catastrophic events may be due to interactions among multiple risks causing chains of events having severe impacts. Therefore, it is necessary to understand and to define risk scenarios in order to support **single-risk** as well as **multiple-risk assessments**.

A common pitfall in risk identification is overlooking dependencies that are embedded or hidden in plain sight, such as ICT services that are widely used - thus implicitly taken for granted - but are key services to OES and DSPs.[38]

Existing methodological approaches supporting risk analysis often involve different types of modelling and characterisation of risk (e.g. Fault Tree Analysis, Event Three Analysis, Failure Mode and Effect Analysis, Bayesian Network Analysis, etc.). Methodological approaches supporting risk analyses of (inter)dependencies of OES and DSPs include[39]:

[37] Risk scenarios are representations of risk situations leading to significant impacts, selected for the purpose of assessing in more detail a particular type of risk for which it is representative, or constitutes an informative example or illustration.

[38] Interview referring to Luiijf, E., Klaver, M. (2015). Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Symposium on Critical Infrastructures: Risk, Responsibility and Liability, Vol. 6, Issue 2 pp. 263 – 270.

[39] Ouyang, M. (2014): Review on modelling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety (RESS), Elsevier 121:43-50. DOI https://doi.org/10.1016/j.ress.2013.06.040

1. **Empirical approaches** analyse (inter)dependencies taking into account historical data of incidents (e.g. in terms of frequency and severity of incident patterns) and expert opinions (based on their domain-specific experiences).
2. **Agent based approaches** capture the complexity of (inter)dependencies as interactions of autonomous agents that interact among one another in their environments based on specific rules. Such approaches adopt a bottom-up method and assume the complex behaviour or phenomenon emerge from many individual and relatively simple interactions of autonomous agents.
3. **System dynamics based approaches** represent (inter)dependencies as results of emergent system behaviours. Such approaches take a top-down method to manage and analyse complex adaptive systems involving (inter)dependencies.
4. **Economic based approaches** capture (inter)dependencies as results of economic and market theories involving exchanges of values (e.g. capital, demand, offer, etc.). Such approaches take into account the production and consumption of services (or other related constrained resources).
5. **Network based approaches** capture (inter)dependencies as results of the relationships (e.g. information flows) among individual components. Such approaches model single systems/services by networks and describe their (inter)dependencies by inter-links, providing intuitive representations along with detailed descriptions of their topologies and flow patterns.
6. **Service-based approaches** capture the modelling of interdependencies conducted on the basis of services that infrastructures exchange. This allows the development of a simulation framework which is sector agnostic[40].

A more detailed description of the aforementioned approaches and an overview of the relevant research activities is available in Annex B.

3.4 Analysis and measurement of dependencies and interdependencies

The overall objective of the risk analysis is to assess the likelihood and impact of the identified risks. In a quantitative risk analysis, risks are the combination of the consequences of a critical risk and the associated likelihood of its occurrence[41]. Consequences are the negative effects of a disaster expressed, for example, in terms of human impacts, economic and environmental impacts, and political/social impacts. The probability of occurrence captures (in those situations that it is possible to quantify) the likelihood of occurrence of a hazard (or threat) of a certain intensity, whereas, the severity of impact provides an assessment of the consequences of critical events (occurrence of hazards or threats). Analysis and measurements of (inter)dependencies typically involves:

1. **Scenarios and simulations**; and
2. **Metrics**.

A special case of (inter)dependencies analysis and measurement are the **national risk assessments** conducted by Member States in order to assess their exposure to critical events including natural and

[40] Ihttp://publications.jrc.ec.europa.eu/repository/bitstream/JRC102547/lbna28073enn.pdf

[41] The classical algebraic representation of risk is that Risk is equal to the Impact (severity of hazard/threat consequences) times Frequency (likelihood of occurrences). Note that not all risks are quantifiable, socio-technical aspects of risks highlight the limitation of quantitative approaches to risks. It is necessary to understand also the limitations of risk assessments (and quantification approaches) in order to conduct them properly. For a socio-technical account of risk see: Anderson, S., Felici, M. (2012): Emerging Technological Risk – Underpinning the Risk of Technology Innovation, Springer. DOI https://doi.org/10.1007/978-1-4471-2143-5

man‑made disasters[42]. The conducted national risk assessments provide an overview of current practices adopted by Member States in assessing their exposures to diverse risks (e.g. earthquake, flooding, critical infrastructure disruption, cybercrime, etc.). National risk assessments typically involve developing specific scenarios (or simulations) under which to evaluate (possibly, quantitatively) the risks associated with specific threats. These national risk assessments provide insights in order to define crisis management strategies and contingency plans. National risk assessments are described in more detail in section 3.6.

3.4.1 Scenarios and simulations

The (inter)dependencies risk assessments may involve different types of scenarios and simulations and the scenarios themselves can involve different types of incidents or disruptive events, from natural disasters due to earthquakes to incidents to essential services (e.g. transport incidents such as collisions, explosions of oil and gas pipelines, disruptions of energy supplies, etc.). Examples of cyberattacks, affecting organisations and individuals, targeting OES and DSPs include **syntactic attacks** (using malicious software relevant to intrusion, cyber espionage and sabotage and **semantic attacks** (through the dissemination of incorrect information to affect credibility of the target resources, relevant in the case of cyber subversion).

Other forms of cyber threats have become increasingly relevant, such as the risk of social engineering involving insider manipulation of individual data and installation of malware[43]. Hybrid threats involve military and non-military actions, which state or non-state actors can use in a coordinated manner, often in a disguised and deniable form, to undermine public trust in government institutions or exploiting social vulnerabilities while remaining below the threshold of formally declared warfare. Hybrid threats can involve cyberattacks having an impact on critical information systems causing disruptions to critical services such as energy supplies or financial services. Important components of a scenario-based risk assessment are:

- **Different scenarios for an incident:** it is necessary to develop different scenarios for the same type of incident covering different magnitudes and different interactions among threats.
- **Defined time and space scope of each scenario:** it is necessary to define the scope (e.g. in terms of time and geographical distribution) for each scenario in order to clarify also its validity. Some scenarios may also have a scope beyond the national boundaries involving multiple Member States.
- **Identify underlying cause(s) and important trends:** it is necessary to recognise the underlying causes and important trends (e.g. increasing deployments of Internet of Things, digitalisation of essential services, etc.) that may provide contextual information.
- **Catastrophic Scenarios:** it is necessary to develop also catastrophic scenarios (i.e. highly improbable events to which response is difficult) overwhelming national or organisational capacity to respond (e.g. coordinated cyberwarfare targeting simultaneously all operators of essential services).

Scenarios and simulations, therefore, capture critical events of cyberattacks exploiting vulnerabilities (at organisational and system level) in order to assess the impact on essential and digital services. For example, national risk assessments have taken into account scenarios of cyber terrorism, cyber incident to network and information systems, cyberattacks on electricity services, cyber espionage and cyber activism. Tools can support the analysis and measurement of security incidents affecting dependencies and interdependencies. For example, the EC JRC developed the **Geospatial Risk and Resilience Assessment**

[42] European Commission (2017). Overview of natural and man‑made disaster risks the European Union may face. Commission Staff Working Document, SWD(2017) 176 final.

[43] ENISA (2018). ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends. Version 1.0, ETL 2017.

Platform (**GRRASP**[44]), which supports the analysis of complex networked systems taking into consideration cross-sectoral and cross-border (inter)dependencies. However, such types of tools/platforms are often specialised and require specific expertise. Other tools (e.g. Zero Outage, CIPRTrainer Web Service, etc.) may support the simulation and analysis of crisis conditions for essential services.

3.4.2 Metrics

Metrics are commonly used in quantitative risk assessment approaches to facilitate measurements computing the likelihood of a potential risk and the severity of its impact (or consequence). Metrics used for the evaluation and representation of (inter)dependencies can be grouped in two main categories:

- **Weighted Metrics:** involving measurements of different variables (or indicators) providing specific risk values (e.g. values or percentages of risks). Metrics may require data gathering resulting from scenarios or simulations. Indicative examples of weighted metrics may include number of users affected, geographical distribution of services, number of SLAs with third parties, performance measures related to resilience etc.
- **Nominal Scales:** involving assigning nominal values (i.e. qualitative category labels) associated with different risk levels (e.g. likelihood or impact: very low, low, medium, high and very high.). Indicative examples of nominal scale metrics may include social, economic or environmental impact, loss of service capabilities, criticality of services in terms of security, coupling and complexity of services etc.

When analysing and measuring (inter)dependencies, it is also possible to create correspondence between the results of weighted metrics and nominal scales, thus combining qualitative and quantitative assessments.

Note that deciding whether to adopt either a qualitative or a quantitative approach (or a combination of both) depends on different factors (e.g. data availability, expert involvement, etc.) that need to be evaluated case by case. The level of awareness and maturity on the topic of (inter)dependencies is key in this decision. In order to analyse and measure risks associated with (inter)dependencies, specific challenges need to be addressed, in particular the **lack of data** - including unavailable, untrusted and incomplete data - and **lack of expertise** in conducting (inter)dependencies risk assessments.

OES and DSPs rely on their own historical[45] data or specific data sets coming from the industry itself (e.g. insurance companies) to conduct such risk assessments. On the other hand, the most common sources of information used by Member States in their NRA are historical records and databases of events, impacts and recorded losses and damages. One additional challenge is that different organisations (both public and private) may often own and manage proprietary databases. This may limit the data availability for conducting risks assessments. It is necessary to support information sharing (e.g. by incentives, developing

[44] https://ec.europa.eu/jrc/en/grrasp GRRASP consists of a distributed architecture involving open source technologies, which bring together geospatial technologies and computational tools for the analysis and simulation of critical infrastructures. It allows information sharing and constitutes a basis for future developments in the direction of collaborative analysis and federated simulation. It takes into account security concerns in the information sharing process (managing users and roles consistently). GRRASP can be deployed in separate servers and used by EU Member States as a means to facilitate the analysis of risk and resilience in critical infrastructures. It supports analyses of critical infrastructure disruptions at local, regional, national and international level. GRRASP follows a tiered approach – Tier 1 modules can be used for the analysis of critical infrastructures at sectoral level, Tier 2 modules for cross sector analyses (of dependencies and interdependencies), and finally Tier 3 modules for high level economic impact of critical infrastructure disruptions at state level.

[45] It should be noted that when assessing past incidents / historical data, lack of such information or absence of previously materialised risks should not be interpreted as reduced likelihood that a risk may occur in the future.

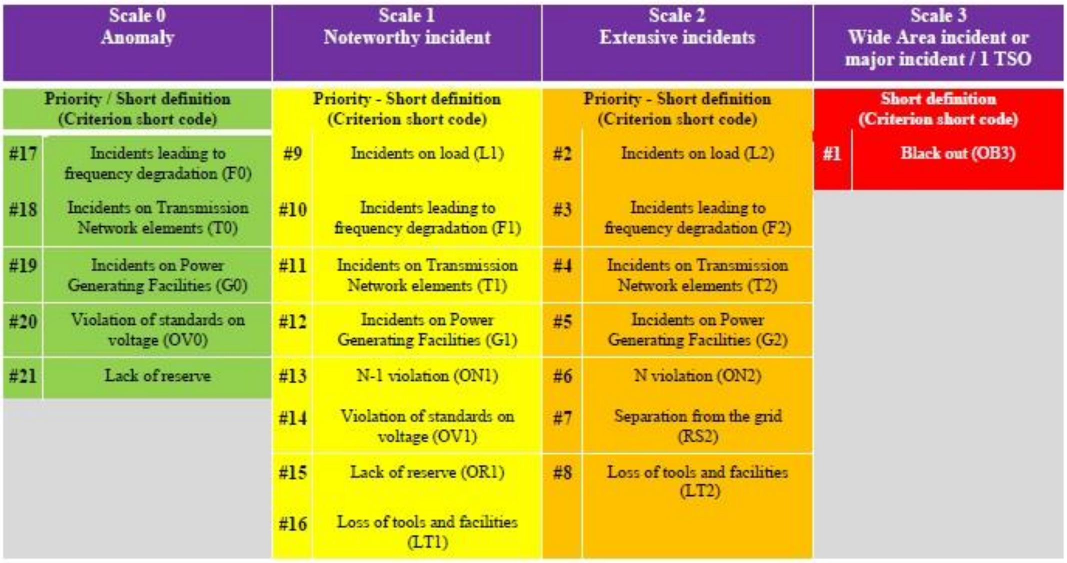
collaborative cultures, technologies such as sharing platforms). Data may provide evidence and understanding of past events, their occurrences, magnitudes and even their consequences. This also involves data about previous events that may have occurred in different Member States.

3.5 Evaluation of impact of dependencies and interdependencies

The final phase of risk assessment involves **comparing** the identified (inter)dependency risks with specific (often, sectorial) criteria to determine whether risks and/or their magnitudes are acceptable or tolerable.

For example, the sectors of banking and financial market infrastructures provide another instance of sectorial criteria and thresholds for the classification of incidents. For example, the European Banking Authority (EBA) provides guidelines, criteria and thresholds for incident notification under the PSD2 Directive. The incident classification distinguishes only two different types of incidents: Major Incident and Non-Major Incident. The classification dependents on thresholds of Lower Impact Level and Higher Impact level for different criteria (i.e. transactions affected, Payment service users affected, Service downtime, Economic impact, High level of internal escalation, Other payment service providers or relevant infrastructures potentially affected, and Reputational impact). These examples of different evaluation criteria for the assessment of incidents highlight the problem of defining common criteria (and thresholds) across sectors and Member States.

Moreover, ENTSO-E has defined an incidents classification scale methodology for the electricity sector, in particular, for transmission operators[46] depicted in Figure 10.



Scale 0 Anomaly		Scale 1 Noteworthy incident		Scale 2 Extensive incidents		Scale 3 Wide Area incident or major incident / 1 TSO	
Priority / Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Priority - Short definition (Criterion short code)		Short definition (Criterion short code)	
#17	Incidents leading to frequency degradation (F0)	#9	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Black out (OB3)
#18	Incidents on Transmission Network elements (T0)	#10	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
#19	Incidents on Power Generating Facilities (G0)	#11	Incidents on Transmission Network elements (T1)	#4	Incidents on Transmission Network elements (T2)		
#20	Violation of standards on voltage (OV0)	#12	Incidents on Power Generating Facilities (G1)	#5	Incidents on Power Generating Facilities (G2)		
#21	Lack of reserve	#13	N-1 violation (ON1)	#6	N violation (ON2)		
		#14	Violation of standards on voltage (OV1)	#7	Separation from the grid (RS2)		
		#15	Lack of reserve (OR1)	#8	Loss of tools and facilities (LT2)		
		#16	Loss of tools and facilities (LT1)				

Figure 10: ENTSO-E Incidents Classification Scale overview

National Risk Assessments highlight additional important aspects and challenges of impact evaluation. The impact may be assessed either quantitatively (e.g. in terms of clear magnitude: number of affected persons, monetary loss in euro, service unavailability in hours/day) or qualitatively. In the case of semi-

[46] ENTSO-E (2014). Incidents Classification Scale Methodology, Working group incident classification scale under system operations committee. European Network of Transmission System Operators for Electricity (ENTSO-E).

qualitative analysis, different criteria may be considered for the impact evaluation. National Risk Assessments have adopted different impact categories and criteria[47]:

- **Human impact:** usually quantified in terms of number of affected citizens.
- **Environmental impact:** quantified or assessed qualitatively in terms of harm to natural resources.
- **Economic impact:** usually quantified in terms of financial and material losses.
- **Societal impact:** taking into account disruptions of daily activities and usages of essential services.
- **Political impact:** taking into account the affected capacity to govern and control a country.

These impact criteria are in alignment with the ones that the NIS Directive identifies, including also duration of the incident and geographical spread with regard to the area affected by the incident. The review of National Risk Assessments highlights that impact criteria are often assessed differently. This is a critical challenge for impact assessment in relation to (inter)dependencies across sectors and Member States. It is necessary to provide a basic framework that can be used and tailored to different sectors and to national contexts. The impact framework would support identifying different criteria for assessing the impact of security incidents propagating also via (inter)dependencies.

3.6 National risk assessments

The following highlight key methodological elements related to how national risk assessments (NRAs) address risks affecting the European Union[48]. The European Commission is supporting NRAs in order to assess the exposure of Member States to different types of threats, including threats affecting the security of network and information systems. NRAs therefore provide also insights about the exposure to cyber threats of OES and DSPs. Figure 11 provides an account of the characteristics of NRAs.

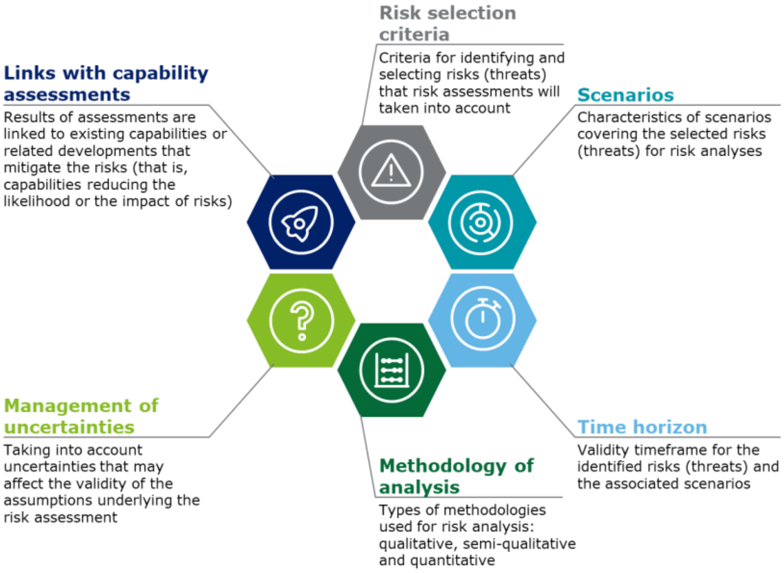

Risk selection criteria
Criteria for identifying and selecting risks (threats) that risk assessments will taken into account
Links with capability assessments
Results of assessments are linked to existing capabilities or related developments that mitigate the risks (that is, capabilities reducing the likelihood or the impact of risks)
Scenarios
Characteristics of scenarios covering the selected risks (threats) for risk analyses
Management of uncertainties
Taking into account uncertainties that may affect the validity of the assumptions underlying the risk assessment
Methodology of analysis
Types of methodologies used for risk analysis: qualitative, semi-qualitative and quantitative
Time horizon
Validity timeframe for the identified risks (threats) and the associated scenarios

Figure 11 Characteristics of National Risk Assessments

[47] The ECI Directive 2008/114/EC also makes reference to casualties, economic and social impact of infrastructure disruption
[48] European Commission (2017): Commission Staff Working Document – Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final.

- **Risk selection criteria:** Different criteria may be considered to identify and select the risks (threats) defining the scope of risk assessments. Past incidents (e.g. historical data of past incidents) or expert opinions may guide the definition of selections criteria, hence the identification and selection of risks.
- **Scenarios:** Definition of scenarios with varying different levels of criticality should capture critical events related to specific risks (threats). It is necessary to develop a detailed assessment programme consisting of scenarios of different severity (e.g. from limited impact to catastrophic incidents) and complexity (e.g. single-risk and multiple-risk scenarios) covering all identified risks.
- **Time horizon:** It is necessary to clarify the timeframe validity of risk assessments. This is to make sure that the developed scenarios and the risk assessments take also into account assumptions based on emerging trends or potential constraints (e.g. technological trends, regulatory frameworks, etc.).
- **Methodology of analysis:** Methodological approaches supporting risk analyses can provide different types of results: qualitative, semi-qualitative and quantitative.
- **Management of uncertainties:** It is necessary to take into account uncertainties that may undermine or invalidate the assumptions underlying risks assessments (including assumptions shaping risk scenarios).
- **Links to capability assessments:** The results of risk assessments should be linked to existing capabilities or their developments mitigating risks, for example, by deploying security controls in order to reduce the likelihood of threats, or by defining crisis management strategies or contingency plans in order to reduce the impact of threats.

4. Challenges for assessing (inter)dependencies

Integrating (inter)dependencies in the risk management process introduces a number of challenges that, to some extent, differ between OES/DSPs and NCAs due to varying context and focus. This section highlights the main challenges for managing (inter)dependencies these stakeholders respectively face.

Table 2 Challenges for assessing dependencies and interdependencies

	CHALLENGES
OES / DSPs	• Lack of data • Complexity of service supply chains • Specialised methodologies • Lack of skills • Taxonomy of incident impact assessment
NCAs	• Sectorial approach • Lack of data • Complexity of scenarios • Cross border notification and coordination • Identification of operators of essential services • Auditing OES

The following sections highlight the main challenges, in particular, with identifying and modelling, analysing and measuring, and evaluating dependencies and interdependencies.

4.1 Challenges for OES and DSPs

OES and DSPs face different challenges that limit assessing dependencies and interdependencies. Taking also into account their roles and responsibilities (including, security requirements and incident notifications) for assessing the potential risks associates with the security of network and information systems, this section pinpoints and discusses such challenges.

- **Lack of Data.** OES and DSPs face a lack of data to assess their (inter)dependencies. There are limited incentives supporting sharing of information concerned with emerging operational (inter)dependencies. To a certain extent, this is due to the fact that some (inter)dependencies may be discovered only once incidents occur. OES and DSPs often gather their operational data in order to provide their services. It is necessary to develop specific processes and mechanisms in order to share relevant information confidentially with order OES, DSPs and other NIS actors such as NCAs.
- **Complexity of Service Supply Chains.** Another challenge for assessing (inter)dependencies is due to the complexity of service supply chains. Although OES and DSPs can probably identify direct dependencies on other services, it is often difficult to identify and assess second order dependencies. Moreover, service supply chains may also have complex dependencies in operations.
- **Specialised Methodologies.** Developing data-driven assessment requires often combining different specialised methodologies (including tools). These methodologies enable OES and DSPs to develop data-driven risk assessments, heuristics and decision-making processes related to (inter)dependencies. In order to reach the required organisational and methodological maturity, there is need for a substantial investment to develop tailored specialised methodologies and to integrate them into organisational practices.

- **Lack of Skills.** OES and DSPs face the common problem of shortage of qualified personnel, who has the required skills for applying specialised methodologies in their complex operational environments.
- **Taxonomy of Incident Impact Assessment**. The analyses of different cyber incidents highlight that there is a lack of common criteria for assessing and describing their impact. Most of the incident reports focus on describing the type of attacks, the exploited vulnerabilities and some dynamics how infections spread across network and information systems. The incident impact is often described/assessed in aggregated terms (e.g. number of systems affected, number of countries affected, etc.). However, there is yet little emphasis on analysing the dynamics and impact of cyber incidents in terms of cross-sector and cross-border propagations due to (inter)dependencies among OES and DSP.

These challenges affect all phases (i.e. Identification and Modelling, Analysis and Measurement, and Evaluation of Impact) of assessing (inter)dependencies, but more so their identification. The lack of data poses additional challenges in identifying and assessing cross border (inter)dependencies. The emergent complexity of (inter)dependencies combined with the required specialised methodologies and skills may expose OES and DSPs to further challenges in analysing, measuring and assessing the potential impact of security incidents.

4.2 Challenges for NCAs

National Competent Authorities (NCAs) have critical roles and responsibilities in developing a coordinated approach supporting the security of network and information systems. They are responsible for establishing incident notification and information sharing practices supporting cooperation and coordination among all relevant stakeholders (nationally and cross-border). NCAs need to cooperate closely, nationally and cross-border (e.g. via the Cooperation Group and CSIRTs Network) in the implementation of the NIS Directive. NCAs face different challenges when dealing with assessment of (inter)dependencies: sectorial specialisation, lack of data, and complexity of the scenarios.

- **Sectorial Approach:** The NIS Directive identifies different sectors of OES and types of DSPs. Depending on the different transpositions of the NIS Directive and its implementations across the Member States, some NCAs and CSIRTs may be required to develop a sectorial approach specifying different thresholds and incident notification practices capturing the specificities of the different sectors (and subsectors) that the NIS Directive identifies. NCAs may have limited or patchy availability of data resulting in partial sectorial knowledge. This represents a challenge for developing a comprehensive sectorial approach and developing a complete overview of the security of network and information systems across all sectors. This hinders assessing emerging (inter)dependencies among all sectors. Moreover, NCAs operate at national level, which means that they have limited security operational knowledge of the status of OES and DSPs operating cross-border in other Member States. This implies that while NCAs may be able to deal with the assessment of (inter)dependencies nationally, they may face additional challenges when assessing cross-border (inter)dependencies among all sectors of OES and types of DSPs.
- **Lack of Data:** Deeply related to the previous challenge, NCAs often face a lack of data. Indeed, in order to assess (inter)dependencies, they need to develop an understating of the different operational environments of OES and DSPs. However, OES and DSPs typically consider such type of data to be confidential. Another reason for the lack of data is that NCAs may operate at a sectorial and national base in many cases, which limits their access only to data related to their own sector or national scope.
- **Complexity of Scenarios:** National Risk Assessments (NRAs) provide useful insights in order to understand the risk exposures of OES and DSPs operating nationally and cross-border. However, NCAs taking part in NRAs, may need to deal with designing complex scenarios involving single as well as

multiple risks. Lack of data or methodologies (and tools) may constraint and limit the complexity of scenarios in NRAs. Typically, it is difficult to create realistic scenarios that can be analysed without historical data and knowledge of different sectors across Member States. This means that in many cases NRAs take into account scenarios that may overlook complex emerging (inter)dependencies among sectors. Thus, NCAs are in many cases underprepared to deal with cross border and/or cross sector (inter)dependencies.

- **Cross Border Notification and Coordination:** In order to deal with cross border incidents, Member States via NCAs and CSIRTs, need to establish synergies, foster close cooperative schemes and probably develop a common response and crisis management plan (as required by the ECI Directive 2008/114/EC on the protection of critical infrastructures and the NIS Directive). The complexity increases as more actors (e.g. NATO, national security/defence agencies) are involved in the process of identifying cross border threats and transboundary risks posed against cross border services. This involves shared responsibilities among NCAs and CSIRTs operating cross border in different Member States. Managing challenges regarding the responsibility for restoration or incident coordination/management when establishing cooperation mechanisms/ mutual aid agreements between different operators, which are principally competitors, is an important and complex aspect that should be addressed by the Member States. Moreover, in case that essential services (e.g. transmission of electricity) extend beyond the EU territory, there are various concerns and challenges for the notification requirements of incidents that affect at least an EU Member State and a non-EU country. Transboundary essential services across the EU Member States, are raising challenges regarding the notification of cross border incidents, which may affect either non-essential services in a neighbouring EU Member State or essential/non-essential services in a non-EU country. These operational challenges concerned with cross border notification and coordination affect the assessment of (inter)dependencies.
- **Identification of Cross Border Dependencies and Interdependencies:** Coordination and cooperation among Member States are essential in order to support the identification of cross border (inter)dependencies of OES and DSPs. However, NCAs may face different challenges when identifying cross border dependencies and interdependencies. In particular, there is lack of common terminology at EU level for critical sectors, critical infrastructures and operators of essential services. Member States and NCAs often use similar terms interchangeably, for example, *"vital"*, *"essential"* and *"time critical"*. Member State and NCAs may seek cross border (inter)dependencies with other operators of other sectors (e.g. telecommunications), which possibly are identified as essential at national level, but they fall outside the scope of the NIS or ECI Directives. Member States may need to proceed further beyond the identification of critical infrastructures sectors and move towards the identification of operators of essential services (Article 5 of the NIS Directive) and possibly the identification of related essential services too.
- **Identification of Operators of Essential Services:** Member States may identify more entities (essential service operators), e.g. heating operators, considered as essential, according to their needs (e.g. distribution system operators for electricity). The absolute value of thresholds used for the identification of the European Critical Infrastructures (with respect to the ECI Directive) and for the identification of essential services operators may vary across EU Member States, due to their different sizes. The sensitivity of the business data might affect the ability of the EU Member States to collect cross border data from national operators.
- **Auditing OES:** NCAs will face difficulties when auditing OES, e.g. within the context of auditing compliance to the provisions of the NIS Directive, that has (inter)dependencies with other OES and DSPs, particularly when the latter are based in another Member State. The challenges are not limited to the identification of those (inter)dependencies but also to the limitations in auditing the security conformity level of the OES/DSPs on whose services the audited OES relies.

5. Indicators for assessing (inter)dependencies

This section provides a mapping of the key elements for assessing (inter)dependencies to risk assessment and audit frameworks. The mapping supports an analysis of (inter)dependencies with respect to the most relevant and used standards and frameworks in the risk management area. In particular, this section focuses on three main standards: ISO/IEC 27002, NIST Cybersecurity Framework and COBIT 5. These risk assessment and audit frameworks capture different risk domains and provide specific guidelines in order to plan and implement very detailed risk-based strategy in an organisation. A genuine benchmark between these standards provides a set of checklists composed of tailored and comprehensive risk criteria that may be associated to indicators of (inter)dependencies between OES and DSPs. The resulting mapping between indicators of interdependencies and risk assessment and audit frameworks will form a meta-framework for risk assessment and audit of interdependencies.

5.1 Mapping to risk assessment and audit frameworks

This section provides a brief overview of the risk assessment and audit frameworks taken into account in order to provide a characterisation of the (inter)dependencies' indicators. **ISO/IEC 27002** focuses on implementing an Information Security Management System by defining risk criteria within a specific external context. The **NIST Cybersecurity Framework** dives into security by providing a methodology to implement organisational cyber-security strategies. **COBIT5** integrates other frameworks by furnishing guidance organizing IT objectives and good practices. ISO/IEC 27002, NIST Cybersecurity Framework and COBIT5 are interdependent in many aspects. One focus is located at the governance level when others cover the operational as well as the management stage. The detailed mapping of the proposed indicators to all three standards provides a framework for operators to quickly and easily use their own tailor-made implementation of ISO/IEC 27002, NIST and/or COBIT5 for (inter)dependencies risk assessment and use them in tandem. The risk assessments of dependencies and interdependencies require identifying different criteria and provide guidelines for their evaluation. Annex C: provides further information about the analysed risk assessment and audit frameworks. Annex D: presents a detailed characterisation of different criteria in terms of mappings to ISO/IEC 27002 security controls, NIST Cybersecurity controls and COBIT5 goals (Figure 12).

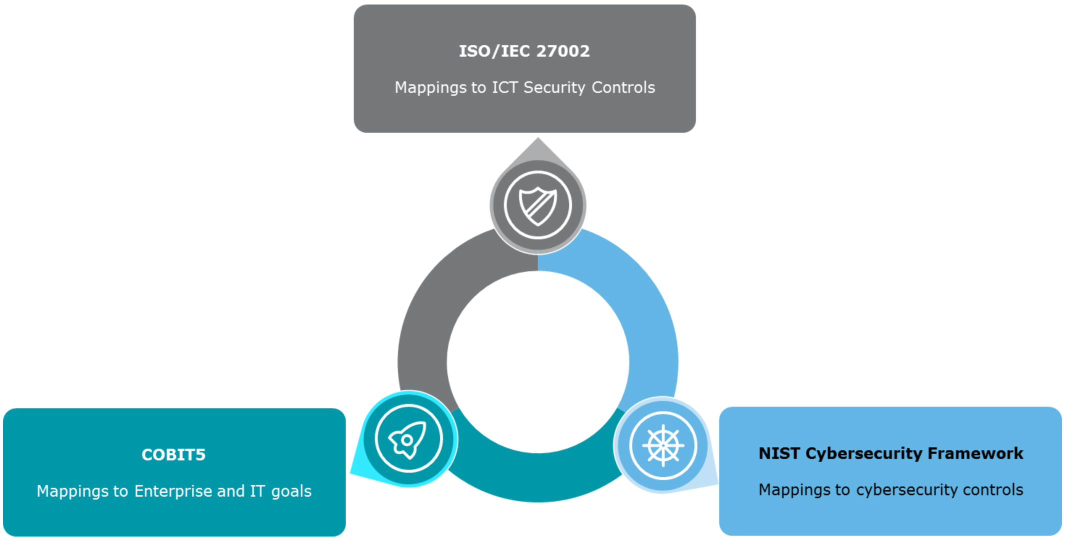

ISO/IEC 27002
Mappings to ICT Security Controls
COBIT5
Mappings to Enterprise and IT goals
NIST Cybersecurity Framework
Mappings to cybersecurity controls

Figure 12 Mappings criteria to ISO/IEC 27002, NIST cybersecurity controls, COBIT5 enterprise and IT goals.

Despite the existence of different risk assessment and audit frameworks, it is difficult to identify one that can cover different criteria for the risk assessment of (inter)dependencies. However, it is possible to map the identified criteria to different risk assessment and audit frameworks. Conceptually, this means combining ICT security, cybersecurity and governance together in order to characterise indicators for assessing the risks associated with (inter)dependencies.

5.2 Indicators

This section identifies a set of indicators that relate to (inter)dependencies and may provide useful insights for assessing them. The identified (types of) indicators relate to the assessment of the impact of an incident in alignment with the security requirements and incident notification of the NIS Directive. The indicators fall into four different domains (or types of indicators):

- **Impact:** the impact indicators relate to information that is concerned with the potential impact of incidents affecting the security of network and information systems.
- **Reliability, Dependability and Resilience:** the reliability, dependability and resilience indicators relate to information that is concerned with the potential impact of incidents on operations of affected essential or digital services.
- **Structure:** the structure indicators relate to information that is concerned with structural aspects of essential and digital services (e.g. market structures and redundancy of services).
- **Time:** the time indicators relate to information that is concerned with dynamics (including evolution of) and timing aspects (e.g. seasonality of demand) of essential services and digital services.

Table 3 lists and describes the identified indicators of (inter)dependencies.

Table 3 Indicators of Dependencies and Interdependencies

ID	INDICATOR	DESCRIPTION
	Indicators for Domain IMPACT	
IND01	The number of serviced users (potentially affected by an incident)[49]	The number of users of OES or DSPs may give preliminary indications of the potential risks associated with dependencies and interdependencies
IND02	Geographical distribution of services (e.g. cross border services potentially affected by an incident)	The geographical distributions of dependent and interdependent OES and DSPs may give preliminary indications of the potential risks
IND03	Social impact	The social impact should also take into account the potential impact of dependent and interdependent OES and DSPs on societal activities
IND04	Economic Impact	The economic impact should also take into account the potential impact of dependent and interdependent OES and DSPs on economic activities
IND05	Environmental impact	The environmental impact should also take into account the potential impact of dependent and interdependent OES and DSPs on the environment

[49] The number of users should reflect any abstractions encountered in practice; for instance, an airport might be a single user for an OES or DSP but counting as one user would be an incorrect indicator of impact.

ID	INDICATOR	DESCRIPTION
Indicators for Domain RELIABILITY, DEPENDABILITY AND RESILIENCE		
IND06	Loss of service capabilities (e.g. reduced services, fail-safe services, etc.)	This indicator takes into account various performance measures capturing the loss of service capabilities associated with dependencies and interdependencies of OES and DSPs
IND07	Resilience (e.g. failure recovery processes, crisis management processes, etc.)	Parameters such as time needed to intervene once a failure has started, time needed in order to start the recovery process, the time it can continue to operate once the infrastructures/services upon which it depends are not provided etc.
IND08	The Recovery Time Objective (RTO) after an incident in the offered service	This indicator takes into account various performance measures capturing the ability to recover after an incident affecting dependencies and interdependencies of OES and DSPs
IND09	The Mean Downtime (MDT) after an incident in the offered service	This indicator takes into account various performance measures capturing the duration (in particular, in terms of service downtime) of an incident affecting dependencies and interdependencies of OES and DSPs
IND10	Redundancy of services (e.g. alternative services, etc.)	This indicator takes into account various measures capturing the extent of redundancy related to dependencies and interdependencies of OES and DSPs
IND11	Criticality of services in terms of security (i.e. availability, integrity and confidentiality)	This indicator takes into account the security criticality of services (in terms of availability, integrity and confidentiality) in order to classify dependencies and interdependencies of OES and DSPs
Indicators for Domain STRUCTURE		
IND12	Number of Service Level Agreements (SLAs) with third parties	The number of SLAs may provide indications of the potential risks as well as structured aspects of dependent and interdependent OES and DSPs
IND13	Market share and structure (e.g. number of operators, number of alternative providers, multi-service market, monopoly, etc.)	Market share and structure may provide indications of the potential risks as well as structured aspects of dependent and interdependent OES and DSPs
IND14	Coupling and complexity of services (e.g. structures of services, system and network designs, etc.)	Market share and structure may provide indications of the potential risks as well as structured aspects of dependent and interdependent OES and DSPs
Indicators for Domain TIME		
IND15	Seasonality of dependencies/interdependencies (e.g. variations of service levels over seasons)	This indicator takes into account the risks associated with the seasonality (e.g. high demand of services during a particular time of the year) of dependent and interdependent OES and DSPs
IND16	Temporal aspects of critical events (e.g. time criticality, time-critical dependencies, etc.)	This indicator takes into account the temporal dimension of critical events (e.g. timeline, probabilistically independent and dependent events, etc.) associated with dependencies and interdependencies
IND17	Dynamic aspects of dependencies/interdependencies (e.g. volatility, evolution, etc.)	This indicator takes into account how dependencies and interdependencies of OES and DSPs interact in operations and evolve overtime

5.3 Assessment checks of (inter)dependencies

Table 4 provides assessment checks (drawn from mappings to ISO/IEC 27002, NIST Cybersecurity Framework and COBIT5) for the identified indicators of (inter)dependencies.

Table 4 Indicators of Dependencies and Interdependencies

ID	INDICATOR	ASSESSMENT CHECKS
IND01	The number of serviced users (potentially affected by an incident)	• System and application access controls may provide indications of the potential number of users affected • Operation security controls (e.g. malware controls, software restrictions, event logs, etc.) may provide indications of the potential number of users affected • The number of users informed and trained reduce drastically the number of users likely to be affected by an incident
IND02	Geographical distribution of services (e.g. cross border services potentially affected by an incident)	• Security controls related to supplier relationships (including ICT supply chains) may provide indications of the potential geographical distributions of incidents • Geographical distribution as an indicator plays a role in identifying third - party stakeholders and ensure that they understand their roles and responsibilities. • Geographical distribution as an indicator plays a role in identifying the entire workforce as well as third - party stakeholders and ensure that they understand their roles and responsibilities. • Geographical distribution as indicator may be related to the establishment of critical functions and zones of dependencies for delivery of critical services • Geographical distribution as indicator may be related to the localisation and documentation of asset vulnerabilities
IND03	Social impact	• Controls on Human Resource Security may also provide insights about the social impact of incidents • There may be a genuine link between social impact as indicator and the specific control, which consists in embedding cybersecurity in human resources practices
IND04	Economic Impact	• Controls on Supplier Relationships may also provide insights about the economic impact of incidents • Physical and information security personnel not being able to understand roles and responsibilities may result in major incident leading to a severe economic impact • No serious protection implementation against data leaks will more likely result in major incidents leading to an economic impact • The exercise of determining the impact of events is relevant in the sense that one of large effect may be economic • Reputation damage is more likely to be translated in economic impact
IND05	Environmental impact	• Physical and Environmental Security controls may also provide insights about the environmental impact of incidents • Mapping data flow may lead to the identification and localisation of environmental impact
IND06	Loss of service capabilities (e.g. reduced services, fail-safe services, etc.)	• Controls related to "management of information security incidents and improvements" may provide information on the risks associated with incidents • Controls related to "information security continuity" may also provide information on the risks associated with incidents • Redundancy controls may provide information on the risks associated with incidents • Monitoring and review of supplier services may also provide information on mean downtime
IND07	Resilience (e.g. failure recovery processes, crisis management processes, etc.)	

ID	INDICATOR	ASSESSMENT CHECKS
IND08	The Recovery Time Objective (RTO) after an incident in the offered service	• Event logging may also provide information on mean downtime associated to NIS incidents • Criticality of information may also provide insights on the criticality of services • Supplier controls may also provide insights on the criticality of services • Compliance controls may also provide information on the risks associated with incidents
IND09	The Mean Downtime (MDT) after an incident in the offered service	
IND10	Redundancy of services (e.g. alternative services, etc.)	
IND11	Criticality of services in terms of security (i.e. CIA)	
IND12	Number of Service Level Agreements (SLAs) with third parties	• Service level agreements may provide information on the risks associated with incidents • Mapping data flow may lead to the identification and localisation of number of SLA
IND13	Market share and structure (e.g. number of operators, number of alternative providers, multi-service market, monopoly, etc.)	• Suppliers related controls may provide information about market share and structure, and the risks associated with incidents
IND14	Coupling and complexity of services (e.g. structures of services, system and network designs, etc.)	• Suppliers related controls may provide information about coupling and complexity of services, and the risks associated with incidents • Information classification may provide insights about coupling and complexity of services, and the risks associated with incidents • Access controls and policies may provide insights about coupling and complexity of services, and the risks associated with incidents • Security requirements and specification may provide insights about coupling and complexity of services, and the risks associated with incidents • Secure system engineering principles may provide insights about coupling and complexity of services, and the risks associated with incidents • Mapping data flow may lead to the identification and localisation of number of coupling and complexity of services
IND15	Seasonality of dependencies/interdependencies (e.g. variations of service levels over seasons)	• Capacity management may provide information about variations of service levels, and the risks associated with incidents • Event logging may provide information about variations of service levels, and the risks associated with incidents • Controls related to "supplier service delivery management" may also provide information on variations of service levels, the risks associated with incidents • Management of information security incidents and improvements may also provide information on variations of service levels, the risks associated incidents • Information security continuity controls may also provide information on variations of service levels, the risks associated incidents • Redundancy controls may also provide information on variations of service levels, the risks associated with incidents
IND16	Temporal aspects of critical events	• Temporal aspects of critical events should be taken into account in order to assess the risks associated with incidents
IND17	Dynamic aspects of dependencies/interdependencies	• Dynamic aspects of services should be taken into account in order to assess the risks associated with incidents

5.4 Expanding the framework

The framework for the indicators for assessing (inter)dependencies is built on three standards selected in part due to their applicability in most if not all sectors and contexts. However, the framework can be further expanded to address sectorial specificities or operational priorities by including mappings to other relevant standards. One example of this is the ISA/IEC 62443[50] family of standards, which covers Industrial Automation and Control Systems Security and is very relevant to sectors that rely on Operational Technology (OT) as well as IT. Another example would be the ISO 22301:2012[51] that focuses on Business Continuity Systems.

While addressing specific sectorial examples is beyond the scope of the proposed framework, an indicative list of relevant standards and frameworks that can complement the mapping is presented below:

Table 5 Indicative list of additional relevant standards

SECTOR	STANDARDS
Cross sector	• ANSI/ISA, Series “ISA-62443: Security for industrial automation and control system” • ISO 22301:2012 • ISO/IEC 27004:2016 • ISO/IEC 20000-1:2011 • ISO/IEC 10181-2:1996 • ISO/IEC 27033-1:2015 • ISO/IEC TR 19791:2010
Energy / Electricity	• **NIST SP800-82** Guide to Industrial Control Systems (ICS) Security • **ISO 27019** -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry • **NERC CIP** Series "Critical Infrastructure Protection Cyber Security": CIP–002 to CIP-011.
Energy / Oil & Gas	• **API STD 1164** - Pipeline SCADA Security • Oil and Natural Gas subsector cybersecurity capability maturity model - (**ONG-C2M2**)
Transport / Air	• **ICAO** Aviation Security Manual - Document 8973 (Restricted Access)
Transport / Water	• **BIMCO Guidelines on Cyber Security on board Ships** - The Guidelines on Cyber security on board ships
Finance and Banking	• Payment services (**PSD 2**) - Directive (EU) 2015/2366 • Payment Card Industry Data Security Standard (**PCI DSS**) • **ISO/TR 13569:2005** Financial services - Information security guidelines
Healthcare	• **ISO 27799:2008** Health informatics - Information security management in health using ISO/IEC 27002 • Health Insurance Portability and Accountability Act of 1996 (**HIPAA**)
Digital Infrastructures	• **ISO/IEC 27011:2008** Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC

[50] https://www.isa.org/isa99/
[51] https://www.iso.org/standard/50038.html

6. Good Practices for (inter)dependencies

This chapter presents good practices to support stakeholders in assessing (inter)dependencies. These good practices provide a pragmatic approach to assist OES and DSPs on the one hand and NCAs on the other hand, taking into account their respective roles and responsibilities in the implementation of the NIS Directive, with particular emphasis on the assessment of (inter)dependencies

Table 6 Good practices for assessing dependencies and interdependencies

	GOOD PRACTICES
OES / DSPs	• Operational accounts of dependencies and interdependencies • Training and awareness • Methodologies and Tools
NCAs	• Information sharing • Methodologies and tools • Cyber security intelligence

6.1 Good practices for OES and DSPs

OES and DSPs can take pragmatic actions enabling the assessment of (inter)dependencies including:

- **Operational accounts of (inter)dependencies:** At the operational level, OES and DSPs need to develop an account of their (inter)dependencies. This will require investing in operational, analytical and data-driven (or event-driven) capabilities (e.g. monitoring systems, incident notification practices, etc.) supporting the identification and analysis of emerging (inter)dependencies in their operations. This approach addresses, to a certain extent, the lack of data and enables OES and DSPs to further understand their (inter)dependencies, while enhancing their overall resilience in dealing with security incidents related to cyber (inter)dependencies After identifying these (inter)dependencies OES and DSPs should examine whether existing plans for security or for business continuity take them into account and update these plans accordingly.
- **Training and Awareness:** In order to understand (inter)dependencies, it is necessary to develop a comprehensive understanding of different operational aspects of OES and DSPs. Moreover, it is necessary to link policy and regulatory frameworks with environments and operations of OES and DSPs. This may require specialised skills combining, for example, policy analyses, analytics, risk assessments, cyber security and so on, including skills concerned with the applications of methodologies in specific contexts and situations (e.g. incident scenarios). Tailored training and awareness programmes support developing the skills and practices required in the assessment of (inter)dependencies.
- **Methodologies and Tools:** OES and DSPs present different (inter)dependencies in their operations. Although it is challenging to identity generic methodologies and tools that fit all different operational environments, OES and DSPs would benefit from tailoring and integrating diverse methodologies and tools that provide support for assessing dependencies and interdependencies.

These recommendations intend to support OES and DSPs in developing and integrating practices for assessing dependencies and interdependencies. In particular, it is advisable to develop, tailor and integrate practices supporting all phases (i.e. Identification and Modelling, Analysis and Measurement, and Impact Evaluation).

6.2 Good practices for NCAs

Due to their roles and responsibilities, NCAs are in a good position to implement practices supporting the assessment of (inter)dependencies, in particular their cross border identification.

- **Information Sharing:** In order to create cross-sectoral and cross-border approaches, it essential to support the collaboration and information sharing among NCAs. On the one hand, NCAs may support ad-hoc collaborations and information sharing in order to support national risk assessment exercises and to assessing particular cross border dependencies and interdependencies. Working groups under the leadership of NCAs can also be established. These groups should agree on the kind of data to be shared and the NCAs could take the burden of performing simulation since they are in a position to have a better view of the whole system of infrastructures. On the other hand, EU-wide initiatives (potentially driven by centralised authorities) should encourage and enable the exchange of information among NCAs and CSIRTs during their operations in order to support the identification and assessment of emergent cross border (inter)dependencies.
- **Methodologies and Tools:** NCAs have patchy knowledge of cross sector and cross border (inter)dependencies. The enforcement of the NIS Directive's security requirements and incident notification for OES and DSP will better position designated NCAs to identify and assess emergent (inter)dependencies in operations. This may require them to develop and integrate tailored methodologies and tools, which would help NCAs in developing a comprehensive account, reflecting the emergent complexity in operations, of (inter)dependencies. Even if a sophisticated tool or method is missing, a first step would be to make a workshop or exercise with key representatives of sectors in order to perform an initial, simplified mapping of dependencies. It is necessary to develop additional capabilities enabling the assessment of (inter)dependencies. In order to develop and disseminate best practices (including the experiences of adopting methodologies and tools in specific contexts), the roles and responsibilities of the Cooperation Group and the CSIRTs Network are essential.
- **Cyber Security Intelligence:** NCAs and CSIRTs can engage constructively with OES and DSPs in order to guide them in gathering the necessary information (e.g. records of past incidents affecting essential services) for assessing (inter)dependencies. Moreover, NCAs and CSIRTs may have a convenient position and active role in sharing critical knowledge about (ongoing) incidents. This would help NCAs supporting the definition of reaction and mitigation measures, and their cross border adoption by OES and DSPs. This means supporting a bidirectional information sharing among NCAs, CSIRTs, OES and DSPs, hence supporting the gathering and dissemination of cyber security intelligence. This also would encourage OES and DSPs to go beyond mandatory incident notification and to support voluntary notification in order to enhance the assessment of (inter)dependencies. Cyber security intelligence would enable NCAs, CSIRTs, OES and DSPs to further develop their technological (e.g. including data analytics) and organisational structures required for assessing emergent cross sector and cross border (inter)dependencies.

7. Conclusions and Recommendations

This report has investigated good practices on (inter)dependencies between OES and DSPs, specifically how OES and DSPs can identify and assess the potential risks associated with emerging (inter)dependencies. Taking into account diverse contributions (e.g. literature reviews, interviews with experts, online surveys), this report also provides a detailed account of the landscape of (inter)dependencies between OES and DSPs. Moreover, it provides a comprehensive overview of risk assessment practices, including methodologies that Member States adopted in National Risk Assessments (NRAs).

- **Dependencies and Interdependencies.** The review of relevant literature and experts' opinions provide insights for defining the concepts of dependencies and interdependencies. This report provides definitions tailored to the analysis of dependencies and interdependencies among OES and DSPs. Such definitions enable analysing emerging (in particular, cyber) (inter)dependencies across all sectors of the NIS Directive. Moreover, this report discusses dependencies of OES to DSPs in order to emphasise emerging digital dependencies across sectors. Overall, this report provides an account that clarifies the concepts of dependencies and interdependencies of OES and DSPs.
- **Assessing Dependencies and Interdependencies.** Current industry practices highlight key phases – Identification and Modelling, Analysis and Measurement, and Evaluation of Impact – forming a systematic process for dependency and interdependency assessment. These phases involve diverse methodologies and approaches, which allow investigating (inter)dependencies in order to assess their potential impact on OES and DSPs. Member States and other authorities (e.g. the EC Joint Research Centre) have adopted similar processes involving specific methodologies for conducting National Risk Assessments (NRAs). NCAs, OES and DSPs, who may be involved in or conduct related assessments, have to face various challenges due to the lack of operational data, the complexity of emerging dependencies and the specificity of methodologies.
- **Good Practices for Dependencies and Interdependencies.** Based on the characterisation of (inter)dependencies and the review of risk assessment practices, this report discusses challenges and provides good practices for their assessment. OES, DSPs and NCAs may benefit from the analysis of such challenges and good practices.

In order to address the challenges that OES, DSPs and NCAs face in the assessment of (inter)dependencies, this report provides the following recommendations:

- **OES and DSPs should conduct empirical investigations to collect data:** The lack of data represents a common challenge for assessing (inter)dependencies. Future initiatives should support information sharing in order to conduct empirical investigations of emerging (inter)dependencies in the operations of OES and DSPs.
- **OES, DSPs and NCAs should develop and integrate methodologies and tools:** Risk assessment practices highlight specific phases (i.e. Identification and Modelling, Analysis and Measurement, and Impact Evaluation) for assessing (inter)interdependencies. Future initiatives should investigate further how specific methodologies and tools support each phase. In particular, they should provide guidance how to integrate methodologies and tools in practices across sectors. This also would help tailoring methodologies and tools to the needs of OES, DSPs and NCAs.
- **OES and DSPs should promote training and awareness:** Another common challenge is due to the need of specialised expertise in order to assess emerging (inter)dependencies. Future initiatives should support developing competencies for applying different methodologies and tools in specific

operational contexts. This also would support further understanding (inter)dependencies among OES and DSPs.

- **NCAs should work towards developing a common taxonomy of incident impact assessment:** In order to support the assessment of cross-sector and cross-border incidents, it is necessary to develop a common taxonomy of incident impact assessment. The implementation of the NIS Directive can provide a good starting point for providing some harmonisation (e.g. by developing incident notification mechanisms tailored to the NIS Directive and supporting information sharing across relevant stakeholders such as OES, DSP, CSIRTs and NCAs).
- **OES and DSPs should address (inter)dependencies at operational level:** OES and DSPs should integrate (inter)dependencies in their risk assessment and security operations and this should be reflected in the development of tools, methodologies, skills and the way incidents are presented, reported and analysed.
- **NCAs should facilitate information sharing:** At a national level, NCAs should facilitate information exchange about (inter)dependencies, including direct dialogue between (inter)dependent organisations. At cross-border level, Member States should promote a framework for the exchange of information regarding cross-border (inter)dependencies that establishes how information exchange can take place and what type of information is relevant.
- **OES, DSPs and NCAs should invest on resilience:** Boost resilience by developing response management capabilities and establishing common response and crisis management plans. Member States should invest on the resilience by addressing redundancy (the availability of alternatives), diversity of technical implementations and time for recovery.
- **NCAs should integrate cross-border (inter)dependencies in NRAs:** Member States should address cross-border (inter)dependencies when conducting NRAs by identifying services which create such dependencies. **Identification should be based on a granular process**, **all relevant parties should be identified** and a **national registry of cross-border dependencies** should be developed and maintained.

Annex A: Glossary of terms and definitions

TERM	DEFINITION
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
Cascading failure	How a disruption in one infrastructure causes a disruption in the second.
Cloud Computing Service	A digital service that enables access to a scalable and elastic pool of shareable computing resources.
Common cause failure	Disruptions of two or more infrastructures is due to a common cause.
Cross border dependencies and interdependencies	Dependencies and interdependencies between OES themselves, between DSPs themselves, and between OES and DSPs operating in different Member States.
Cross sector dependencies and interdependencies	Dependencies and interdependencies between OES, between DSPs, and between OES and DSPs operating in different sectors.
Cyber dependency or interdependency	A service (or an infrastructure) has a cyber dependency if its state of operation depends on information and data transmitted through the information service (infrastructure) via electronic or informational links. Outputs of the information service (infrastructure) are inputs to the other service (infrastructure), and the commodity passed among the service (infrastructure) assets is information.
Cyber Resilience	The overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them Cyber security - the protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Dependency	A linkage or connection between two services (or underlying infrastructures), through which the state of one service (infrastructure) influences or is correlated to the state of the other.
Digital Service	Any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.
Digital Service Provider (DSP)	Any legal person that provides a digital service.
Escalating failure	How a disruption in one infrastructure exacerbates an independent disruption of a second.
Geographical dependency or interdependency	Service (or infrastructure) assets are geographically dependent if a local environmental event can create changes in the state of operations in all of them. A geographic dependency occurs when elements of service (infrastructure) assets are in close spatial proximity (e.g. a joint utility right-of-way).

TERM	DEFINITION
Incident	Means any event having an actual adverse effect on the security of network and information systems.
Incident Response	The activities that address the short-term, direct effects of an incident, and may also support short-term recovery.
Industrial Control System (ICS)	An information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.
Information security incident management	Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Interdependency	A bidirectional relationship between two services (or underlying infrastructures) through which the state of each service (infrastructure) influences or is correlated to the state of the other. More generally, two services (infrastructures) are interdependent when each is dependent on the other.
Internet Exchange Point (IXP)	A network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic.
Logical dependency or interdependency	A service (or an infrastructure) is logically dependent if its state of operations depends on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes.
Online Marketplace	A digital service that allows consumers and/or traders […] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.
Online Search Engine	A digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.
Operator of Essential Services (OES)	A public or private entity of a type referred to (including Energy sector, Transport sector, Banking Sector, Financial market infrastructures, Health sector, Drinking water supply and distribution sector, Digital infrastructure sector.
Physical dependency or interdependency	A service (or an infrastructure) is physically dependent if the state of its operations is dependent on the material output(s) of another service (infrastructure) through a functional and structural linkage between the inputs and outputs of two assets: a commodity (i.e. good or service) produced or modified by one service (infrastructure) – an output – is required by another service (infrastructure) for its operation – an input.
Risk	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.

TERM	DEFINITION
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.
Risk Identification	Process of finding, recognising and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization.
Top-level domain name registry (TLD)	An entity which administers and operates the registration of internet domain names under a specific top-level domain.
Value chain	A set of activities that a firm operating in a specific sector/sub-sector performs in order to deliver a valuable product or service for the market. The phases are "production", "transmission" and "distribution".

Annex B: Research on (inter)dependencies risk assessment methods

B.1 Empirical approaches

These approaches involve the use of statistical data as well as expert opinions in order to identify and capture dependencies and interdependencies. There are different possibilities in order to take an historical account, such as qualitative approaches based on databases, quantitative approaches (e.g. metrics) for probabilistic risk assessment and regression analysis for analysing relationships (e.g. emerging correlations).

Studies with databases involve the analysis of patterns of a given phenomenon, which may be the interdependence of the infrastructures suggested in failures of some of them, according to information collected in publications officers, or in the media, in expert surveys, or in other relevant sources. This kind of work can be useful for characterizing the phenomena and compare their consequences[52].

The quantitative metrics are ways of quantifying the interdependence. In this sense, it is common to use simple ratios to show the direction of faults in infrastructure. For instance, the interaction ration to measure interdependence relates to the number of times when the problem of one infrastructure affects another. Researchers have proposed a duration ratio of failure in the service of an infrastructure, on the duration of the failure in another, with the objective of analysing the direction of the cascade effect that occurs from a particular failure[53]. Other authors have used the Pearson's correlation coefficient as the metric to quantify the intensity of interdependence[54].

Probabilistic risk assessments can be used together with decision analysis approaches, incorporating different groups of interest, to build scenarios that provide information on interdependencies potential[55]. An initial event generates a scenario that in turn generates others according to existing interdependencies. The probabilistic risk assessments include the statistical analysis of historical events, bibliographic review and inputs of the different interest groups. This focuses on studying the severity and probability of the event, according to the parameters previously stipulated, considering historical databases. Finally, it is important to note that methods, such as the probabilistic risk approach, are used to the extent that there is a lack of sufficient information to apply econometric methodologies. When there is more data that can be used, for example, some authors have worked with time series to evaluate the interdependencies. They

[52] McDaniels, T.; Chang, S.; Peterson, K.; Mikawoz, J.; Reed, D. (2007): Empirical framework for characterizing infrastructure failure interdependencies. Journal of Infrastructure Systems; 13(3):175–84. DOI: https://doi.org/10.1061/(ASCE)1076-0342(2007)13:3(175)

[53] Zimmerman, R. & Restrepo, C. E. (2006): The next step: Quantifying infrastructure interdependencies to improve security. International Journal of Critical Infrastructures, 2, 215–230. DOI: https://doi.org/10.1504/IJCIS.2006.009439

[54] Mendonca, D.; William, A.W. (2006): Impacts of the 2001 World Trade Center attack on New York City critical infrastructures. Journal of Infrastructure Systems; 12(4):260–70. DOI: https://doi.org/10.1061/(ASCE)1076-0342(2006)12:4(260)

[55] Li, H.; Apostolakis, G. E.; Gifun, J.; VanSchalkwyk, W.; Leite, S. & Barber, D. (2009): Ranking the risks from multiple hazards in a small community. Risk Analysis, 29, 438–456. DOI: https://doi.org/10.1111/j.1539-6924.2008.01164.x

have used cross-correlation coefficients to show different kinds of interdependencies[56]. Very similarly, other authors have proposed the use of Statistical Learning Theory (STL) in case of sufficient information[57].

B.2 Agent based approaches

Agent-based models are computational models that allow the simulation of actions and interactions of autonomous individuals within an environment, and allow to determine what effects they produce in the system as a whole. An agent-based model adopts a bottom-up approach to analyse the complex architecture and adaptive behaviours of the components of infrastructure systems. Agent-based approaches have the capability to model down to the level of a single component of an infrastructure system as well as the behaviour of a decision-maker. Through discrete-event simulations, such methods can capture all kinds of the interdependencies among infrastructure systems[58]. One of the major advantages of using agent-based methods is that they can provide flexible scenario-based what-if analyses assessing the effectiveness of different strategies. They can also be integrated with other modelling techniques to provide a detailed analysis. Our research suggests that agent-based methods can be applied to a range of decision contexts involving a host of stakeholder concerns. However, agent-based approaches present some challenges. The modeller needs to make some strong assumptions about the behaviour of an agent, and, in some cases, such assumptions are hard to justify. In order to properly calibrate the parameters of a simulation model, agent-based methods require a large set of detailed data about infrastructure systems and agent behaviour; it is sometimes difficult to collect such detailed information on infrastructure performance particularly when the relevant infrastructures have data sensitive to public safety and/or stakeholder interests. Considering this context, it is possible to develop models that include networks of agents of different classes (firms, households) with particular emphasis on how they use the particular infrastructures, and how these agents and infrastructures respond to hypothetical faults. For its development, economic and infrastructure in standardized databases, to then create the simulations during normal conditions and disruptive events[59].

B.3 System dynamics based approaches

Models based on system dynamics are another technique of modelling complex systems. The conceptualisation is based on the feedback, or circular causality between observable variables. Because of its structure, it is possible to represent these models using traditional mathematical language, with a set of algebraic equations whose variables are properties of the modelled system. The problem lies in identifying the causal links. Circuits, stocks and feedback flows must be differentiated. Circuits are the connections or directions of the effects and stocks are the amounts in the system, whose levels are given by the flows

[56] Dueñas-Osorio et al. (2012): Spatial Quantification of Lifeline System Interdependencies. Proceedings of the 15th world conference in earthquake engineering (15WCEE), Lisbon, Portugal.

[57] Guikema, S. D. (2009): Natural disaster risk analysis for critical infrastructure systems: An approach based on statistical learning theory. Reliability Engineering and System Safety, 94, 855–860. DOI: https://doi.org/10.1016/j.ress.2008.09.003

[58] Ouyang, M. (2014): Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety 121, 43–60. DOI: https://doi.org/10.1016/j.ress.2013.06.040

[59] Ehlen, M. (2010): Economics Definitions, Methods, Models, and Analysis Procedures for Homeland Security Applications. SAND2010-4315.

between the parties. With this kind of models, it is possible to analyse the consequences of a failure of a sector / infrastructure in others and in the economy in general[60].

The product input matrix describes the equilibrium behaviour of regional and national economies. It is a useful tool to describe the interactive nature between different systems of the economy and can obviously be used for analysing the interdependencies in infrastructure. In practice, this model aims to use information of input product of national accounts to estimate the impact of failures of an infrastructure in another and study the spread of that impact. A further step consists of having computable general equilibrium models[61], and even having spatial equilibrium models computable in general[62]. Research provides also instances of system-based models for capturing dependencies in critical infrastructures[63].

B.4 Economic theory based approaches

There are different models that take into account economic indicators in order to assess various aspects of services. For example, utility theory provides a modelling approach for assessing alternative choices and supporting decision making. Utility theory modes services and their properties by functions (i.e. the utility functions) in order to assess the results according to assumed behaviours (e.g. consumer behaviour, service demand, etc.). The objective is often to maximise the utility function assuming that it corresponds to best choice (that is, the highest utility satisfaction).

The input-output model provides another approach for assessing various economic indicators from a functional viewpoint. In particular, rather than assessing individual services, the input-output model provides a quantitative economic approach for capturing and assessing interdependencies between different branches of a national economy or different regional economies. The input-output model is also useful for assessing the risks associated with interdependencies of critical activities (including essential services) across Member States. For example, the JRC has adopted the input-output model for conducting a national risk assessment[64]. The reported risk assessment involved evaluating emerging interdependencies among critical sectors (e.g. electricity, telecom, water supply and distribution, road transport, etc.) in different disruptive scenarios (e.g. blackout, gas leak, earthquake and explosion).

B.5 Network based approaches

In network-based models, infrastructures are modelled as networks, composed of nodes and arcs, with goods flowing between them (represented by flows). In these models, the services are desired levels of the

[60] Bush, B., Dauelsberg, L., Leclaire, R., Powell, D., Deland, S., and Samsa, M. (2005): Critical infrastructure protection decision support system (CIP/DSS) overview. *Los Alamos National Laboratory Report LA-UR-05-1870, Los Alamos, NM 87544*.

[61] Rose, A.; Liao, S. (2005): Modelling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. Journal of Regional Science; 45:75–112. DOI: https://doi.org/10.1111/j.0022-4146.2005.00365.x

[62] Zhang, P., & Peeta, S. (2011): A generalized modeling framework to analyze interdependencies among infrastructure systems. Transportation Research Part B: Methodological, 45(3), 553–579. DOI: https://doi.org/10.1016/j.trb.2010.10.001

[63] Nieuwenhuijs, A., Luiijf, E., Klaver, M. (2008): Modeling Dependencies In Critical Infrastructures. IFIP International Federation for Information Processing, Volume 290; Critical Infrastructure Protection II, ICCIP 2008, Springer, pp. 205–213. DOI: https://doi.org/10.1007/978-0-387-88523-0_15

[64] Galbusera, L., Giannopoulos, G., Agius, J., Chetcutci, G. (2016): Reporting the outcome of the Input-Output Inoperability Modelling for Interdependent CI sectors in Malta. Joint Research Centre (JRC), Institute for the Protection and Security of the Citizen, JRC 102363 EN.

aforementioned flows. Network based approaches are usually divided into those whose objective is a structural analysis and those who are intended to perform a functional analysis. The former analyse the design of the infrastructure and the relationship between designs, and the latter consider operational issues. This class of models is useful to analyse how critical a certain location is, in case of a certain failure, and perform vulnerability analysis. It is also possible to create a link with the use of geographic information data[65].

Infrastructure systems can be represented by networks, where nodes or vertices represent different components of a system and links or edges represent relationships among them. Network based approaches can analyse interdependencies through different analytical techniques. Through network based approaches, intuitive representations of critical infrastructures are possible by providing the detailed descriptions of their structures and flow patterns. In these approaches, individual component failures of a single infrastructure under a disruption can be modelled and the performance response of the infrastructure system can be analysed. Network based approaches can be divided into two groups: (a) topology based approaches, and (b) flow based approaches.

These modelling and simulation based approaches can be used for vulnerability assessment of large scale data sets of infrastructure systems. However, such approaches are limited since they ignore the functional relationships among the different elements of the network missing vital information about infrastructure performance. Flow-based methods, on the other hand, can capture the flow characteristics of interdependent infrastructures, and provide more realistic descriptions on their operation mechanisms. However, these approaches are not scalable since when the network is modelled in detail the computational cost to analyse it is very high.

B.6 Service based approaches

Service based approaches capture interdependencies on the basis of exchange of services between infrastructures of the same or different sector. For example, transport infrastructure depends on services from electricity infrastructure and if the amount of provided service falls below a certain threshold then the disruption propagates to the dependent infrastructure. This enables the development of a sector agnostic analysis framework which can be applied without entering into the details of the underlying physics and flow models. The amount of a service disruption for a given scenario can be provided by other more detailed models (i.e. flow models) or from expert judgement.

B.7 Comparative analysis of different approaches

The aforementioned methodologies based on five criteria: **amount of data** needed, **accessibility** of data, **types of (inter)dependencies** surveyed, **computational cost** and **maturity** of investigations. Regarding data, most methodologies are intensive in the use of information, though the ones with a structural approach require the least amount of data. At the other extreme, there are the simulation-based models. Regarding the type of interdependencies studied, the models that have a broader scope are those based on the product input matrix, since consider the geographical and logical interdependencies. The rest, in most of their variants, limit their study to the four different types of dependencies (i.e. physical, cyber, geographic and logical). In terms of computational cost and complexity, those less intensive in this regard are the empirical approaches in general, in the same way that the approach that uses the product input

[65] Ouyang, M.; Dueñas-Osorio, L. (2011). An approach to design interface topologies across interdependent urban infrastructure systems. Reliability Engineering and System Safety; 96(1):1462–73. DOI: https://doi.org/10.1016/j.ress.2011.06.002

matrix and the simulation models based on networks with a structural approach. Agent-based models and Network-based, flow-based models are the more cost intensive approaches. It is important to point out here that there is a proposal to unify and consolidate current research on analysis of interdependencies based on a five dimensional framework[66]: system analysis, behaviour analysis, knowledge discovery, visualisation and information sharing. These methodologies support the identification and modelling of dependencies and interdependencies in order to assess the associated risks[67].

[66] Bagheri, E., Ghorbani, A. A. (2008): The state of the art in critical infrastructure protection: A framework for convergence. International Journal of Critical Infrastructures, 4, 215-224. DOI: https://doi.org/10.1504/IJCIS.2008.017438

[67] Hokstad, P., Utne, I. B., Vatn, J. (2012): Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis. Springer. DOI: https://doi.org/10.1007/978-1-4471-4661-2

Annex C: Standards and frameworks

This annex provides a schematic review of the main standards (or families of standards) and frameworks taken into account when creating the characterisation of the interdependencies' indicators: COBIT5, ISO/IEC 27000 and the NIST Cybersecurity Framework. These standards have been chosen because look at three different areas particularly affected by dependencies and interdependencies. Indeed, as shown in Figure 13 COBIT5 deals with Enterprise and IT goals; ISO/IEC 27002 deals with ICT Security Controls and finally; the NIST Cybersecurity Framework provides a substrate of cybersecurity controls that bring the other two standards together.

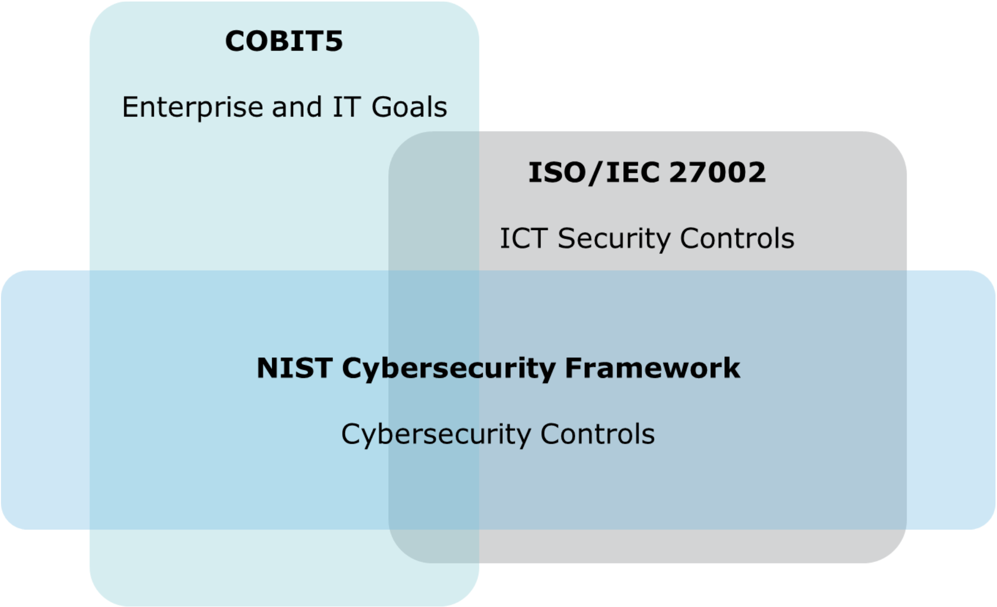


Figure 13 Intersections between ISO/IEC 27002, NIST Cybersecurity Framework and COBIT5

C.1 COBIT5

COBIT stands for 'Control Objectives for Information and related Technology'. Its fifth and latest version was launched in April 2012. The mission of COBIT is *"to research, develop, publish and promote a set of control objectives generally accepted for information technologies that are authorized (given by someone with authority), updated, and international for the day-to-day use of business managers (also managers) and auditors"*. This means that not only managers and auditors, but also general users, can benefit from the development. Indeed, COBIT5 can help them to understand their Information Systems (or information technologies) and decide the level of security and control that is necessary to protect the assets of their companies through the development of a model of administration of information technologies. These are the elements of COBIT5:

- **Framework:** COBIT5 Organizes IT governance objectives and good practices by IT domains and processes and links them to business requirements.
- **Process Model:** COBIT5 is a reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run, and monitor.
- **Maturity model:** COBIT5 assesses maturity and capability per process and helps to address gaps.
- **Controls:** COBIT5 provides a complete set of high-level controls to be considered for the effective management of each IT process.

- **Guidelines:** COBIT5 helps assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.

COBIT5 defines a set of generic processes for the management of IT. Each process is formulated based on process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. The framework also provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. In this regard, the business orientation of COBIT5 consists of linking IT goals to the general business goals of the stakeholders, identifying the associated responsibilities of business and IT process owners and providing metrics and maturity models to measure their achievement.

C.2 ISO/IEC 27000/1/2 Standards

ISO/IEC put in place an Information Security Management System family of standards in order to tackle constantly evolving information security issues faced by organizations. The series provides specific controls and recommendations in order to manage adequately security risks. The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT/technical/cybersecurity issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents.

In the family, particularly relevant for the purposes of this study is ISO/IEC 27002, Code of practice for information security controls. The latter is essentially a detailed catalogue of information security controls that might be managed through Information Security Management Systems. It provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining ISMS. Information security is defined within the standard in the context of the Confidentiality-Integrity-Availability triad.

C.3 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is US Government guidance for private sector organizations that own, operate, or supply critical infrastructure. It provides a reasonable base level of cyber security. It establishes basic processes and essential controls for cybersecurity. It is designed for individual businesses and other organizations to use to assess risks they face.

The framework is composed of three main components “Core”, “Profile” and “Tiers”. The “Framework Core” contains an array of activities, outcomes and references about aspects and approaches to cyber security. The “Framework Implementation Tiers” are used by an organization to clarify for itself and its partners how it views cybersecurity risk and the degree of sophistication of its management approach. A “Framework Profile” is a list of outcomes that an organization has chosen from the categories and subcategories, based on its needs and risk assessments.

An organization typically starts by using the framework to develop a “Current Profile” which describes its cybersecurity activities and what outcomes it is achieving. It can then develop a “Target Profile”, or adopt a baseline profile tailored to its sector (e.g. infrastructure industry) or type of organization. It can then define steps switch from its current profile to its target profile.

Annex D: Mapping of proposed indicators to standards

Table 7 provides an overview of the mapping of the proposed indicators to standards, listing the number of respective links of the mapped indicators and standards' domains/controls/goals.

Table 7: Mapping of indicators to standards

ID	INDICATOR	ISO/IEC 27002	NIST FRAMEWORK	COBIT 5
IND01	The number of serviced users (potentially affected by an incident)	15	3	2
IND02	Geographical distribution of services (e.g. cross border services potentially affected by an incident)	7	4	13
IND03	Social impact	6	1	2
IND04	Economic Impact	5	4	7
IND05	Environmental impact	2	1	4
IND06	Loss of service capabilities (e.g. reduced services, fail-safe services, etc.)	11	6	4
IND07	Resilience (e.g. failure recovery processes, crisis management processes, etc.)	11	4	2
IND08	The Recovery Time Objective (RTO) after an incident in the offered service	13	5	3
IND09	The Mean Downtime (MDT) after an incident in the offered service	10	5	3
IND10	Redundancy of services (e.g. alternative services, etc.)	14	4	6
IND11	Criticality of services in terms of security (i.e. CIA)	18	5	6
IND12	Number of Service Level Agreements (SLAs) with third parties	6	1	14
IND13	Market share and structure (e.g. number of operators, number of alternative providers, multi-service market, monopoly, etc.)	5	0	15
IND14	Coupling and complexity of services (e.g. structures of services, system and network designs, etc.)	12	1	19
IND15	Seasonality of dependencies/interdependencies (e.g. variations of service levels over seasons)	10	0	14
IND16	Temporal aspects of critical events	16	0	8
IND17	Dynamic aspects of dependencies/interdependencies	23	0	14

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

TP-04-18-962-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-265-3
DOI: 10.2824/124305