D6.2

Guidelines on cybersecurity governance for EPES (V2)

DOCUMENT	D6.2	**WORKPACKAGE**	WP6
DELIVERABLE STATE	FINAL	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V1.0	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	31/03/2024	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PU	**DURATION**	3 YEARS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560

DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain CyberSEAS consortium parties, and may not be reproduced or copied without permission. All CyberSEAS consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CyberSEAS consortium as a whole, nor a certain party of the CyberSEAS consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020)
TOPIC	SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)
PRINCIPAL CONTRACTORS	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP6
DELIVERABLE TYPE	R Document, report
DISSEMINATION LEVEL	PU Public
DELIVERABLE STATE	FINAL
CONTRACTUAL DATE OF DELIVERY	31/03/2024
ACTUAL DATE OF DELIVERY	07/06/2024
DOCUMENT TITLE	Guidelines on cybersecurity governance for EPES (V2)
AUTHOR(S)	ENERIM
REVIEWER(S)	CINI, ZIV
ABSTRACT	SEE EXECUTIVE SUMMARY

HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	Cybersecurity governance, electric power and energy system

Document History

Version	Date	Contributor(s)	Description
D6.1 *V1.0*	*03/04/2023*	*ENERIM, ENG, ARN, CRE, ELV, ENE, ENG, FRA, SYN, TEL, WIN, CINI, ZIV*	*The original version of deliverable D6.1 on which deliverable D6.2 is built upon*
V0.1	20/03/2024	ENERIM	New chapter 6
V1.0	07/06/2024	ENERIM, ENG	Final version

Table of Changes in Version 2

Section	Contributor	Change description and motivation
Chapter 6	ENERIM	New chapter discussing Common governance model for EPES operators.

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

BMI	Federal Ministry of Interior and Community in Germany
BSI	Federal Office for Information Security in Germany
CAN	Agenzia per la Cybersicurezza Nazionale
CDS	Common Data Space
CIC	Comitato Interministeriale per la Cybersicurezza
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team Italia
CVCN	Centro di Valutazione e Certificazione Nazionale
DGA	Data Governance Act
DPO	Data Protection Officer
DSBA	Data Spaces Business Alliance
DSO	Distribution System Operator
ECDS	Energy Common Data Space
ECRI	Electricity Cybersecurity Risk Index
EECDS	European Energy Common Data Space
EPES	The Electrical Power and Energy System
EU	European Union
GR-CSIRT	Cyber Defense Directorate in Greece
HVK	Finnish National Emergency Supply Agency (huoltovarmuuskeskus)
HNDGS	Hellenic National Defense General Staff
IDS	International Data Space
ISA	Information Security Act
ISAC	Information Sharing and Analysis Centre
KRITIS	Operators of Critical Infrastructures in Germany
NCSA	National Cybersecurity Authority in Greece
NDGS	National Defense General Staff in Greece
NFV	Network Function Virtualisation

NIS 2	The Network and Information Security Directive
NORM	New-generation Open Real-time Smart Meter
OES	Operators of Essential Services
PMU	Phasor Measurement Unit
RES	Renewable Energy Sources
SPOC	Single Point of Contact
TSO	Transmission System Operator
URSIV	Government Information Security Office in Slovenia
WP	Work Package

Executive Summary (Updated)

This document is a deliverable reporting contribution made under Task 6.1 of project CyberSEAS. The main target of Task 6.1 is developing cybersecurity governance related guidelines for the cooperation between different players in energy supply chain. Guidelines for cybersecurity governance of common energy data spaces as a building block for the cooperation are under special focus. To support the target, this document encompasses the following content:

1) Recent European funded projects contributing to cybersecurity governance in energy sector are briefly reviewed. The projects are EU-SysFlex, Phoenix and SUCCESS. The aim of this study is to gather and present the recently developed knowledge on cybersecurity governance in energy domain.
2) Regulatory frameworks regarding cybersecurity governance on both national and European levels are reviewed. For the European level, the focus is on the network code for cybersecurity aspects of cross-border electricity flows provided by ENTSO-E and EU-DSO in 2022. For national level frameworks, different European countries including Finland, Estonia, Slovenia, Italy, Greece and Germany are under focus. The aim of the review is to extract the best and worst practices and lessons learned.
3) Comparing the information gathered about national and European level frameworks as well as from the recent European projects, a list of guidelines about how to develop a cybersecurity governance model for cooperation of different players in energy domain (specifically in energy common data spaces) is provided.
4) Exploring NIS 2 directive and its requirement for organizations and provide a common cybersecurity governance model for EPES operators in compliance with NIS 2.

This report is the second deliverable of Task 6.1. and it will extend the first version of the deliverable by exploring NIS 2 directive and its implications and requirements. Furthermore, a common cybersecurity governance model is provided based on research and lessons learned throughout the period of CyberSEAS project.

1 Introduction (Updated)

The modern and restructured electric energy systems need for significant interactions and data exchanges between different stakeholders to ensure security and efficiency of energy system operation. In modern energy systems, several stakeholders play different roles with different goals. Needless to mention, prosperity of the system is tightly tied to an effective cooperation among the stakeholders. The effective cooperation calls for interactions and data exchanges which can be executed in common data spaces. To ensure security of electric power supply, it is necessary to ensure cybersecurity in the multi-stakeholder environment as well as the common data spaces as building blocks of the environment. This deliverable elaborates on cybersecurity guidelines for the cooperation between different players in energy supply chain as well as energy common data spaces.

1.1 Objective of the deliverable

The main objective of this deliverable is to study the existing cybersecurity governance models in different countries in Europe as well as to present relevant guidelines for cybersecurity governance of the cooperation between different players in energy supply chain as well as energy common data spaces. With the knowledge gained by research and lessons learned, a common cybersecurity governance model is provided.

The overall planning of the CyberSEAS project is depicted in the following figure. As can be seen, WP6 in the project focuses on cybersecurity of energy common data spaces. In the work package, there are four tasks namely cybersecurity governance for EPES operators and other stakeholders, secure and privacy preserving data exchange among operators, orchestrated management of data breaches among supply chain operators and rules & tools for operators' coordination and reporting to CERTs in case of incidents. Current report is dedicated to the first task which is cybersecurity governance for EPES operators and other stakeholders. As the title implies, the focus of the task, and thus this report, is on guidelines for cybersecurity governance model for energy sector. This mainly includes but not limited to a set of policies for ensuring cybersecurity of energy system as well as authorities and bodies in charge of ensuring that the policies are adhered. To take steps in that direction, this report gathers and studies recent European projects in cybersecurity area. In addition, existing cybersecurity governance models in both European and national levels are reviewed. Comparing the gathered information, guidelines on cybersecurity governance models are provided in the report.

In summary, the main objectives of this report are listed below:

- Gather existing knowledge on cybersecurity governance from recent European funded projects in cybersecurity subject.
- Gather and study national and European level cybersecurity governance models for energy sector.
- List the best and worst practices and lessons learned from the studied governance models.
- Explore NIS 2 directive and its requirements
- Provide a common cybersecurity governance model in compliance with NIS 2 for EPES operators.

1.2 Connection to other tasks in the project

This report is a deliverable for Task 6.1 in WP6 of CyberSEAS project. The task is highly connected to activities and studies in the other tasks in the work package. The connections are briefly described here in below:

- Task 6.2 focuses on secure and privacy preserving data exchange among operators. It is clear that policies regarding secure and privacy preserved data exchange among different players are part of cybersecurity governance in energy common data spaces. Therefore, the authors assume that this task provides input to Task 6.2 about general policies for ensuring security of potential data exchanges among different players.
- Task 6.3 focuses on data breach event management. The current task covers different aspects of cybersecurity and variety of actions and measures including but not limited to data breach incidents. So, the authors assume that the current report provides inputs to Task 6.3 where some of the guidelines and policies are allocated to data breach management.
- Task 6.4 focuses on rules & tools for operators' coordination and reporting to CERTs in case on incidents. That task provides a general playbook for operators' coordination and reporting to CERTs that can handle different cyber incidents. This means that the rules in the playbook covers operators' coordination and reporting to CERTs in case of data breach incidents. So, the authors assume this task and Task 6.4 inputs each other regarding the coordination and reporting of cybersecurity events.

1.3 Structure of the document

This deliverable begins with some preliminary knowledge about energy common data spaces and their governance model in Europe. Then, cybersecurity policies and committees responsible for ensuring that the policies are adhered in different countries will be reported. Finally, the best and worst practices are followed by guidelines for cybersecurity governance of energy common data spaces.

The rest of the report is structured in four chapters:

- Chapter 2 provides background knowledge required by readers to better understand contribution of the report. The chapter contains five sections. The first section defines concepts which are used or pointed out in the report. The second section reviews European Common Data Spaces. The third section reviews different levels, players and their roles in electric power and energy system. The fourth section reviews energy common data space. Governance of the energy common data space is briefly described in the fifth section.
- Chapter 3 reviews EU funded projects dealing with cybersecurity governance. Among different projects, EU-SysFlex, Phoenix, SUCCESS and NRG5 are selected as the most relevant ones to be briefly reviewed.
- Chapter 4 reviews both national and European level regulatory frameworks for cybersecurity governance. In the European level, the focus is on network code for cybersecurity aspects of cross-border electricity flows published by ENTSO-E and EU-DSO in 2022. On the national level, cybersecurity governance models in energy sector

in different European countries including Finland, Estonia, Slovenia, Italy, Germany, Greece and Romania are covered.

- Chapter 5 provides the best and worst practices and the lessons learned based on the reviews provided in previous chapters.
- Chapter 6 explores NIS 2 directive and provides a common cybersecurity governance model in compliance with NIS 2 for EPES operators.
- Chapter 7 concludes the report by highlighting the most important and relevant findings and observations.

2 Background knowledge

This chapter provides the background and basic knowledge about different major players in energy domain as well as the European energy common data space and its governance model to ensure that potential readers are on the same page when talking about cybersecurity governance of energy common data spaces.

2.1 Electric power and energy system overview

An electric power and energy system consists of different elements ranging from electric power generators to the devices consuming electric energy at end user property. The elements in the system are usually categorized into four following levels:

- Generation level: The elements in the generation level mainly convert energy from different sources and in different forms to electric energy. Electric power generators in power plants and distributed energy resources are the main elements in the generation level. The elements can be divided into renewable and non-renewable power generators according to the source of energy. Fossil-fuel based power plants and nuclear power plants are examples of non-renewable power generators. Wind turbines and solar panels are samples of renewable power generators. In the generation level, the trend is towards renewable and distributed power generators which are expected to be locally installed very close to electricity consumption areas.
- Transmission level: Conventionally, power generators have been located outside of cities since they produce pollutions as well as they need water and fuel which are not necessarily available inside cities. This means that the power generated by power generators need to be transmitted to consumption areas which are cities and large industrial sites. In order to transmit electricity in long distances without significant energy loss, voltage level should be increased. This way, current level is decreased which decreases energy loss significantly. In many countries, elements in electricity networks with voltage levels higher than 115 kV form transmission level.
- Distribution level: In cities where electricity is consumed by the society, there is an electricity network which receives electricity from transmission network and distributes it among electricity consumers. The network and its elements form distribution level. The voltage level in distribution level cannot be the same as in transmission level mainly because land is scarce and expensive inside cities and the high voltage levels are dangerous for the society members. On the other hand, decreasing voltage to the consumption level can be translated to higher energy losses. To this end, voltage levels from a few kV to tens of kVs are usually selected for distribution level in order to make a trade-off between energy losses and safety of the society individuals.
- Consumption level: In consumer territory, there are different equipments that consume electricity such as a washing machine and a dishwasher. These equipments basically transform electricity into other forms of energy according to the end user wishes. The voltage level in the consumption level is either 110 V or 220 V. Larger consumers receive a 3-phase circuit and smaller ones have 1-phase circuits. In some countries like Finland where electricity is the main energy source of end users and electricity consumption per capita is high, 3-phase circuits are implemented almost everywhere.

In electric energy supply chain, there are many players acting in the above levels to ensure that the electricity is produced, transmitted, distributed and consumed economically, safely, securely, reliably and environmentally friendly. The main players and a brief description about their roles are provided in the following:

Power producer: Electric power generators from any type are owned/operated by power producers. In addition to technical operation of the generation facilities, these players participate in electricity market to sell their electricity production too. They may participate in ancillary service markets such as flexibility market too.

Transmission system operator: Transmission system operators construct, maintain and operate electricity transmission systems. In the construction phase, transmission system operators forecast potential changes in size and location of electricity demand and supply and develop their systems accordingly. Their objective is to ensure affordability and security of electric power supply with minimum required investments. In the operation phase, they forecast near future supply and demand and operate the system to economically and reliably transmit electricity to electricity consumption points. In the maintenance phase, transmission system operators ensure that the existing system and its components are operated in an appropriate way. Needless to mention, transmission system operators are mainly focusing on technical activities rather than business. Transmission system operators have natural monopoly so their business is under regulation.

Distribution system operator: Similar to transmission system operators, distribution system operators do construction, maintenance and operation of electric circuits but their systems are mainly in urban and suburban areas and have lower voltage levels. Distribution system operators mainly focus on technical activities, and due to their natural monopoly, their business activities are under regulation.

Market operator: In energy systems, different markets are developed to ensure transparent and competitive prices for electricity. The player is responsible for operating electricity market to ensure consumers have access to affordable and secure energy. Market operators develop and maintain relevant markets places for energy and ancillary service markets where power producers can sell their electricity production and consumers, aggregators and electricity retailers can buy their or their customers electricity needs. The markets places are developed and operated in a way that most affordable electricity production considering energy system security is implemented.

Balance responsible party: In electric energy system, electricity supply and demand should always be balanced to maintain system frequency. In any energy system, market players are also balance responsible parties who plan their operations to maintain the balance between their electricity supply and demand as well as their electricity procurement and sale. The player can be a producer, consumer or even a trader of electricity.

Balancing service provider: This player provides balancing services to a transmission system operator. This player can be a producer, consumer or a trader of electricity. By providing balancing services, balancing service providers give the chance to transmission system operators to invoke the service to maintain system frequency when necessary.

Imbalance settlement responsible: The player is responsible for the settlement of the difference between the contracted and realised quantities of energy products for the balance responsible parties. This player checks the exchanged energy and the amount of energy that was supposed to be exchanged with each balance responsible party and makes an invoice according to that. The invoice value depends on the difference between the contracted and realized energy exchange as well as imbalance price.

Electricity retailer: This player sells electricity to an end user. It sells and buys electricity directly from a producer, another retailer or via participating in the energy market. The competition among electricity retailers ensure that the retail price of electricity which is paid by end users is fair.

Energy service company: This player is a party that provides different services to the other players in electric energy system. Energy data exchange, energy metering operations, asset monitoring and energy trading companies are some examples for an energy service company.

Aggregator: In energy system, there are limits for market participants. As an example, a residential electricity consumer is not eligible to participate in wholesale energy market due to set threshold. So, the end residential consumer is bound to make a supply contract with a retailer who then participates in the wholesale market. The consumers can form a coalition which is managed by an aggregator to meet the threshold for participating in the wholesale market. Then, they can procure their electricity needs as well as offer ancillary services to the energy system. It is worthwhile to mention that an aggregator does not aim for aggregating consumers, it can aggregate small power production units to enable them participate in energy market and offer ancillary services too.

In order to have an affordable, secure and reliable energy system, the above-described players exchange relevant data and interact both with end users and each other. It is crystal clear that the data exchange and maintenance must be secure to achieve the target. This is the main incentive for the studies conducted to provide approaches for enhancing cybersecurity of the system.

2.2 Energy common data space

The Energy Common Data Space (ECDS) refers to a digital platform that provides a centralized and secure repository of energy-related data, allowing data to be shared across different organizations and stakeholders such as energy producers, distributors, and consumers in a harmonized manner. The data stored in the ECDS can be used for a variety of purposes, including market analysis, energy management and the development of new energy technologies and services. The European Energy Common Data Space (EECDS) is an initiative of the European Union (EU) to create a unified and secure platform for collecting, exchanging and sharing energy-related data. The EECDS is part of the European Commission’s efforts to create a European energy union and secure, sustainable, and competitive energy for all Europeans. It allows energy data to be exchanged and shared between different stakeholders such as energy related companies, national authorities, researchers and consumers. The platform will also ensure that data privacy and security are maintained.

Having these mentioned, EECDS increases transparency, interoperability and access to energy data across the EU, thereby facilitating the integration of renewable energy sources, energy efficiency measures and smart energy systems into the energy market. This platform is expected to provide valuable data and insights to support decision-making and the development of new energy technologies.

The main objectives of EECDS are listed in the following:

- To enhance the flow of energy data across the EU
- To improve energy market efficiency
- To increase transparency
- To facilitate the integration of renewable energy sources and energy efficiency measures.

The data that will be shared through EECDS will include information on energy consumption, energy production and energy trade. In addition to that, EECDS will contain data on energy infrastructure such as the deployment of renewable energy sources. The implementation of EECDS is being led by the European Commission and involves collaboration between EU Member States, energy market operators and other relevant stakeholders.

Finnish DATAHUB is a sample common data space in energy domain. The data space is designed and operated by FINGRID which is Finland's transmission system operator. The data space is mainly dedicated to retail market data including but not limited to smart meter data of retail customers as well as their contract information. Here, smart meter data is a time series of hourly electricity consumption and contract information includes contact information, address, name, type of connection point, the energy supplier, billing information, etc. Electric distribution companies, energy suppliers and retail customers are the main stakeholders in the common data space. Electric distribution companies provide meter data to the data space. Customer contract data is provided to the common data space by both electric distribution companies and energy suppliers. Electric distribution companies have access to both meter data and contract data for customers connected to their network. Energy suppliers have access to meter data and contract data of customers whose consumption is provided by them. Customers have access to their own meter data and contract data. If a customer terminates the contract with a supplier and signs a new contract with another supplier, access right to the customer data from the previous suppiler will be transferred to the new supplier. This common data space makes it very easy for stakeholders in the retail market to work together and share the necessary data with each other.

2.3 Governance of ECDS

A governance model for a common data space (CDS) is a set of policies, procedures and practices that are used to manage and regulate the use and sharing of data within the CDS. It is designed to ensure that data is used in a responsible and ethical manner, and that the privacy and security of data are protected.

A governance model for a CDS typically includes the following elements:

- **Data access and control policies:** These policies define who is allowed to access and use data within the CDS, and what they are allowed to do with it.
- **Data quality policies:** These policies define the standards and procedures that must be followed to ensure that data within the CDS is accurate, complete and up-to-date.
- **Data security policies:** These policies define the measures that must be taken to protect data within the CDS from unauthorized access, theft and other types of security threats.
- **Data privacy policies:** These policies define the measures that must be taken to protect the privacy of individuals whose data is stored within the CDS.

- **Data management policies:** These policies define the procedures for managing and organizing data within the CDS, including data backup and recovery, archiving and retention.
- **Data sharing policies:** These policies define the conditions under which data within the CDS can be shared with other organizations or individuals.
- **Compliance and audit policies:** These policies define the procedures for ensuring that the policies and procedures within the governance model are being followed, and for auditing the use and sharing of data within the CDS.

The EECDS is governed by the European Commission. The Commission is responsible for the management, maintenance and development of the platform, and for ensuring that the platform meets the needs and requirements of its users. To do so, the Commission works closely with Member States and other stakeholders.

In terms of data security, privacy and data protection, the EECDS is built on a set of technical and legal standards that ensure the responsible use of data shared through the platform. The standards cover a range of areas, including the following items:

- **Data security:** Technical standards are put in place to ensure the secure storage, transmission and processing of energy data. This includes measures to protect against unauthorized access, modification or theft of data.
- **Privacy and data protection:** Legal standards are put in place to ensure that data shared through the EECDS complies with relevant data privacy and protection regulations. This includes standards on data protection and privacy and procedures for obtaining informed consent for the use of personal data.
- **Data quality and accuracy:** Technical and legal standards are put in place to ensure that the energy data shared through the EECDS is of high quality and accuracy. This includes standards on data quality, data accuracy and data validation, as well as procedures for data verification and correction.
- **Interoperability:** Technical standards are put in place to ensure that the EECDS is interoperable with other data platforms and systems. This includes standards on data exchange, data integration and data compatibility.
- **Data sharing and access:** Legal standards are put in place to regulate the sharing and access to energy data shared through the EECDS. This includes standards on data sharing, data access and data use, as well as procedures for data licensing and intellectual property protection.

2.4 European initiatives on common data spaces

At the EU level, some initiatives have been created in recent years to address challenges related to the creation and the usage of European Common Data Spaces. These initiatives and the data space governance they proposed are briefly introduced in this section, as well as some considerations about how cybersecurity is covered so far by these initiatives.

OPENDEI – OPENDEI stands for "Open Data for European Interoperable Energy Services". It is a European Union-funded project aimed at developing an open and interoperable data ecosystem for the energy sector. The project brings together stakeholders from across the energy value chain, including utilities, service providers, technology providers, and research organizations, to develop a common framework for sharing and using energy-related data.

The primary goal of OPENDEI is to create a standardized and interoperable platform for sharing and using energy data.

OPENDEI, Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry, is a EU-funded Community Support Action which aims to detect gaps, encourage synergies, support regional and national cooperation, and enhance communication among the Innovation Actions implementing the EU Digital Transformation strategy in four domains: Manufacturing, Agriculture, Energy and Healthcare [1]. For what the Energy domain is concerned [2], OPENDEI investigates four key aspects, namely:

- Data model/Semantics – as the definition of an appropriate data model beyond a single sector is a key ingredient for interoperability.
- Data Sovereignty – i.e., the ability of a data owner to define what a third party is allowed to do with his data.
- Open API – as closed solutions will not create a real open and competitive market. Open APIs offer the perfect bridge between private infrastructure spaces.
- Security – because systems must be immune to cyber-attacks even under strong growth of IoT and rapid changes in digital technologies and decentralisation.

The **Design Principles for data spaces** position paper released in 2021 [3] mentions the public-private governance as one of the key principles for the successful instantiation of the Energy Data Space, highlighting that "*Public-private governance in the energy domain concerns both personal data and non-personal (i.e. industrial) data*". As noted in the Data space Governance and Business Models section of the same paper, "*Today's lack of a harmonised approach to establishing data spaces is more of a coordination and scaling problem than a technology problem.*". The paper then proposes a framework for the governance of the energy data space based on the Data Governance Act (DGA) [4] governing structure organized around two set of parties: Adhering parties – 'users' of the data space – and Certified parties – those parties that play a facilitating role in the data (sharing) process enabling adhering parties to 'use' the data space –. Each set carrying out specific activities belonging to four main areas:

1. Maintenance and further development of the set of agreements and standards defining the 'soft infrastructure' (i.e., of the authorisation framework).
2. Admission and certification of the members of the network (i.e., of all data intermediaries).
3. Technical and implementation support for certified and adhering parties.
4. Communication and education, aiming both at end users and IT vendors/professionals.

BDVA – The Big Data Value Association (from 2021, DAIRO - Data, AI and Robotics aisbl), is composed by more than 230 members all over Europe. Its mission is to **develop the innovation ecosystem** that will enable the **data and AI-driven digital transformation in Europe** [5]. **It includes a** *Data Sharing Spaces* **task force dedicated to data sharing spaces, which essentially focuses on** engaging the broad BDVA/DAIRO data sharing stakeholder community (producers, intermediaries and consumers along data value chains) to identify opportunities, challenges, and possible solutions for facilitating cross-sectoral data sharing and exchange practices; and to reason on a vision for how a safe, fair and ethical data sharing space can be achieved at EU-level [6]. Also relevant for the topic are the BDVA i-Spaces that offers secure data experimentation environments allowing Research, Education, and Innovation stakeholder to experiment and innovate with data, acting as hubs to connect different stakeholders at local and regional levels [7].

FIWARE – FIWARE position itself as *A curated framework of Open Source Platform components to accelerate the development of Smart Solutions*. It is a foundation driving the definition – and the Open Source implementation – of key open standards that enable the development of portable and interoperable solutions in a faster, easier and affordable way [8]. Particularly relevant for the EU Data Spaces are the FIWARE iHUBS, i.e. innovation hubs focused on the building of communities and collaborative environments to enable digital businesses to thrive at regional and global levels [9].

The **FIWARE FOR DATA SPACES** position paper of 2021 [10] includes security aspects related to the authentication and access control to shared data. The document includes a finer grain approach to these processes w.r.t. the one supported by the secure gateway of the IDS-connector.

Gaia-X – The GAIA-X European Association for Data and Cloud aisbl was funded in September 2020 to develop the technical framework and operate the Gaia-X Federation services. The association, which now counts over 350 members, has the main goal in the establishment of a federated ecosystem, where data is shared and made available in a trustworthy and transparent environment and where control is back to the users by retaining sovereignty over their data [11]. In particular, Gaia-X Hubs are the central, national contact points to inform about the Gaia-X Association. They are not a body or part of the Association, but rather act as independent think tanks, supporters or ambassadors and influencers for Gaia-X. Hubs group together all members from a specific region, users and providers, to work together at designing ideas, whilst implicitly identifying the consortia that will be able to implement those projects. Also, hubs collaborate across different territories to ensure the creation of pan-European data spaces where this is possible [12].

The **Data Space Business Committee position paper** of 2021 [13] provides the current state of data spaces in a set of verticals, including energy. In the document, security is mentioned as one of the key elements for the success of the data space usage in all sectors. In particular for the energy domain the focus seems to be on the prevention of data breaches, mainly through: federated identity management for individuals and organizations, sovereign data exchange to manage consent and usage control, and cybersecurity compliance and certification. It is not clear if and how other cybersecurity functions (e.g. detect, response and recovery) are addressed by the cases presented. The **Gaia-X architecture framework** [14] also mentions security-by-design as one of the Gaia-X principles, while the **Policy Rules Document** [15] also introduces a set of 20 cybersecurity measures that individual organizations that contribute solutions/services to the Gaia-X environment should implement to safeguard the shared data.

IDSA – The International Data Spaces Association, composed by 138 members, aiming at the development of a global standard for international data spaces (IDS) and interfaces, as well as to foster the related technologies and business models that will drive the data economy of the future across industries [16]. The IDSA Hubs incorporate all members, research organisations and companies that use IDS concepts and standards per country (currently

Hubs have been established in: Belgium, Bulgaria, Czech Republic, Finland, France, Greece, Italy, The Netherlands, Poland and Spain). The IDSA Hub is facilitated by a university, research organisation or non-profit entity. It enables communication between the Hub and the Association and drives forward the dissemination and adoption of the IDS standard. The hub facilitator reaches potential members, projects, research centres and connects with governments. In addition, there are IDSA Competence Centers. They offer specialized knowledge or a specific service as part of the IDS offering, such as a testbed or training services (currently there are competence Centers established in Germany, in Greece and in Spain) [17].

On cybersecurity governance, IDSA published in 2021 the **Governance for Data Space Instances** position paper, with the aim of "*identify the topics requiring adequate governance in the broader context of both intra data and inter data space interoperability [...] and to detail the associated roles and responsibilities for the main IDS- stakeholders in jointly providing the governance for developing and deploying data space instances*" [18]. The report, which builds upon the OPEN DEI data space design principles, the IDS Reference Architecture Model [19] and the IDSA Rule Book [20], mentions security, especially in relation to the usage of the security gateway [21] as part of the IDS-connector (the application container proposed by IDSA).

In September 2021 BDVA, FIWARE, Gaia-X and IDSA launched the **Data Spaces Business Alliance (DSBA)** with a common objective to accelerate business transformation in the data economy [22]. One of the joint working areas of the DSBA is supporting the existing organisations and data spaces by pooling their tools, resources, and expertise in a focused way. As described above, each of these four initiatives developed its own concept of hubs, with similarities and complementarities. Put together, they reach the number of 90+ hubs distributed over 34 countries, thus having the potential to achieve global impact [23]. Current activities of the DSBA Hubs are directed toward two main goals: first, the definition of the DSBA radar, which aims at providing DSBA partner network with an overview of current data space initiatives. Second, the creation of the DSBA brokering and project ideation platform, to facilitate networking and brokering activities among the members and communities of the DSBA associations and with other key players in the Data Spaces landscape. The platform is accessible at [24].

In conclusion, the analysis shows that all major EU initiatives are working to define the data governance for EU data spaces. Cybersecurity is mentioned by most of the initiatives as an important aspect of the governance, that at the moment seems more oriented to the support for federated authentication and access control processes, and less covering other cybersecurity aspects like the detection of attacks and breaches, as well as how data space participants should behave and interact to react to cyber-attacks and incidents that involves data and services across the data spaces.

It is also not well clear from the documents above how cybersecurity governance and its processes are integrated with the broader data space governance, e.g., by defining potential interdependencies and effects of cybersecurity procedures to data governance procedures. Examples of this are cases where data exchanges might be temporarily suspended as a consequence of a cyber-attack, or cyber incident, to one or more members of the data space. This may depend on the relative newly of some of the governance defined.

3 EU funded projects dealing with cybersecurity governance

This chapter reviews the works that have been done in different EU funded projects. The study covers EU-SysFlex, Phoenix and SUCCESS projects.

3.1 EU-SysFlex

During the H2020 EU-SysFlex project [25], similar challenges in the EPES cybersecurity governance and gaps in standards were analysed. The aim of the EU-SysFlex project was to identify issues and solutions associated with integrating large-scale renewable energy and create a plan to provide a practical assistance to power system operators across Europe. This included the ability to enable cross boarder data exchange between EU energy data hubs, operated by TSOs.

Although there was ambition to develop a cybersecurity governance model during the EU-SysFlex project, the reality was, that the different approaches for EU countries on centralisation, decentralisation of data, privacy requirements for energy data and energy sector policies required more research and discussions before reaching a common understanding on a cybersecurity governance model.

Here are the key takeaways form the governance perspective from EU-Sysflex [26]:

1) The current legislation and standards provide generally sufficient guidelines how to ensure data protection through technology design, especially when updates to ePR and NIS, new Network Code on Cybersecurity, ISO/IEC 2700X:2021, etc. enter into force soon. However, there are areas where more work is needed. For example, when changing the smart meter operator (in case this is different from system operator) and transferring customer data and the consumption data from old to new one. Additionally, the complexity lies in investing sufficient resources into the privacy domain to enable privacy by design.
2) There is a lack of communication to exchange the data about cyber incidents both in energy sector in general but also in the energy data exchange domain specifically. The experiences from different sector's technology providers and system operators need to be shared and used among the energy sector participants in order to learn from mistakes and achievements related to cyber incidents. While the new Network Code on Cybersecurity will address some of the issues, unfortunately the information sharing (e.g., on vulnerabilities, misconfigurations, 0-day exploits) between the adversaries is much more efficient.
3) The governance and control mechanisms need support from the participating organisations to make policy and business decisions and pave the way for different technological solutions and capabilities to have security by design as a main building block enabled from the beginning. Also, slow technology adaption by energy sector participants is a bottleneck in coping with cybersecurity challenges.

In conclusion, a political challenge must be solved first for the cybersecurity governance in EPES before full technical solutions can be applied. This needs the active participation of EU member states together with ENTSO-E and EU-DSO and ENISA to work on industry regulations level with EU government bodies. From the Horizon Europe project perspective (like CyberSEAS and EU-SysFlex), the contribution from technology demonstrations and industry inside information can help showcasing the problem areas and available solutions.

3.2 Phoenix

Phoenix is a project developed under Horizon 2020 call H2020-SU-DS-2018-2019-2020 focused on Digital Security.

The project title was Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks. The project started in September 2019 and ended in September 2022 after 37 months of development.

PHOENIX aimed to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at a reasonable cost.

PHOENIX considered to fulfil 3 strategic goals:

- Strengthen EPES cybersecurity preparedness by employing security a) "by design" via novel protective concepts for resilience, survivability, self-healing and accountability, and b) "by innovation" via adapting, upgrading and integrating a number of TRL5 developments to TRL7-8 and validating them in real-live large-scale pilots.
- Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level, a novel fully decentralized inter-DLTs/blockchain based near real-time synchronized cybersecurity information awareness platform, among authorized EPES stakeholders, utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group.
- Accelerate research and innovation in EPES cybersecurity by a novel deploy, monitor, detect and mitigate DevSecOps mechanism, a secure gateway, privacy preserving federated Machine Learning algorithms and establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.

PHOENIX project based of a prestigious consortium of 25 partners (+1 third party), supported by the CERT-RO, covering all required expertise including renewable energy sources (RES) generation/VPP, TSO, DSOs, aggregators, retailers, prosumers, end-users, technology providers, SMEs. PHOENIX validation will take place in 5 large scale pilots covering the complete value chain from generation to consumption, including cross-border experiments and cascading effects to other critical infrastructures.

Phoenix project was a very ambitious project and the Phoenix platform that was the main product of the project was based on multi-layered architecture which is shown in the following figure.

.

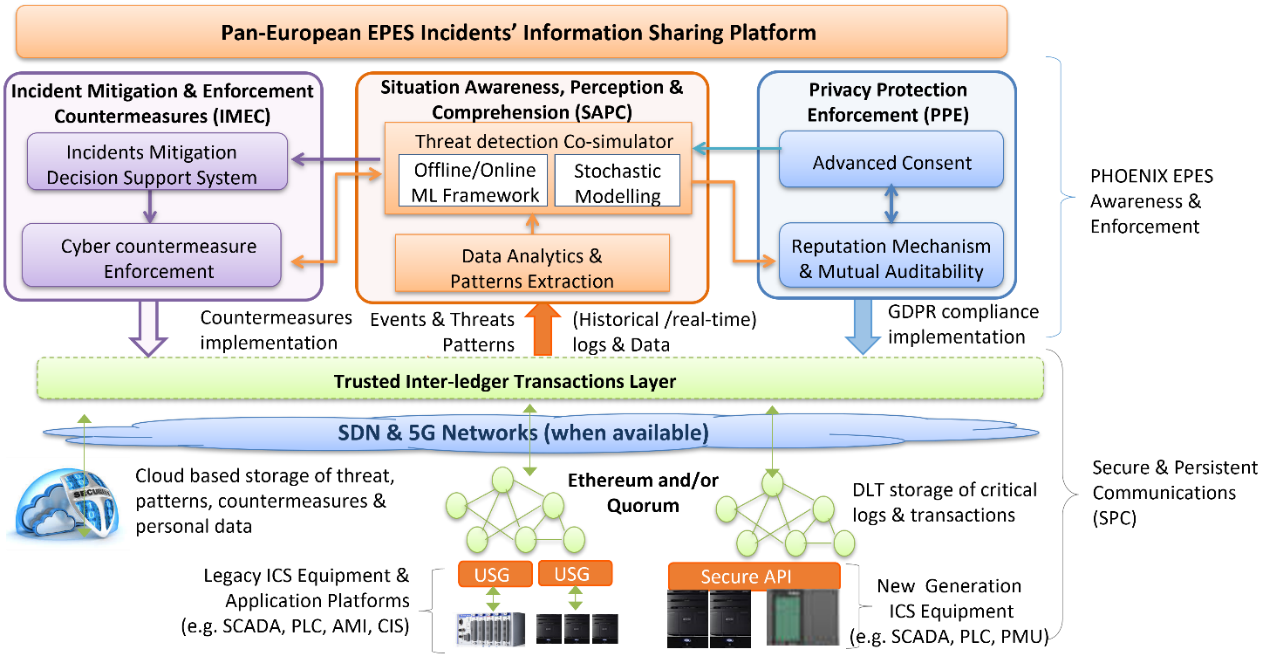

Pan-European EPES Incidents' Information Sharing Platform
Incident Mitigation & Enforcement Countermeasures (IMEC)
Incidents Mitigation Decision Support System
Cyber countermeasure Enforcement
Situation Awareness, Perception & Comprehension (SAPC)
Threat detection Co-simulator
Offline/Online ML Framework
Stochastic Modelling
Data Analytics & Patterns Extraction
Privacy Protection Enforcement (PPE)
Advanced Consent
Reputation Mechanism & Mutual Auditability
PHOENIX EPES Awareness & Enforcement
Countermeasures implementation
Events & Threats Patterns
(Historical /real-time) logs & Data
GDPR compliance implementation
Trusted Inter-ledger Transactions Layer
SDN & 5G Networks (when available)
Cloud based storage of threat, patterns, countermeasures & personal data
Ethereum and/or Quorum
DLT storage of critical logs & transactions
Secure & Persistent Communications (SPC)
Legacy ICS Equipment & Application Platforms (e.g. SCADA, PLC, AMI, CIS)
USG
USG
Secure API
New Generation ICS Equipment (e.g. SCADA, PLC, PMU)

Figure 1 Phoenix Project multi-layered architecture [27]

The aim of Phoenix was to provide a platform that can be used on different layers of an Electricity Grid (national, regional and local) by different EPES and share the Cybersecurity Intelligence Information acquired on any level to trusted partners based on standard protocols.

The approach for cybersecurity governance in Phoenix was based on detecting cybersecurity incidents using different tools and using federated machine learning and disseminate them over a trusted and secure channel based on Inter-ledger communication and standard protocols.

The communication over different participants of the Energy grid was an important aspect in Phoenix project that developed the I2SP Pan-European Incidents Information Sharing Platform that is in the top of the architecture. In Phoenix project, one large scale pilot was dedicated and extensively testing the I2SP Platform. The LSP was hosted in Romania communicating with all other LSPs.

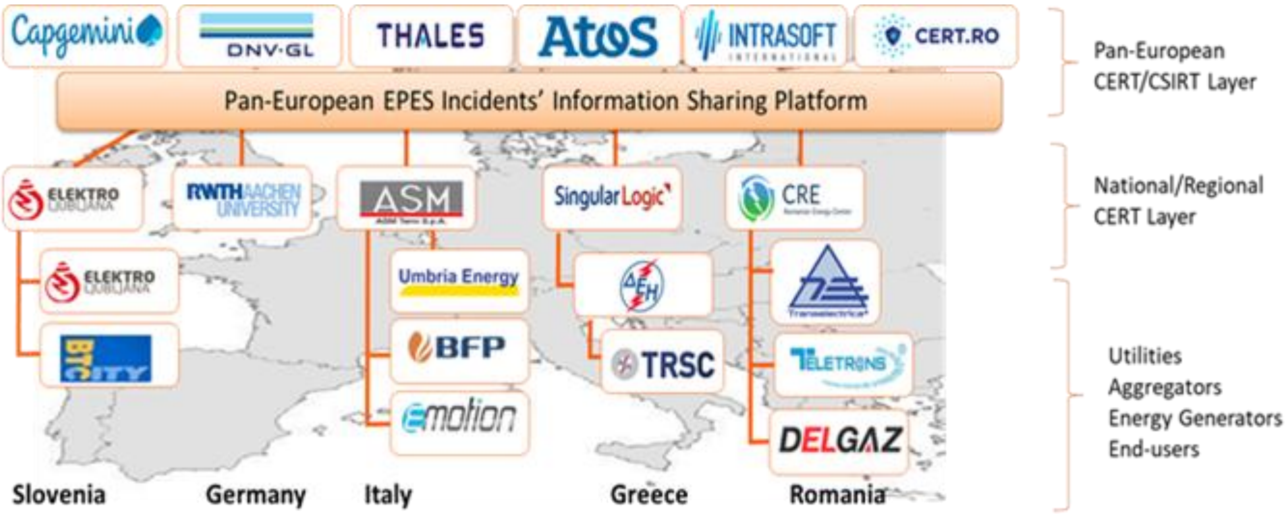


Figure 2 Pan-European EPES Incidents Information Sharing Platform [27]

In the information sharing over different entities that participated to the project is depicted in different layers.

- Utilities, aggregators, energy producers, end-users
- National and regional CERT Layer
- Pan European CERT/CSIRT Layer

3.3 SUCCESS

The SUCCESS project was developed under Horizon 2020. The complete title of the project was SUCCESS - Securing Critical Energy Infrastructures. The project was developed starting in September 2016 and concluding in February 2109.

The success project developed an overarching approach to threat and countermeasure analysis with special focus on the vulnerabilities introduced by Smart Meters. Success will achieve this objective by encapsulating the key challenges of Security, Resilience, Survivability and Privacy in 3 use cases which will focus the Research, Implementation and Evaluation concepts.

Using a security by design approach focussing on resiliency and survivability, SUCCESS proposed a new joint design of Energy Infrastructure and ICT. SUCCESS will build on these research results, implementing a New-generation Open Real-time Smart Meter (NORM). NORM aims to secure the end nodes of the energy system while providing innovative services in a customer centric grid.

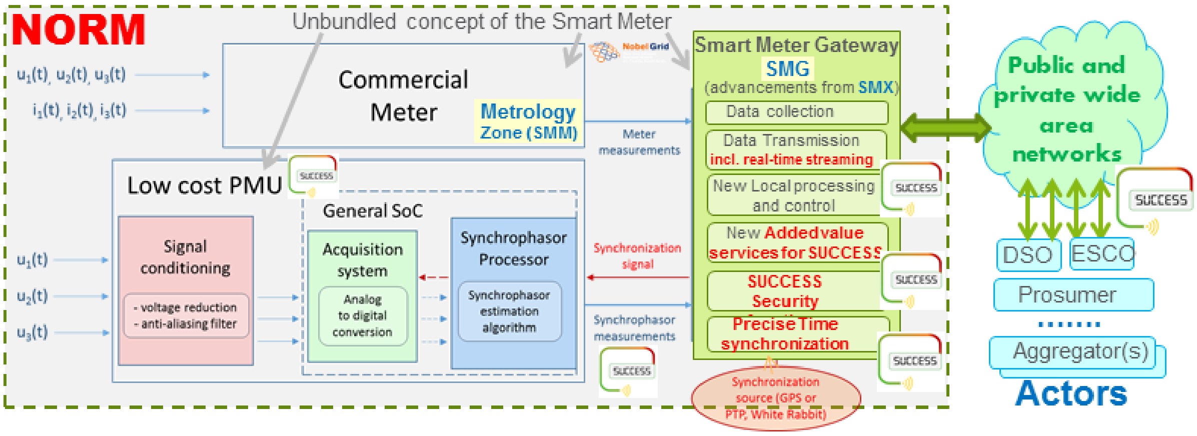

NORM
Unbundled concept of the Smart Meter
$u_1(t)$, $u_2(t)$, $u_3(t)$
$i_1(t)$, $i_2(t)$, $i_3(t)$
Commercial Meter
Metrology Zone (SMM)
NobelGrid
Meter measurements
Smart Meter Gateway SMG
(advancements from SMX)
Data collection
Data Transmission incl. real-time streaming
New Local processing and control
New Addedvalue services for SUCCESS
SUCCESS Security
Precise Time synchronization
Synchronization source (GPS or PTP, White Rabbit)
Low cost PMU
SUCCESS
General SoC
Signal conditioning
- voltage reduction
- anti-aliasing filter
Acquisition system
Analog to digital conversion
Synchrophasor Processor
Synchrophasor estimation algorithm
Synchronization signal
Synchrophasor measurements
$u_1(t)$
$u_2(t)$
$u_3(t)$
Public and private wide area networks
DSO
ESCO
Prosumer
Aggregator(s)
Actors

Figure 3 NORM Architecture defined in SUCCESS project [28]

At systems level, a cloud approach, based on double virtualization, is proposed. SUCCESS defined security countermeasures, Security Monitoring Centres at DSO and Pan-European levels, secure communications solutions using Network Function Virtualisation (NFV) and the LTE and 5G mobile communication technologies. This work was complemented by data privacy studies to ensure the acceptability of the results by consumers. Trials will be run in Ireland, Italy and Romania.

SUCCESS development was also based on an architecture that is detailed in Figure 5. SUCCESS produced a comprehensive framework for securing Smart Grids and similar critical infrastructures expressed as:

- A set of concepts for Security, Resilience, Survivability and Privacy by design,
- Further development of the New-generation Open Real-time Smart Meter (NORM) produced by the NobelGrid project www.nobelgrid.eu with security functionality and the inclusion of a Phasor Measurement Unit (PMU),
- A range of prototypes and blueprints for future energy and ICT sector products and services,
- Recommendations on countermeasures to address short-, medium- and long-term threats.
- The SUCCESS platform implementing countermeasures at TRL-4 level and demonstrated in field trials Specifications for Certification testing and standardization of the approaches.

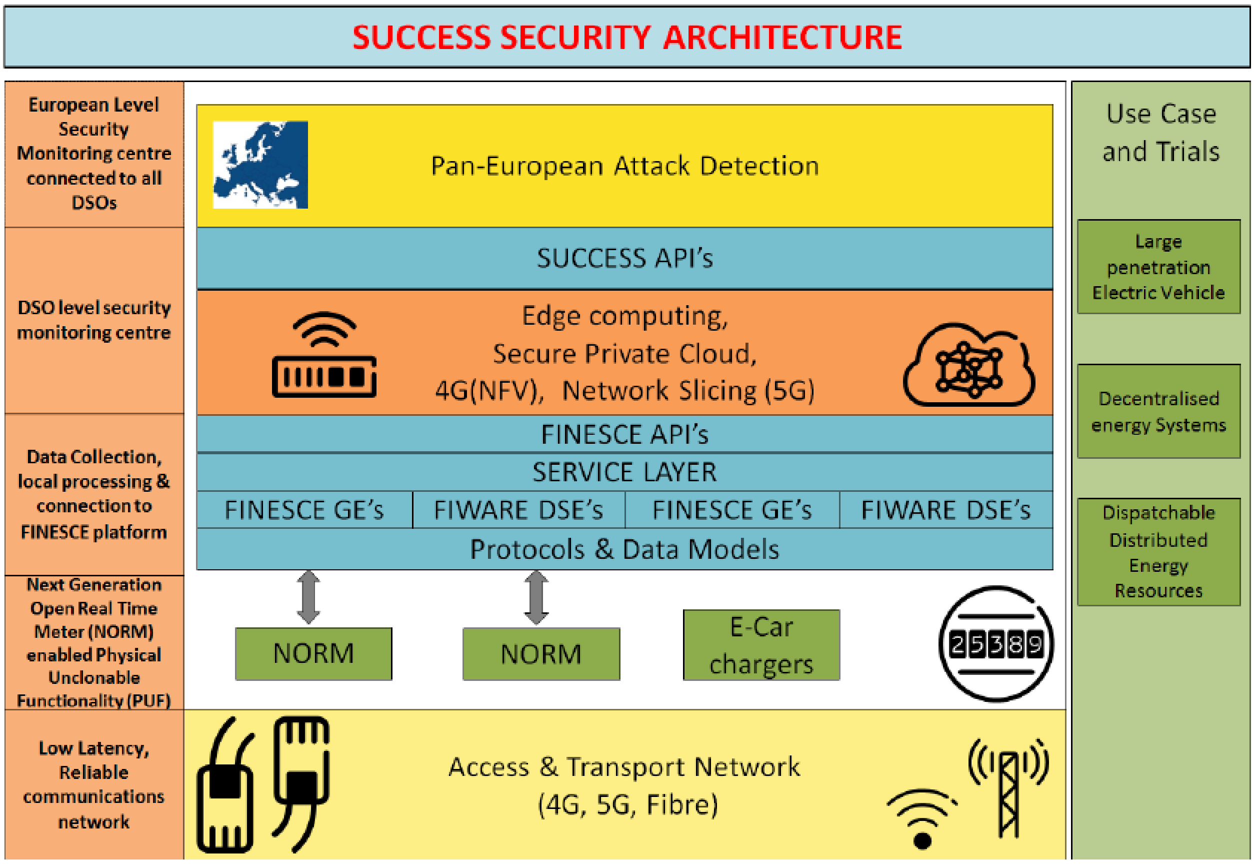

SUCCESS SECURITY ARCHITECTURE
European Level Security Monitoring centre connected to all DSOs
DSO level security monitoring centre
Data Collection, local processing & connection to FINESCE platform
Next Generation Open Real Time Meter (NORM) enabled Physical Unclonable Functionality (PUF)
Low Latency, Reliable communications network
Pan-European Attack Detection
SUCCESS API's
Edge computing,
Secure Private Cloud,
4G(NFV), Network Slicing (5G)
FINESCE API's
SERVICE LAYER
FINESCE GE's
FIWARE DSE's
FINESCE GE's
FIWARE DSE's
Protocols & Data Models
NORM
NORM
E-Car chargers
25389
Access & Transport Network
(4G, 5G, Fibre)
Use Case and Trials
Large penetration Electric Vehicle
Decentralised energy Systems
Dispatchable Distributed Energy Resources

Figure 4 SUCCESS Security architecture [28]

3.4 Conclusion

Chapter 3 tried to review the work that has been done in different EU projects regarding the cybersecurity governance of common data spaces especially in energy domain. The reviewed projects are EU-SysFlex, Phoenix and SUCCESS. This list can be extended by reviewing more relevant projects in D6.2.

4 Regulatory framework on national and European levels

This chapter reviews existing cybersecurity governance frameworks on European and national levels. The frameworks focus on high-level policies as well as committees which are responsible for ensuring implementation of the policies.

4.1 Network code for cybersecurity aspects of cross-border electricity flows

The European Commission is very interested in the Cybersecurity problem that is more challenging every day considering the political developments inside EU and at the EU borders.

In the attempt to shape The Europe's Digital Future, a strategy was defined and developed by EC. More details about the strategy are provided in the following table.

Table 4-1 EC Cybersecurity development

	Cybersecurity Policies
New Strategy	The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy at the end of 2020.
Legislation and certification	• Directive on security of network and information systems (NIS Directive) • ENISA – the EU cybersecurity agency • Cybersecurity Act • Certification • NCCS Network Code for Cyber-Security focusing on aspects of cross-border electricity flows
Investment	• Support for research and innovation: Horizon 2020 and cPPP; Horizon Europe • Cybersecurity Competence Centre and Network; Romania
Policy guidance	The Commission's blueprint for rapid emergency response provides a plan in case of a large-scale cross-border cyber incident or crisis.
Skills and awareness	We can only ensure digital security if we have experts with the right knowledge and skills, and there are currently not enough. That is why the Commission is taking action to stimulate the development of cybersecurity skills.
Cyber community	ENISA, ISACs, JRC, CSIRTs/CERTs

Other cyber policy areas	Cybercrime, Cyber diplomacy, Defence

This section reviews cybersecurity governance model and policies explained in "Network Code for Cybersecurity Aspects of Cross-border Electricity Flows" by ENTSO-E and EU-DSO, 2022. The critical infrastructures that are a target for cyber-attacks are one of the concerns in European Cybersecurity strategy. The Energy grid is one of the most complicated and geographically extended networks that are interconnected over different European borders.

The interconnection of different national grids in different Europe countries was succeeded, not easily but we have a stable interconnected grid over EU. Even there is an important degree of heterogeneity of the National Grid adapting the Network Codes for being able to interconnect the grids.

Different TSOs that control the interconnected transmission networks have different cybersecurity approaches and strategies. In this case, the EC has tried to homogenise the cybersecurity approaches of different TSOs and other EPES connected to the transmission grid. The first step for alignment of cybersecurity strategies not only for the energy grids is the NIS Directive indicated in Table 4-1 EC Cybersecurity development. Considering that a more detailed document focusing the Energy Grid, EC has the initiative to sustain the defining and applying such a document. This document is based on the models of Network Codes and was handed for development to ENTSO-E and EU-DSO.

The Network Code on Cybersecurity aims to set a European standard for the cybersecurity of cross-border electricity flows. It includes rules on cyber risk assessment, common minimum requirements, cybersecurity certification of products and services, monitoring, reporting and crisis management. This Network Code provides a clear definition of the roles and responsibilities of the different stakeholders for each activity.

The timeline for developing the document is indicated in Figure 5 Network Code Cybersecurity timeline.

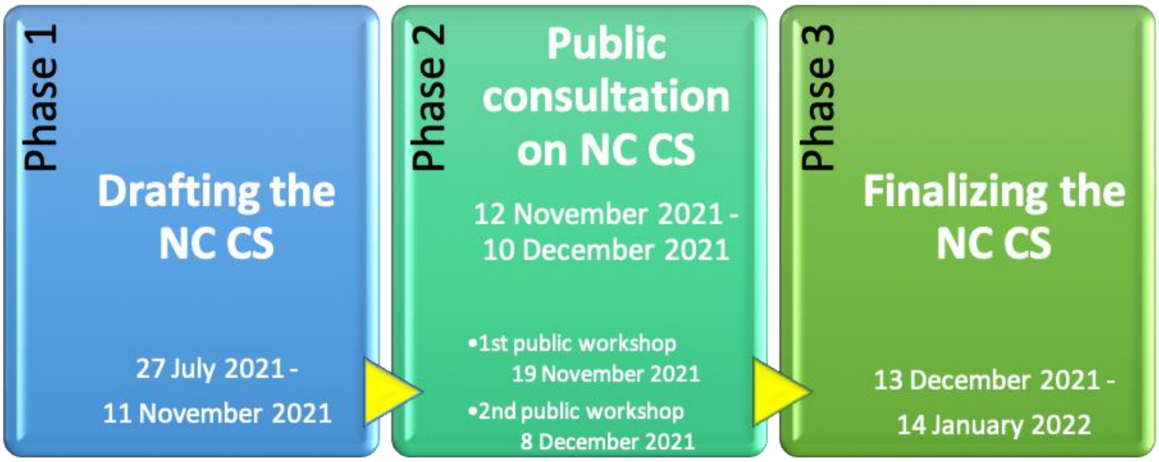


Figure 5 Network Code Cybersecurity timeline

It is worthwhile to mention that during the development of the network code, other entities provided important insights as:

- ACER
- DG Energy
- Enisa
- All Nemo committee
- NIS cooperation Group
- Smart En
- T&D Europe

4.2 Finland

In Finland, the first cybersecurity strategy was published in 2013. The strategy was part of the national security strategy implementation. The main target for the strategy is to increase comprehensive security as well as to initiate nationwide contingency management planning. In order to put the strategy into practice, an action plan consisting of 74 actions was prepared in 2014. The second action plan consisting of 22 actions was prepared in 2017. The updated cybersecurity strategy was published in 2020.

The Finnish cybersecurity strategy developed and published in 2013 contains ten alignments out of which six alignments set requirements to the national critical infrastructures including energy sector. The alignments are listed here:

- An efficient cooperation model will be set up between the authorities and the different actors to promote cyber threat prevention.
- The overall cybersecurity situational awareness of the vital functions of society will be increased.
- The ability to detect and combat cyber threats and incidents of vital functions of society as a part of economic continuity management will be maintained and further developed.
- The understanding and competence of all actors in society over cybersecurity will be improved.
- Cybersecurity will be ensured via enforcing national law.
- Relevant service models, common fundamentals and responsibilities will be assigned to authorities and business operators to manage cybersecurity.

The second action plan published in 2017 had two main goals for critical infrastructures:

1. The adequate level of security of supply based on energy and climate strategy must be secured by the ministry of economic affairs and employment of Finland.
2. The cybersecurity of the companies critical to the security of supply must be improved by Finnish National Emergency Supply Agency (huoltovarmuuskeskus (HVK)). This is done by providing resources for a program called KYBER2020 which aims to improve cybersecurity of companies.

It is worthwhile to mention that KYBER2020 program consists of different sector specific programs including KYBER-ENE which is an energy sector specific program. The KYBER-ENE was initiated to develop guidelines for energy sector cybersecurity. The program was voluntary, but several energy sector companies took part in the program.

As mentioned earlier, ensuring the security of supply is one of the main goals for the second action plan published in 2017. From energy perspective, Finnish national emergency supply agency (HVK) assures an uninterrupted availability of energy where ecological sustainability and competitive pricing are among goals too. The Finnish national emergency supply agency (HVK) designed sector specific pools where preparedness of the companies in the sector is continuously monitored and developed. It is worthwhile to mention that energy production, transmission and distribution system operators are in the same pool.

4.2.1 KYBER-ENE

The KYBER-ENE program aims at developing cybersecurity in the energy sector. To do so, the main activity of the program is to develop and maintain level of competence of different players in the energy sector since they know best the correct operation and appropriate use of the energy system. The target group of KYBER-ENE are the key actors who produce critical energy products and services, as well as the key actors who maintain and secure the critical infrastructure of energy production, transmission and distribution. The KYBER-ENE program mainly focuses on cybersecurity management in an energy company, cyber detection capability in an energy company, safe utilization of IoT and developing cooperation in the area of cybersecurity in energy sector. The activities of KYBER-ENE program in the focal areas are briefly described hereinafter. The KYBER-ENE comprises of some other activities which are not covered here since the activities such as company-specific workshops are confidential. It is worthwhile to mention that KYBER-ENE provides recommendations about cyber detection capabilities and safe utilization of IoT technologies which are not reviewed here.

4.2.1.1 Cybersecurity Management in Energy Companies

In energy sector, basic operations of the system including energy production, transmission, distribution and related services can be affected by cyber incidents. Energy sector is subject to variety of incidents including but not limited to data fishing, denial of service attacks, business interruption ransomware, data leaks and thefts, the threats related to remote control of systems and devices and attacks through vulnerable building automation systems and weakly protected IoT systems.

It is usually difficult to delegate or outsource cybersecurity work to one person mainly since understanding the subject needs knowledge in a variety of disciplines. In order to facilitate that, KYBER-ENE developed various workshops, models and mapping procedures for energy companies. Among the activities, KYBER-ENE developed the following cybersecurity management model.

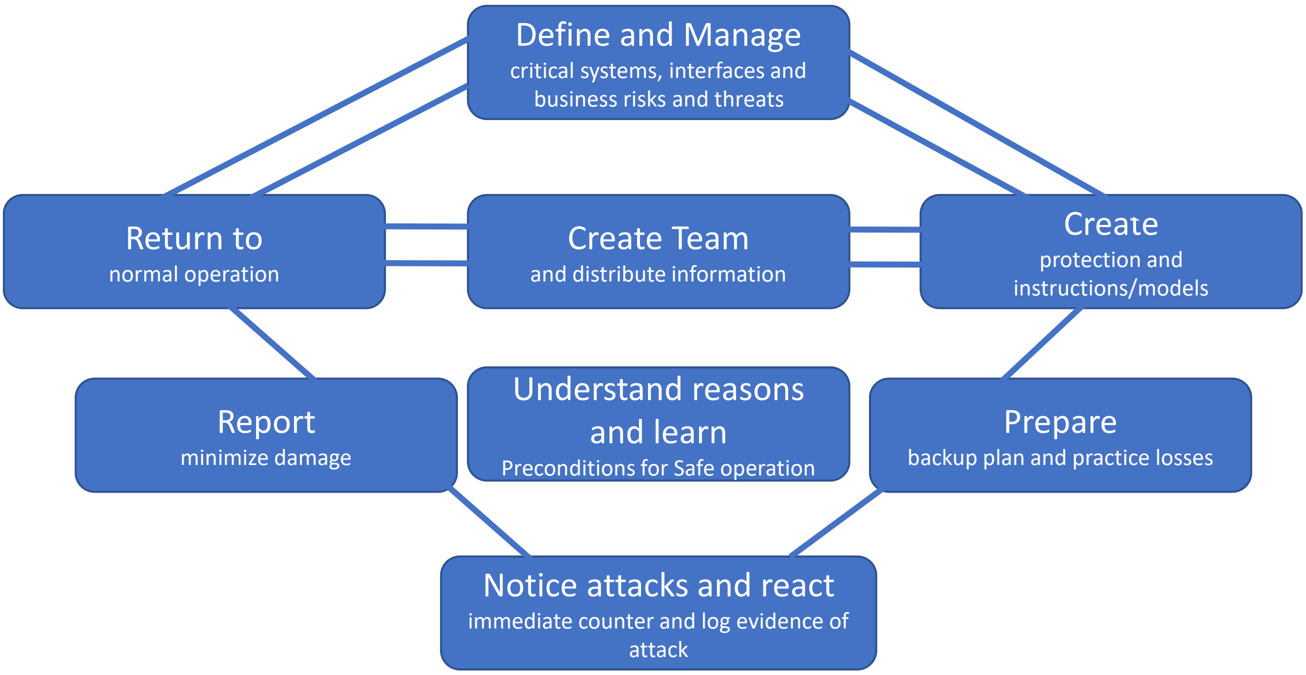

Define and Manage
critical systems, interfaces and business risks and threats
Return to
normal operation
Create Team
and distribute information
Create
protection and instructions/models
Report
minimize damage
Understand reasons and learn
Preconditions for Safe operation
Prepare
backup plan and practice losses
Notice attacks and react
immediate counter and log evidence of attack

Figure 6 Cybersecurity management model and elements

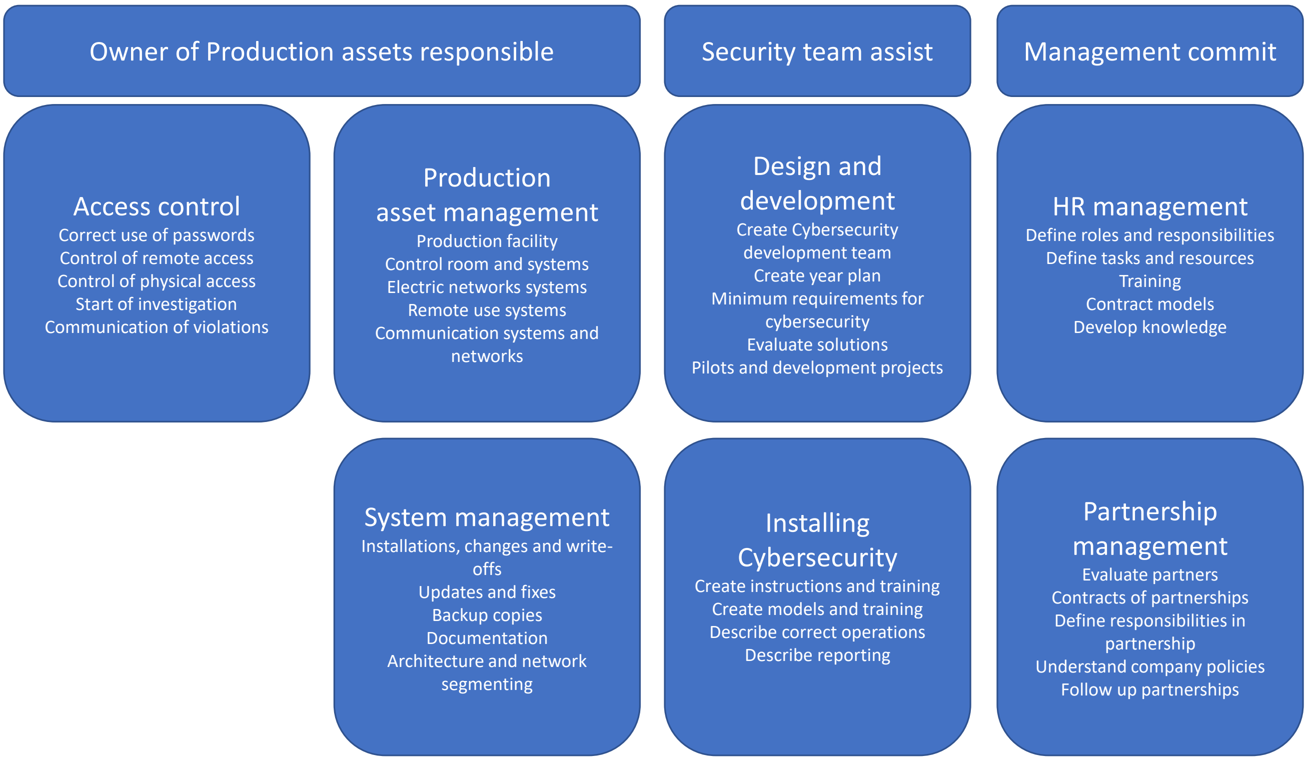
The management model consists of different elements which are described in below:

- Team assembly and information sharing: Any organization must identify and commit necessary key personnel who are responsible for cybersecurity development of the organization as well as support groups with a positive attitude towards cybersecurity development. It is recommended to setup an internal forum to share cybersecurity materials including but not limited to development plans, training materials, instructions, potential risks and jeopardizing events.
- Studying reasons and prerequisites for cybersecure operation: Understanding cybersecurity holes and weaknesses is necessary to improve the current situation.
- Map and manage critical systems, interfaces, risks and threats: Identifying critical systems, interfaces, risks and threats for the business and managing the life cycle of the critical systems in a good fashion are critical for security and continuity of services. These activities must ensure that systems which are already at the end of their supported life cycle are in the priority list in investment plans.
- Build protection instructions: In cybersecurity studies, the most important threats for the system should be identified. Then, the most important operating methods that improve the protection against cybersecurity threats are devised to increase cybersecurity. The most important security practices include but not limited to secure communication architecture, secure remote connections, access rights management and disruption situation management and training.
- Develop contingency plans: The critical systems should have already developed plans to ensure predefined contingencies do not cause significant losses or disruption to the society functions. The plans can be based on providing enough spare for critical parts of the system.
- Recognize violations and react accordingly: The systems for identifying cybersecurity breaches are divided into two main types namely the systems that analyse network traffic and the systems that analyse terminal device events. However, in the energy sector, the systems cannot identify all attacks. In order to ensure cybersecurity, in

addition to the systems, suspicious contacts, emails, contacts on social media channels, phone calls, random conversations in public environments like airports as well as suspicious company visitors, sales representatives, subcontractors deputies and educational institution visitors should be observed carefully. In case a suspicious activity is identified, it is important to investigate the traces it leaves. To do so, logs should be recorded for subsequent analyses.

- Report and minimize damages: Documentation of events is necessary to learn from cybersecurity incidents which have already taken place in the past. It is also valuable to be familiar with previously carried out attacks regarding other companies. These help to know about the tools attackers have used and the traces they left.
- Restore normal operation: Once a cyber incident is revealed, having accurate information about the infected systems and the time they became contaminated is required for a fast restoration process. Having understanding about a clean normal state is also necessary. This includes but not limited to the software version information, installed patches, system settings and backup and recovery systems with instructions.

In addition to the cybersecurity management model, KYBER-ENE defined the most important tasks of developing and maintaining cybersecurity. The list of tasks helps in defining responsible parties for each task group. The following figure shows the work division model.



Owner of Production assets responsible

Security team assist

Management commit

Access control
Correct use of passwords
Control of remote access
Control of physical access
Start of investigation
Communication of violations

Production asset management
Production facility
Control room and systems
Electric networks systems
Remote use systems
Communication systems and networks

Design and development
Create Cybersecurity development team
Create year plan
Minimum requirements for cybersecurity
Evaluate solutions
Pilots and development projects

HR management
Define roles and responsibilities
Define tasks and resources
Training
Contract models
Develop knowledge

System management
Installations, changes and write-offs
Updates and fixes
Backup copies
Documentation
Architecture and network segmenting

Installing Cybersecurity
Create instructions and training
Create models and training
Describe correct operations
Describe reporting

Partnership management
Evaluate partners
Contracts of partnerships
Define responsibilities in partnership
Understand company policies
Follow up partnerships

Figure 7 Cybersecurity tasks

It is important to note that the above work division model is only to help companies in understanding the tasks of cybersecurity and in defining the responsible body.

4.2.1.2 Cooperation among energy companies

The limitations of technical cybersecurity solutions and emerging requirements due to new threats call for an effective cooperation between several different entities in the sector. The program recommends companies to network with each other to share confidential threat information within the community, generate and implement effective peer support, enable learning from pioneers, transfer best practices and share good and bad experiences.

In addition to the above topics, KYBER-ENE emphasizes on the importance of cybersecurity training of personnel. The trainings can show deficiencies in personnel or companies preparedness, develop threat and disturbance situation communication and showcase potential shortcomings within the company and in communication between companies.

In Finland, industry specific information exchange groups for information security issues (Information Sharing and Analysis Centre (ISAC)) are national cooperation bodies between organizations established for different sectors. The main purpose of the ISAC groups is to enable confidential handling of information security issues among the participants to develop information security expertise of the organizations. The ISAC group for energy sector is called EÿISAC. The group is an active information sharing forum where members exchange their good and bad experiences.

The size of typical ISAC groups is around 10 to 20 people/companies. If the size is increased larger than this, a lack of trust starts to become a problem. This can be due to the fact that sensitive information may easier spread outside the group from a larger group. However, there are hundreds of SME companies operating in energy sector in Finland. One idea to bring all of them into the cooperation process is to establish regional energy industry ISAC groups.

In addition to information sharing described in the above, a lot of internal and external communication and a good ability of cooperation are needed for effective incident management. The following figure shows a few possible cooperation targets for disturbance management for different actors.

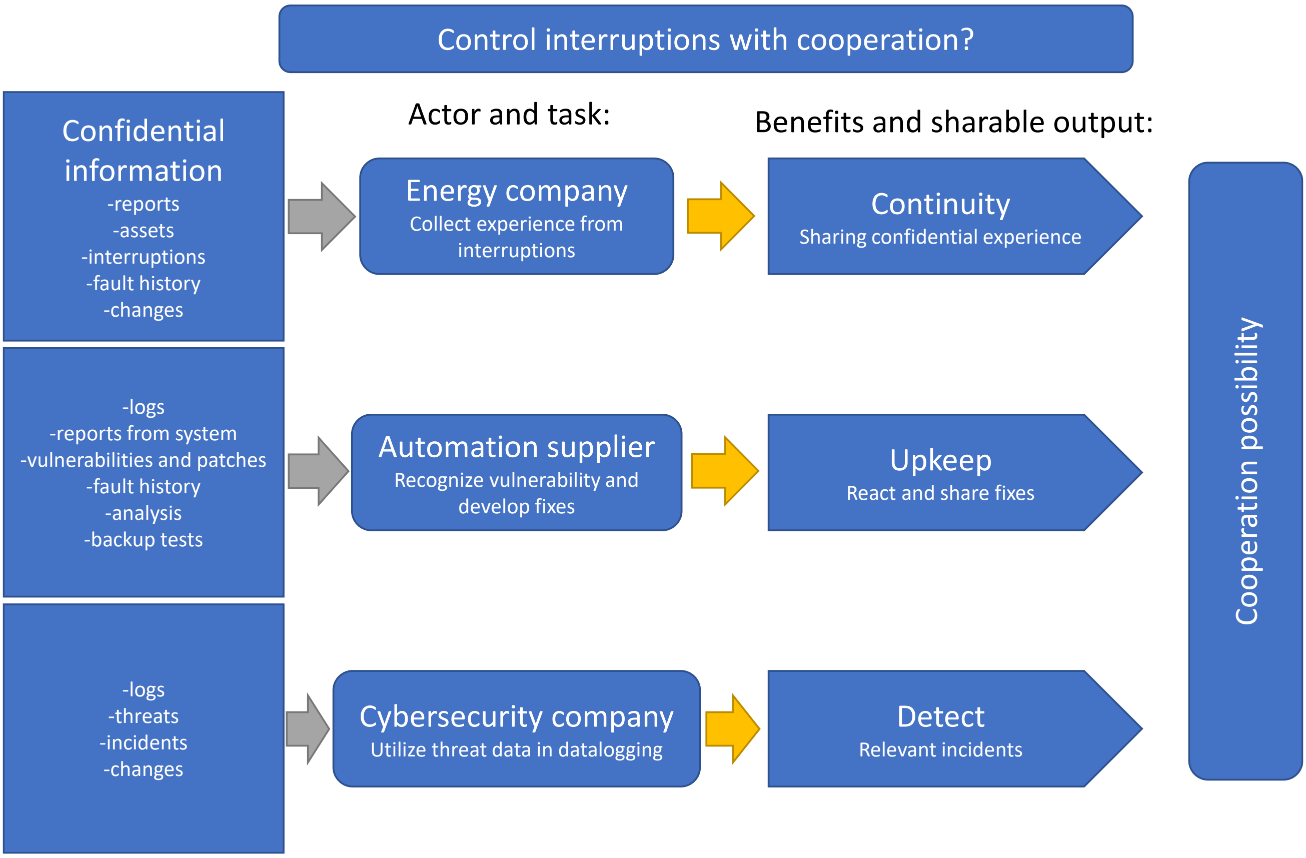


Figure 8 Interruption management cooperation targets for different operators

In the above figure, the energy company collects its required information through various channels such as supplier reports and asset stock and production disruption reports. The company can share the experience compiled from the information to its trusted community. If the other companies do similar, the entire community would gain very valuable experience for developing their cyber situational awareness and cybersecurity. Similarly, the automation supplier collects system log files to develop its processes to react to new threats faster. An information security company can use log and event information of energy companies and international threats to increase accuracy of cyber incident analyses as well as to create new measures for threat detection.

4.2.2 Finnish National Emergency Supply Agency (HVK)

The Finnish National Emergency Supply Agency (HVK) is an administrative institution of the Ministry of labour and economy. The mission of the institute is to plan and operate the maintenance and development of the activities regarding security of supply in the country. To HVK, security of supply refers to the ability to maintain the basic functionalities of the society. The basic functionalities are necessary to secure the population’s viability, functionality and safety as well as to secure the requirements of national defence in serious disturbances and emergency situations.

4.3 Estonia

Estonia's national regulatory framework for cybersecurity governance in the energy sector is built upon its broader cybersecurity governance model. The energy sector, being a critical part of the nation's infrastructure, is subject to various regulations and guidelines aimed at securing the operation of Electric Power and Energy Systems (EPES) and protecting the data involved in these systems.

The main organizations and policies involved in Estonia's cybersecurity governance for the energy sector are as follows:

- Ministry of Economic Affairs and Communications: This ministry oversees the development and implementation of national cybersecurity policies and strategies that are applicable to the energy sector, such as Estonia's Cyber Security Strategy.
- Estonian Information System Authority (EISA): EISA is responsible for managing and supervising information systems within the energy sector, ensuring the security of critical infrastructure, and coordinating incident response activities. EISA works closely with energy sector stakeholders to develop sector-specific guidelines and best practices for cybersecurity.
- National Cyber Security Centre (NCSC): Operating under EISA, the NCSC focuses on the protection of critical information infrastructure within the energy sector. It monitors and analyses potential cybersecurity threats and advises organizations on how to mitigate risks and ensure the security of their systems and data.
- Data Protection Inspectorate (DPI): The DPI ensures that personal data and privacy are protected within the energy sector, enforcing data protection laws and providing guidance on data protection issues.

Several national laws, regulations, and guidelines govern the cybersecurity of Estonia's energy sector, including:

- Cybersecurity Act: This act provides a legal framework for ensuring the security of Estonia's digital infrastructure, including the energy sector. It outlines the roles and responsibilities of various stakeholders, establishes security requirements for critical infrastructure, and defines the procedures for responding to cybersecurity incidents.
- Sector-specific guidelines: EISA and other relevant organizations develop and disseminate sector-specific guidelines for cybersecurity in the energy sector. These guidelines cover topics such as risk assessment, secure data exchange, incident response, and reporting to CERTs in case of incidents.

Estonia's cybersecurity governance model for the energy sector has demonstrated the following best practices and lessons learned:

- Public-Private Partnerships: Estonia's approach to cybersecurity in the energy sector emphasizes collaboration between the public and private sectors. This collaboration ensures that all stakeholders are engaged in the process of securing the nation's energy infrastructure and sharing best practices.
- International Cooperation: Estonia actively participates in international forums and organizations related to cybersecurity in the energy sector, such as the EU Agency for

Cybersecurity (ENISA) and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). This engagement enables Estonia to stay abreast of global developments and share its expertise with other countries.

- Continuous Improvement: Estonia is committed to continuously improving its cybersecurity governance model for the energy sector. This includes regular updates to its national strategies and policies, as well as ongoing efforts to develop and disseminate best practices and guidelines for the sector.

4.4 Slovenia

Information Security Act (ISA), which implements the EU NIS Directive, defines the Government Information Security Office (URSIV) as the Competent Authority for cybersecurity (Art. 27 of ISA), while on the operational-technical level, Art. 28 defines SI-CERT as the national CSIRT and in Art. 29 SIGOV-CERT as the governmental CSIRT. ISA defines obligatory reporting for governmental institutions and operators of essential services for more important incidents. Similar provisions in reporting to the national CSIRT are defined for operators of electronic communications in the Electronic Communications Act (version 2) while voluntary reporting in line with provisions of ISA is planned for additional entities in the renewed Personal Data Protection Act (version 2). SI-CERT is also tasked with providing the national awareness-raising program (varninainternetu.si).

National Cybersecurity Incident Response Plan defines details for reporting, such as the taxonomy for categorisation of incidents, definitions of severity levels, methods for determining the severity of incidents and reporting timeframes for obligatory reporting.

URSIV heads the Cybersecurity Coordination Body that includes other governmental bodies with operational responsibilities in this field: SIGOV-CERT and SI-CERT, the National Security Agency, Ministry of Defence, Police, and Ministry of Public Administration. URSIV is responsible for coordinating the revisions of the national Cybersecurity Strategy (current strategy was published in 2016).

4.5 Italy

Cybersecurity National Perimeter - DL 105/2019

In 2019, the Decree Law No. 105 (DL105) introduced the "**Perimetro di sicurezza nazionale cibernetica**", a group composed by 150 private and public entities, whose list is restricted, exercising essential functions or services of the State i.e. ensuring, among others, the continuity of the action of government and constitutional bodies and the internal and external security and defence of the State.

Entities included in the perimeter have obligations to:

- prepare and annually update the list of ICT assets necessary to perform the essential function or service;
- assess the impact of an incident on the ICT asset, indicating whether the incident may lead to the total interruption of the performance of the essential function or service;
- assess dependencies with other networks, information systems, IT services, or physical infrastructure pertaining to other entities; and

- notify security incidents impacting ICT assets of respective relevance, within one hour for the most serious and six hours for others, so as to activate the crisis management bodies.

Obligations on companies are subject to heavy fines (up to 1.8M€) and prohibitive penalties. Violating obligations related to the acquisition of ICT goods and services, for example, results in the inability for 3 years to assume top positions in legal entities and enterprises.

More recently, the adoption of Decree Law No. 82 of June 14, 2021 (DL82), redefined the Italian cyber architecture and established the "**Agenzia per la Cybersicurezza Nazionale**" (**ACN**) to protect national interests in cybersecurity.

The ACN is the national cybersecurity authority and it shall:

- ensure coordination among public actors involved in the matter;
- promote the implementation of joint actions aimed at ensuring the cybersecurity and cyber resilience necessary for the country's digital development;
- pursue the achievement of national and European strategic autonomy in the digital sector, in synergy with the national production system, as well as through the involvement of the university and research world;
- promote specific training paths for workforce development in the sector and supports awareness campaigns as well as a widespread culture of cybersecurity.

It is placed under the supervision of the "Presidenza del Consiglio", which has senior management and overall responsibility in the sector as well as the appointment of the director and deputy director. Internally, the agency is structured into 8 general services, which are in turn divided into divisions. Currently, the maximum planned staff is about 300 people while the budget for 2022 is 41 M€. However, for the coming years, a sharp increase in the resources allocated to this structure is expected: 122 M€ is the planned budget from 2026. For the purpose of carrying out the above functions, the following operate at the Agency:

- the Computer Security Incident Response Team Italia (CSIRT), whose action is aimed at preventing, monitoring, detecting, analysing and responding to cyber incidents.
- the "Centro di Valutazione e Certificazione Nazionale" (CVCN), which will be responsible for verifying the security and absence of known vulnerabilities in ICT assets, systems and services in use in the infrastructures on which the country's essential functions and services depend;
- the "Centro Nazionale di Coordinamento" on cybersecurity in industry, technology and research.

In particular, the ACN, while respecting the competencies attributed by current legislation to other administrations, operates as a regulatory, certifying, as well as supervisory body of the cybersecurity sector, defining, for example, the minimum levels of security measures in different areas (including energy), also being able to carry out inspections and impose sanctions.

In the same DL82, the "**Comitato interministeriale per la cybersicurezza**" (**CIC**) has been established under the Prime Minister's Office, it is a committee that brings together the director of the agency, who serves as secretary, the president of the council, who chairs it, the delegated authority, and the ministers of foreign affairs, interior, justice, defence, economy, economic development, ecological transition, university, digital transition, and infrastructure. The main objectives are advice, proposal and supervision on cybersecurity policies.

In detail, it proposes to the president of the council:

- the general directions to be pursued,
- high oversight of the implementation of the strategy, and
- the promotion of initiatives to foster collaboration, nationally and internationally, among the various institutional actors in the field

Furthermore, the DL82 established the "Nucleo per la cybersicurezza" as well. It operates at a more operational level. It is a permanent body, dealing with aspects related to prevention and preparedness for possible crisis situations. It is chaired by the agency director or deputy director and includes the military adviser to the council president, a representative from each of the intelligence agencies, civil defence and each of the ministries in the CIC.

4.6 Greece

In Greece, three authorities are mainly involved in cybersecurity governance. The National Cybersecurity Authority (NCSA) is under the General Secretariat of Telecommunications & Posts of the Ministry of Digital Governance. The Ministry of Digital Governance brings together all the Information Technology and Telecommunications structures related to the provision of digital services to citizens and businesses in Greece. According to Greek National Law 4577/2018 (Official Government, 2018), the NCSA, acts as the National Competent Authority for cybersecurity in Greece. The NCSA a) prepares the National Cybersecurity Strategy which defines the strategic objectives, priorities, policy and regulatory measures, b) collaborates with the relevant CSIRTs and other actors to ensure a high level of security for networks and information systems, c) assesses the technical and organizational measures implemented by Operators of Essential Services (OES) and other entities, c) handles critical incidents, issuing binding instructions and imposing corrective actions and penalties.

The National CERT (National Authority against Cyber Attacks), is under the National Intelligence Service and supports public agencies in preventing, early warning and countering cyber-attacks. As per Greek legislation, the NCERT-GR's constituency consists of the Greek public operators that do not fall under the jurisdiction of the Hellenic National Defense General Staff (HNDGS) Cyber Defense Directorate (GR-CSIRT). Specifically, NCERT-GR supports the public sector, except for the Ministry of National Defense, in the early warning, prevention and responding to cyberattacks.

The Hellenic Computer Security Incident Response Team, under the National Defense General Staff (NDGS), focuses on cyber defence, incident response, and operational integration for the Ministry of Defense. It also caters for Operators of Essential Services – OES (NIS directive). *The CSIRT is responsible for receiving the cybersecurity incident reports for the public and private sector*.

Strategy –Best practices – Reporting

In terms of strategy, policy and best practices, the Cybersecurity strategy (available in Greek), a cybersecurity self-assessment tool (available in Greek) and the Cybersecurity Handbook (available also in English) are provided by the NCIA. The handbook addresses a) the information security and IT organizational units of ministries, public administration entities, and of private sector enterprises, b) the Chief Information Security Officers (CISOs), Data

Protection Officers (DPOs), as well as other executives who deal with the cybersecurity of network and information systems of public and private sector organizations. NCERT-GR also provides a set of best practices and info on threats (including malicious software and cyberattacks).

4.7 Germany

The Federal Ministry of Interior and Community (BMI) is a responsible entity in matters of internal security in Germany, including the drafting, implementation and execution of the Cybersecurity Strategy of the nation.

In terms of incident response, the Cybersecurity Strategy for Germany in 2016 aimed at improving CERTs and increasing the defence capabilities of the nation. The IT-Security-Act 2.0 (ITSiG2.0) introduced in 2021 puts the Federal Office for Information Security (BSI) at the centre of the government's agenda for cybersecurity, with extended responsibilities and aiming at the reduction in the complexity of the Governance Model. One of the most important responsibilities of the BSI is shown in Art.5 of the BSI Law (BSIG), stating that it is its main duty to protect federal Information and Communication Technology against threats. The BSI is the main role in detection and defence, cyber security in mobile communications networks, consumer protection, security for companies and the national authority for cybersecurity certification.

The most important cyber-defence units of the BSI are:

- National Cyber Defence Centre: A Platform for information sharing about cyber threats and effort synchronisation to prevent and counter cyber-attacks.
- Alliance for Cybersecurity: A platform in which private companies and the BSI meet in order to raise awareness, share knowledge, and gather up-to-date information about the extremely dynamic threat landscape.
- CERT-Bund: Federal Computer Emergency Response Team, responsible for creating best practices for damage prevention, sharing information about security vulnerabilities, and publishing recommendations.
- IT-Situation Centre (Nationales IT-Lagezentrum): Coordinate the response in case of a cybersecurity incident.

Based on Special regulation obligation, energy companies need to report IT problems to the BSI [29]. To protect against threats to telecommunications and electronic data processing systems, which are necessary for secure network operation, these minimum standards are included in the so-called "IT security catalogues":

- IT security catalogue for operators of electricity and gas networks (published in August 2015) [30]
- IT security catalogue for operators of energy systems that have been designated as critical infrastructure according to the BSI Critical Ordinance and are connected to an energy supply network (published in December 2018) [31]

The IT security catalogues are based on the ISO standards 27001, 27002 and 27019. The catalogues include categorising critical infrastructures by importance, IT security guidelines for power plants, legally required security minimum for communication and data processing systems regarding electricity and gas network infrastructure, and data confidentially requirements.

Moreover, on April 2021, BSI officially recognised version 1.1 [32] of the industry-specific IT security standard for "Systems for controlling/bundling electrical power" (B3S) developed by BDEW, a collaboration of multiple energy companies. B3S define what the BSI considers state-of-the-art IT Security techniques. Currently, this standard is in use by operators of critical infrastructures (KRITIS) as proof of the guarantee of the IT security requirements.

4.8 Romania

The Cybersecurity governance in Romania is an evolving process in continuous development. The process is based on a strategy described in a document approved by the Romanian government on 30th December 2021 named "The Cyber Security Strategy of Romania, for the period 2022-2027, as well as the Action Plan for the implementation of the Cyber Security Strategy of Romania, for the period 2022-2027" [33].

This document establishes the guidelines for strengthening the capacity of Romanian governance system to fight the cybersecurity threats.

The context declared in the document is highlining some important changes that defines this strategy.

- The continuous development of information and communication technologies and the increasingly high level of interconnectivity and interoperability between systems contribute significantly to changing the perception of risks, vulnerabilities and threats from cyberspace.
- Cyber-attacks are in a continuous evolution, both in terms of the number and the complexity of the specific methods used. They target a large number and variety of networks and computer systems, from those that serve individuals, authorities and institutions of the public administration or private entities, to those that serve entities whose activity is part of the national security equation.
- Cyber-attacks, especially on essential services or critical infrastructures, can, thanks to the interconnectivity, have an impact on the services provided at a regional or international level, with regional or international destabilizing effects, 1 on an economic and social level, and with potential repercussions on the address of peace and stability.
- A safe cyberspace is both the responsibility of the state, through the competent authorities, and of the private sector and civil society. The consolidation of partnerships 1 between the authorities and institutions of the public administration and civil society, respectively the private environment, as well as those 1 between states and international organizations is an essential point to reach 1 in obtaining a global, open and safe cyber space.
- The accelerated development of technologies and the lack of standards and regulations that require manufacturers to implement the concept of their integrated security translate into a precarious level of cybersecurity and into an increased interest of cyber attackers. The cybersecurity of technologies has thus become an aspect of strategic importance.

In this context also a very important element the hosting in Bucharest of the European Industrial, Technological and Research Competence Centre in cybersecurity will have an important role in connecting the relevant actors from the public level with those from research and industry.

The objectives declared by the document are:

a. Developing resilient and secure networks and ITC systems
b. Consolidating the regulatory frame and institutional frame
c. Defining a pragmatic public-private partnership on cybersecurity
d. Increasing the resilience by proactive approach and discouragement
e. Romania to become a relevant actor in international cooperation architecture.

The main actor for Romanian Cybersecurity governance is the National Cyber Security system.

The National Cyber Security System - SNSC represents the cooperation framework that brings together authorities and public institutions, the academic and business environment, professional associations, non-governmental organizations, with responsibilities and capabilities in the field, in order to coordinate actions to ensure the security of the national component of cyberspace.

The coordination of the activity of the National Cyber Security System is ensured by a committee, having as its objectives the implementation of the National Program in the field, the management of actions, at the national level, in the event of a cyber-attack, respectively the correlation of the actions of the component institutions within the international cooperation formats to which Romania is a member part.

One main actor from the SNSC is DNSC.

DNSC is the Romanian national cybersecurity and incident response team, The National Directorate for Cyber Security. DNSC is operating in Romania based on NIS directive.

The DNSC is operating also the CERT-RO that is using several national and regional CSIRT across Romanian territory.

The main critical infrastructure owners and operators also are interconnected and part of cybersecurity topic with SNSC.

Transelectrica is the national and is developing his own strategy for the cybersecurity topic transmission operator. The strategy is based on a set of procedures covering the main aspects on cyber threats.

- Procedures for response to cybersecurity incidents
- Procedures for cybersecurity vulnerabilities management
- Procedures for communication and cooperation

For the Cybersecurity governance aspect, the most important is the collaboration and cooperation with the other parts of SNSC. In this case the communication and cooperation procedure from Transelectrica states that the main objectives are:

- **Maintaining contact with national authorities**
    - The Information Security Manager acts as the single point of contact (SPOC) for all information security issues in the relationship between C.N.T.E.E. "Transelectrica" S.A. and ENTSO-E.
    - The Information Security Manager is in contact with national authorities (e.g. the National Cyber Security Directorate) so that they can advise ENTSO-E on national laws and regulations that may impact the Security Plan and OPDE services.
- **Maintaining contact with special interest groups or other specialized security forums and professional associations**
    - The Information Security Manager follows the decisions taken by the ENTSO-E special interest groups (e.g. the Cybersecurity Special Interest Group) on information security topics and the ENTSO-E IT strategy.
    - The Information Security Manager also maintains appropriate contacts with special interest groups or other specialized security forums and professional associations (by joining or subscribing to them).
    - The Information Security Manager analyses, together with the persons designated for the roles in PSMVS (Access Control Manager, IT Resource Manager, Network Manager, Crypto Custodian, Data Custodian) the received information. The Information Security Manager communicates with the organization's Management the information that may have an impact on the MVS Security Plan and the OPDE services, in order to establish the position that will be adopted by C.N.T.E.E. "Transelectrica" S.A. vis-à-vis this information.

In conclusion in Romania the success of the activities carried out in the SNSC essentially depends on the cooperation, including in public-private partnership formulas, between the owners of the cyber infrastructures and the state authorities empowered to undertake measures to prevent, counter, investigate and eliminate the effects of a threat materialized through an attack.

The success of the approach depends, essentially, on the efficiency of cooperation at the national level to protect the cyberspace, respectively on the coordination of national approaches with the guidelines and measures adopted at the international level, in the cooperation formats to which Romania is a part.

The measures intended for the operationalization of the National Cyber Security System must be harmonized with the efforts on the dimension of the protection of critical infrastructures, respectively with the evolution of the development process of CERT-type capabilities. In the optimal version, the SNSC must have a flexible, adaptive structure that includes identification and anticipation capabilities, resources and operational procedures for prevention, reaction and countermeasures and tools for documenting and sanctioning the authors of cyber attacks.

5 Best practices and lessons learned

In this chapter, the information gathered in chapters 3 and 4 is studied and the best and worst practices and the lessons learned are reported. According to the gathered information, recommendations and policies relevant for cybersecurity governance can be categorized as in the following:

Policy Development: Defining and documenting policies and procedures that establish clear guidelines for how employees/organizations should handle data and systems are critical. In addition, it is necessary to define types of data and systems. In the process, it is very important to ensure that the cybersecurity governance is aligned with the organizations objectives. As an example, strategic alignment of information security with the organization objectives is one of the governance goals in Elektrilevi. In line with this, it is worthwhile to note that the main objectives of EECDS are to enhance the flow of energy data across the EU, improve energy market efficiency, increase transparency and facilitate the integration of renewable energy sources and energy efficiency measures. These objectives beside the role of different stakeholders and their data can be an input for developing the policies, standards and guidelines. The "Network Code for cybersecurity aspects of cross-border electricity flows" developed by ENTSO-E and EU-DSO, besides its main goal, can be considered as an attempt toward this. It is important to consider that different stakeholders need different security standards since impact of their security on the overall system security differs. So, possibility of having different standards for different stakeholders should be considered.

Risk Management: Assessing and managing cyber risks, including identifying and prioritizing threats and vulnerabilities, implementing controls to mitigate risk and monitoring the effectiveness of those controls are all very important. The risk management model proposed by KYBER-ENE in Finland is a good example for representing different elements in a risk management model. The elements are listed in the following:

- Identification and commitment of responsible and support personnel for cybersecurity development
- Development of forums for sharing cybersecurity materials such as development plans, instructions and potential risks
- Studying cybersecurity holes and weaknesses
- Identifying and mapping critical systems, interfaces, risks and threats
- Building protection instructions
- Development of contingency plans
- Recognition and reaction to potential violations or suspicious actions
- Documentation of events and learning from them
- Understanding normal operation and means for restoring normal operation after an incident.

Finally, it is worthwhile to mention that an effective risk management framework should include processes for risk identification, risk assessment, risk treatment and risk monitoring.

Compliance Management: Compliance with relevant cybersecurity standards and regulations should be regularly audited to ensure the common data space is operating in a secure and compliant manner. To do so, compliance management needs to list the relevant standards and conduct internal and/or external audits. An effective cybersecurity governance model should clearly define the necessary standards for different stakeholders as well as timeframe and type of audits to check compliance with the standards.

Incident Response Plan: Having a well-defined incident response plan that outlines the steps to be taken in the event of a cybersecurity incident, including reporting, investigation and recovery is vital. In Slovenia, National Cybersecurity Incident Response Plan defines details for reporting incidents including incident categorization, incident severity and the relevant evaluation method and reporting timeframes. In cooperative environment such as energy common data spaces, predeveloped incident response plans are even more important since cooperation between several stakeholders specially during incidents without clear plans is much more difficult than in an organization.

Awareness and Training: Providing regular training and awareness to people to help them understand their role in protecting the organization's information systems and data is crucial. This can be considered as training and awareness of different stakeholders in a multi-stakeholder environment, like an energy common data space. As an example, KYBER-ENE program has the aim to develop and maintain level of competence of different players in the energy sector in Finland. Since different organizations have different roles and responsibilities and thus they can be prone to different risks, it is necessary to cluster the organizations and consider awareness and training programs for each cluster. Formation of forums and sharing good and bad experiences in the forums can be considered as an awareness and training activity. In line with this, it is important to know that more effective information sharing can be achieved in smaller forums according to the lessons learned from KYBER-ENE program in Finland. So, clustering organizations and forming different forums for each cluster can be a solution. Another solution can be formation of forums for different risk types.

Continuous Review: Reviewing the performance of the governance model, including reviewing policies, procedures and controls, to ensure that they remain effective and relevant is very important. The review can enhance the model by learning from incidents and vulnerabilities. This includes conducting post-incident reviews, updating policies and procedures, and adjusting technical controls as necessary. To do so, it is the best to define a performance measurement index and monitor that too. In Elektrilevi, performance measurement including defining, reporting and using information security governance metrics is one of the governance goals. As another example, in cybersecurity network code, ENTSO-E and EU-DSO are responsible for defining electricity cybersecurity risk index (ECRI) to determine when enterprises are classified as high risk or critical risk entities.

Stakeholders Alignment: It is worthwhile to mention that harmonization of cybersecurity approaches of different stakeholders in systems including more than one player is crucial. This importance comes from the fact that different stakeholders may have different cybersecurity approaches and strategies. For the European energy common data space, a European standard for the cybersecurity is necessary. As a relevant example, the “Network Code for Cybersecurity Aspects of Cross-border Electricity Flows” by ENTSO-E and EU_DSO is an activity toward this harmonization in the cybersecurity approaches of different TSOs.

Preventive activities: In any cybersecurity governance, a special emphasize must be dedicated to preventive activities such as monitoring and logging, access control and data encryption. Monitoring and logging of access and activity on the common data space can help identify and respond to any potential security incidents. This includes tracking user access and activity, as well as system logs and network traffic. Access to the CEDS should be tightly controlled to prevent unauthorized access. This can include using strong authentication methods such as multi-factor authentication and role-based access control to restrict access based on the user's role and responsibilities. Data transmitted over the CEDS should be encrypted to protect it from interception and unauthorized access. Encryption can be implemented using industry-standard protocols such as SSL/TLS.

Reporting Mechanisms: Establishing reporting mechanisms for security incidents and vulnerabilities is necessary. This includes a clear process for reporting incidents, a system for tracking incidents and vulnerabilities and a way to report incidents to the appropriate authorities. More information about reporting mechanisms can be found in CyberSEAS project deliverable D6.7.

The above guidelines can help establishing a more robust cybersecurity governance model that helps protecting against cyber threats.

6 Common cybersecurity governance model and compatibility with NIS 2 directive (New)

This Chapter is based on analysis and lessons learned from the previous Chapters. Additional analysis is made of the Network and Information Security 2 (NIS 2) directive, which has a key role in cybersecurity governance model for organizations, not just in energy sector, but in every essential and important sector introduced in the NIS 2 directive.

The main objective of this Chapter is to create a common cybersecurity governance model, which can be utilized by every organization. This governance model is compliant with the NIS 2 directive and addresses its obligatory features. Some of these items are discussed more deeply in other CyberSEAS work package 6 deliverables such as D6.4 Secure and privacy preserving data exchange among operators, D6.6 Data breach management plan, and D6.8 Rules and tools for operators' coordination and reporting to CERTs, which are cited accordingly.

Objectives:

- Help organizations to create a cybersecurity governance model.
- To understand background of NIS 2 directive and its obligatory features.
- To be compliant with NIS 2.
- To prepare for NIS 2.

6.1 The Network and Information Security 2 (NIS 2) Directive

6.1.1 NIS 2 Directive explained

In the EU legislation portal, the new directive is: "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." [34]

The Network and Information Security (NIS 2) Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The new legislation will take effect in October 2024, raising the collective resilience of European critical infrastructure by enforcing ten broad security requirements, see table 2. This new NIS 2 directive will replace the original NIS directive, see Section 6.1.2.

NIS 2 affects all entities that provide essential or important services to the European economy and society, including companies and suppliers. All medium and large-sized companies in selected sectors will be included in the scope, see expanded sectors in Section 6.1.2.

In principle, the NIS 2 directive aims to achieve following goals:

- Require national governments to pay due attention to cybersecurity.
- Strengthen European cooperation among cybersecurity authorities.

- Require the main operators in key industries of our society to take security measures and report incidents.

Member States must efficiently ensure that entities in the scope of NIS 2 take the necessary measures and report incidents. To do this, they may, for example, conduct regular external audits or inspections, or request certain documentation. The governing bodies or executives of essential and important entities must approve cybersecurity risk management measures, and oversee their implementation, and may be held liable for any breaches. Additionally, financial penalties to businesses can be harsh, up to 2% of global revenue.

In table 2 below are all the cybersecurity risk-management measures given in the NIS 2 directive with brief explanations. Organizations should take actions on each of the items where applicable. The first row on each item represents the directive's expression followed by a brief explanation giving readers a more comprehensive understanding.

Table 2 Cybersecurity risk-management measures in NIS 2 [34]

a)	policies on risk analysis and information system security;
	Implement risk assessments and **security policies** for information systems. Risk management and risk assessment are major components of information security or cybersecurity. Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. [35]
b)	incident handling;
	Plan for handling security incidents. See incident response plan in *D6.6 Data breach management plan*. Entities must report any significant incident without delay to the national authorities including the national CSIRT. More about the incident reporting to CSIRTs can be found in *D6.8 Rules and tools for operators' coordination and reporting to CERTS*.
c)	business continuity, such as backup management and disaster recovery, and crisis management;
	Plan for managing business operations during and after a security incident. Cyber-attack is not the only possible incident as other incidents such as IT outages, public health crises (COVID-19), physical security threats, and other supply chain disruptions can have similar effects on business continuity. Typical risk mitigations are data backups and system backups. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident. The goal of preparation is to minimize the effects of outages and disruptions on business operations.
d)	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
	Implement security around supply chains and conduct due diligence of third party suppliers and service providers. Supply chain security focuses on identifying and

	managing security risks associated with external vendors, and suppliers. Companies must assess the overall security level for all suppliers and take security measures that cover the vulnerabilities related to each supplier. In the EPES domain, operators must understand cyber-physical nature of the systems and devices regarding physical energy generation, transmission, and consumption.
e)	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
	Implement security around the procurement of network and information systems, and system development and maintenance. Cybersecurity must be covered for the whole lifecycle of the products and provide security updates during that period. Manufacturers must disclosure any vulnerabilities and provide resolution for the customers.
f)	policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
	Create policies and **procedures** for evaluating the effectiveness of security measures. In step a) cybersecurity risks are analysed and identified. This is a follow-up activity to performing a security risk assessment and mitigating security risks. It includes the evaluation of both technical controls (such as access management and firewalls) and administrative controls (including policies and procedures). Step 1: Document security control implementation; Step 2: Monitor and verify security controls; Step 3: Report your test results. [36]
g)	basic cyber hygiene practices and cybersecurity training;
	Provide cybersecurity training and **practice** for basic computer hygiene. Cybersecurity training must be provided throughout the organization to protect against the most probable attacks. In cybersecurity, human factors are usually the weakest link in security. Basic computer hygiene includes practices e.g. on how the computer, devices, and software are used. The main goal of cyber hygiene is to keep sensitive data secure and protected from cyberattacks and theft.
h)	policies and procedures regarding the use of cryptography and, where appropriate, encryption;
	Create policies and **procedures** for the use of cryptography and, when relevant, encryption. Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. Encryption is a process of converting data from plain text to a form that is not readable to unauthorized parties, known as cipher-text. Cryptographic controls can be used to achieve different information security objectives, such as: Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted. Integrity/authenticity: using digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information.

	Non-repudiation: using cryptographic techniques to provide evidence of the occurrence of an event or action. Authentication: using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities, and resources.
i)	human resources security, access control policies and asset management;
	Create security procedures for employees with access to sensitive or important data, including policies for data access. Access control is the process of regulating which users can access certain resources and data or perform specific actions in an organization's environment. Organizations must also have an overview of all relevant assets and ensure that they are properly utilized and handled. Identify the resources (data, systems, and applications) that need to be protected. Classify assets based on their importance and sensitivity. Determine the potential impact of unauthorized access to these resources. This will help to determine the appropriate level of access control. Decide who is given access to which resources, and under which conditions. Human Resources Security focuses on safeguarding organization's data and resources by managing the human factors associated with security risks. It refers to a series of policies, procedures, and practices used to ensure that everyone employed by or associated with an organization is trustworthy, adequately trained, and aware of their responsibilities regarding information security. These policies and practices include pre-employment screening, employee training and awareness, contractor, and Third-Party Management, and also the employee exit process. [37]
j)	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
	Implement use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate. If there is a possibility of cyber breach attack utilizing weaknesses in accessing systems, organizations must use more rigorous access control such as multi-factor authentication. Organizations need to assess which users, access methods, and assets should have multi-factor authentication.

6.1.2 From NIS to NIS 2 Directive

Directive (EU) 2016/1148 was the original NIS directive and it came to force in 2016. The NIS 2 directive is built upon the original regulation and will replace it in 2024. The NIS was the first legislative measure at European level aiming to enhance cooperation between Member States and to create a first level of harmonization in the field of cybersecurity. NIS was a result of EU legislators being worried about the insufficient cyber resilience of businesses, lack of joint responses among Member States and businesses, and insufficient understanding of threats and challenges.

NIS was applied only for the essential sectors such as energy, finance, transportation, and health sectors, etc. However, NIS 2 will expand the scope considerably. [38]

The scope of the original NIS: Energy, Health, Transportation, Drinking water, Banking, Digital infrastructure, Financial market infrastructure, Digital service providers.

The additional scope of the NIS 2: Food, Waste water, Manufacturing, Waste management, Postal & courier, Public administration, Providers of public electronic communications network or services, Space, Research, ICT service management, and Chemicals. [39]

In summary, NIS 2 builds upon NIS 1 by addressing emerging threats, harmonizing requirements, and expanding its reach to safeguard critical services and systems across the EU.

6.1.3 NIS 2 Directive in Operational Technology (OT) environment

Operational Technology (OT) cybersecurity is a key component of protecting the uptime, security and safety of industrial environments, and critical infrastructure. In the domain of EPES, operators focus on OT cybersecurity to safeguard operating technology assets, systems, and processes from cyberattacks and comply with strict regulatory requirements, such as NIS 2.

In the webinar "*Unpacking Cyber-Resilience for EPES with NIS2*" [40] held by the CyberSEAS consortium in March 2024, challenges of cybersecurity in operational technology environment and compliance with NIS 2 were discussed. In this section, main points of the webinar are presented, which are relevant to the topic and support formulating governance model for businesses and organizations. [41]

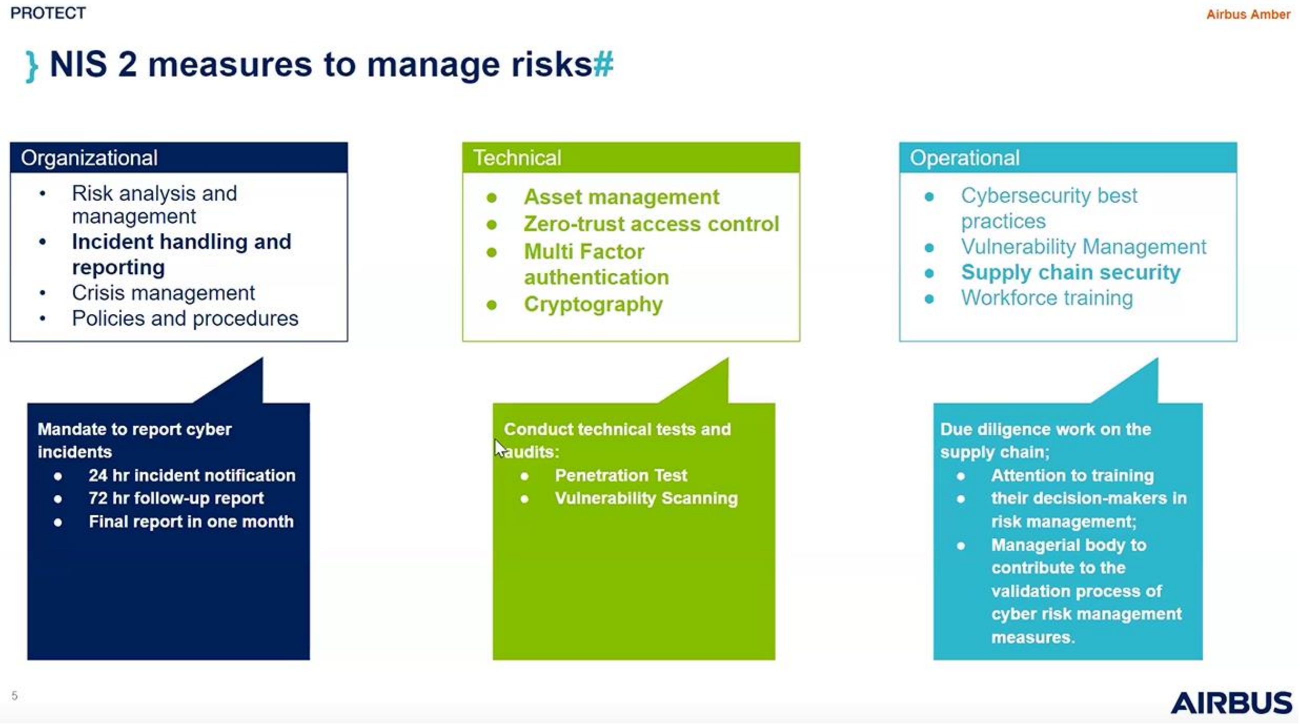
In the webinar, Anna Alfiero from Airbus discussed NIS 2 measures to manage risks, managing cyber risks in OT, and how to be compliant with NIS 2 from the risk management perspective.

In Figure 9, three different risk management perspectives are presented.

At **Organizational** level, risk analysis, risk management, incident handling and reporting, crisis management, and policies and procedures are performed. In NIS 2, a mandate of reporting is obligatory: notification no longer than 24 hr since the incident, follow-up report no longer than 72 hr after the incident, and final report in one month after the incident.

At **Technical** level, asset management, zero-trust access control, multi-factor authentication, and cryptography are performed. Technical tests and audits such as penetration test and vulnerability scanning can be done to validate protection and prepare for incident.

At **Operational** level, cybersecurity best practices, vulnerability management, supply chain security, and workforce training are performed. Due diligence work on the supply chain is performed on the operational level in which training, decision-makers in risk management, and managerial body role in validation process of cyber risk management are evaluated.



PROTECT

Airbus Amber

} NIS 2 measures to manage risks#

Organizational

- Risk analysis and management
- **Incident handling and reporting**
- Crisis management
- Policies and procedures

Technical

- **Asset management**
- **Zero-trust access control**
- **Multi Factor authentication**
- **Cryptography**

Operational

- Cybersecurity best practices
- Vulnerability Management
- **Supply chain security**
- Workforce training

Mandate to report cyber incidents

- **24 hr incident notification**
- **72 hr follow-up report**
- **Final report in one month**

Conduct technical tests and audits:

- **Penetration Test**
- **Vulnerability Scanning**

Due diligence work on the supply chain;

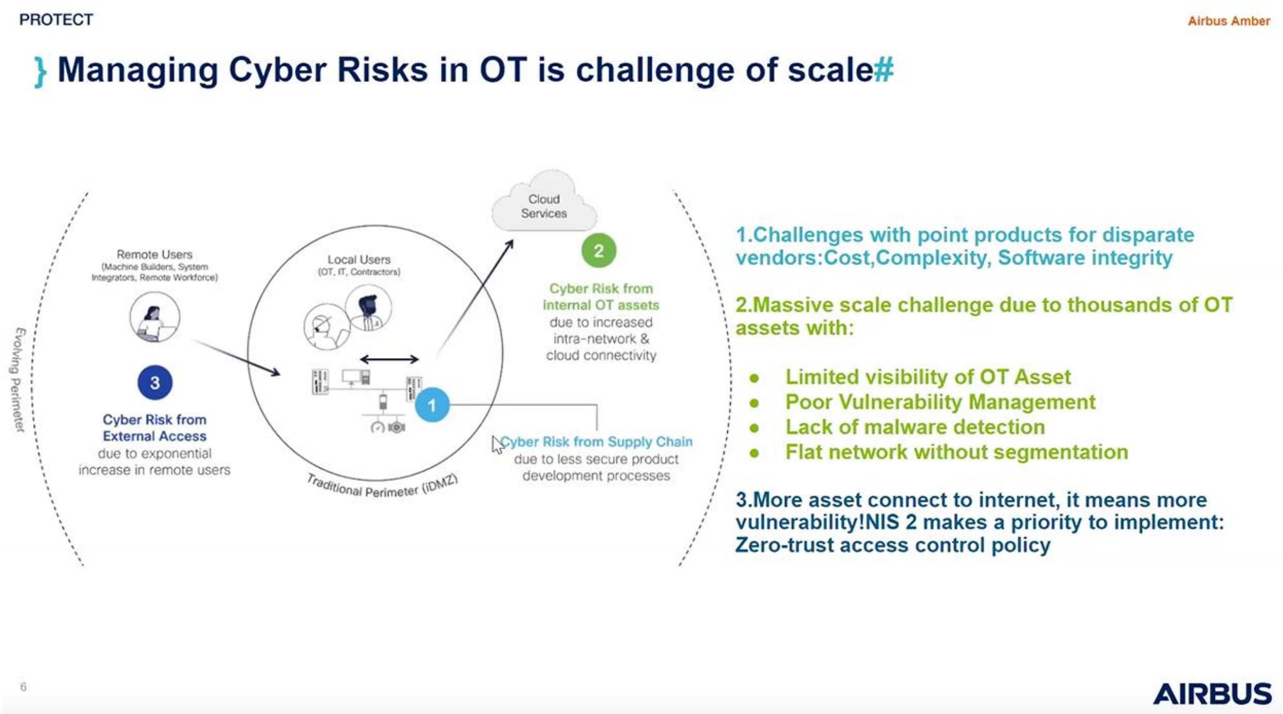
- **Attention to training their decision-makers in risk management;**
- **Managerial body to contribute to the validation process of cyber risk management measures.**

5

AIRBUS

Figure 9 NIS 2 measures to manage risks, Anna Alfiero, Airbus

In complex OT environment, cyber risks are related to three main areas: cyber risk from supply chain, cyber risk from internal OT assets, and cyber risk from external access. See Figure 10. The challenge with supply chain is that all the vendors need to have similar level of cyber security, up to date security updates, and secure communication between systems. Thousands of OT assets cause risks due to limited visibility to assets, poor vulnerability management, lack of malware detection, and possibility of poor network segmentation. Today, most systems are connected remotely, thus providing potential breach easier. Furthermore, access is granted to many 3rd parties, thereby human factors play larger role and access control must be implemented. More connected assets mean more vulnerabilities.



PROTECT

Airbus Amber

} Managing Cyber Risks in OT is challenge of scale#

Cloud Services
Remote Users
(Machine Builders, System Integrators, Remote Workforce)
Local Users
(OT, IT, Contractors)
Evolving Perimeter
3
Cyber Risk from External Access
due to exponential increase in remote users
2
Cyber Risk from internal OT assets
due to increased intra-network & cloud connectivity
1
Cyber Risk from Supply Chain
due to less secure product development processes
Traditional Perimeter (iDMZ)

1.Challenges with point products for disparate vendors:Cost,Complexity, Software integrity

2.Massive scale challenge due to thousands of OT assets with:

- Limited visibility of OT Asset
- Poor Vulnerability Management
- Lack of malware detection
- Flat network without segmentation

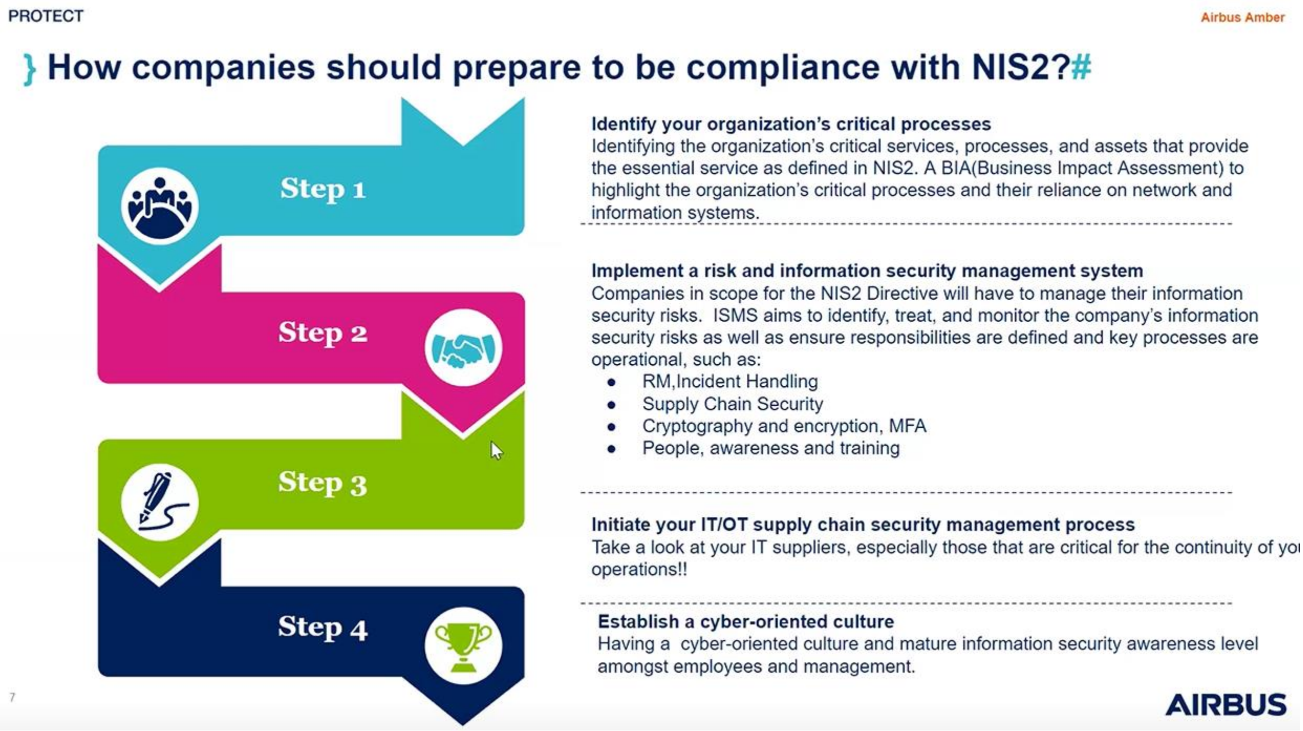
3.More asset connect to internet, it means more vulnerability!NIS 2 makes a priority to implement: Zero-trust access control policy

6

AIRBUS

Figure 10 Managing Cyber Risks in OT, Anna Alfiero, Airbus

In Figure 11, a preparation plan is shown for companies to be compliant with NIS 2. This includes four steps: 1) Identify your organization's critical processes; 2) Implement a risk and information security management system; 3) Initiate your IT/OT supply chain security management process; 4) Establish a cyber-oriented culture. These four steps are expanded in the next Section 6.2.



PROTECT

Airbus Amber

} How companies should prepare to be compliance with NIS2?#

Identify your organization's critical processes
Identifying the organization's critical services, processes, and assets that provide the essential service as defined in NIS2. A BIA(Business Impact Assessment) to highlight the organization's critical processes and their reliance on network and information systems.

Implement a risk and information security management system
Companies in scope for the NIS2 Directive will have to manage their information security risks. ISMS aims to identify, treat, and monitor the company's information security risks as well as ensure responsibilities are defined and key processes are operational, such as:

- RM,Incident Handling
- Supply Chain Security
- Cryptography and encryption, MFA
- People, awareness and training

Initiate your IT/OT supply chain security management process
Take a look at your IT suppliers, especially those that are critical for the continuity of yo operations!!

Establish a cyber-oriented culture
Having a cyber-oriented culture and mature information security awareness level amongst employees and management.

7

AIRBUS

Figure 11 How companies should prepare to be compliance with NIS 2, Anna Alfiero, Airbus

Charukeshi Joglekar from Fraunhofer institute discussed NIS 2 from the perspective of low-carbon energy transition in Europe and its key enablers. Energy transition in Europe is due to centralized energy system becoming more decentralized by consumers turning to prosumers and having a more active role in the system. This has created new market roles and new business models, in which digitalization is a key enabler. Examples of digitalization are smart sensors, meters, IoT devices, big data, and AI. In the energy sector, challenges are convergence of IT, OT, and IoT, legacy technologies and ICS vulnerabilities, highly interconnected actors and stakeholders, and different levels of readiness and cyber hygiene. **Cybersecurity is a key enabler** to build consumer confidence and trust in energy products and services, thus enabling energy transition. In Figure 12 is shown energy transition, which is powered by innovations.

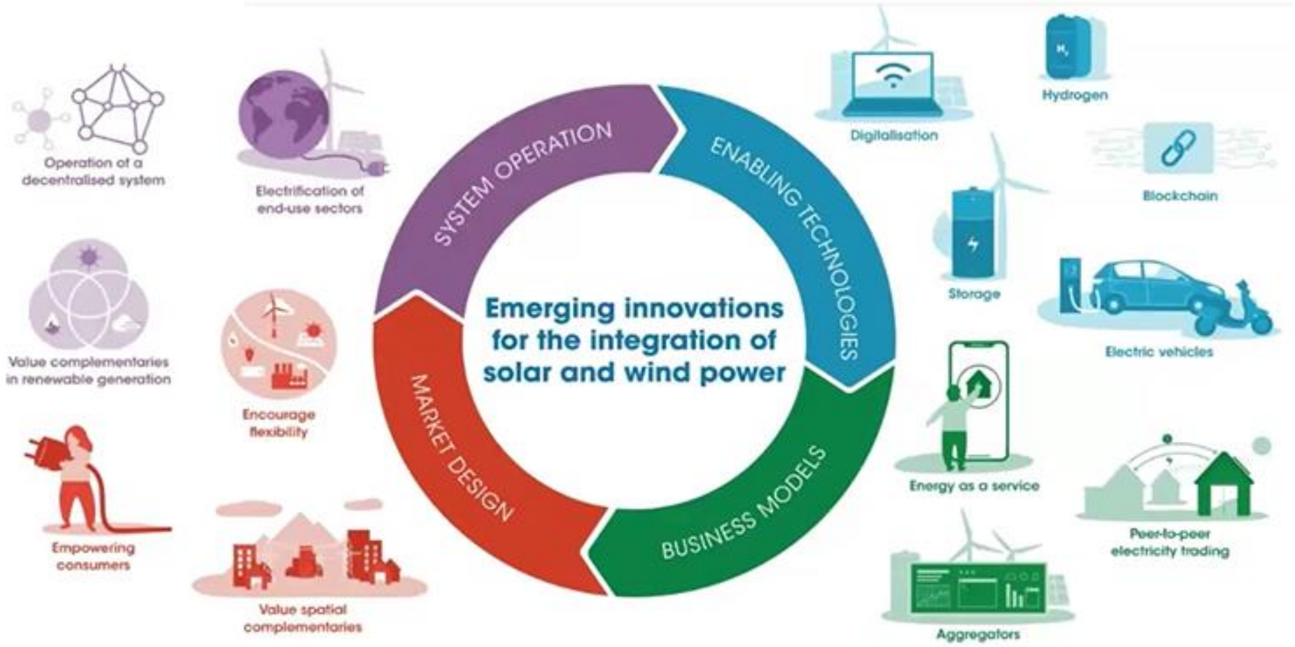

Emerging innovations for the integration of solar and wind power
SYSTEM OPERATION
ENABLING TECHNOLOGIES
BUSINESS MODELS
MARKET DESIGN
Operation of a decentralised system
Electrification of end-use sectors
Value complementaries in renewable generation
Encourage flexibility
Empowering consumers
Value spatial complementaries
Digitalisation
Hydrogen
Blockchain
Storage
Electric vehicles
Energy as a service
Peer-to-peer electricity trading
Aggregators

Figure 12 Energy transition powered by emerging innovations, source: IRENA, World Economic Forum

6.2 Description of Common governance model

In this section, a common cybersecurity governance model for organizations is formed by using previous research and lessons learned. This model is compliant with NIS 2 directive and will give a good understanding of main tasks related to cybersecurity. This model consists of four main steps an organization has to take with consequent tasks. The main steps are: Create a Team, Policy Development, Preventative Activities, and Incident Response, see Figure 13.

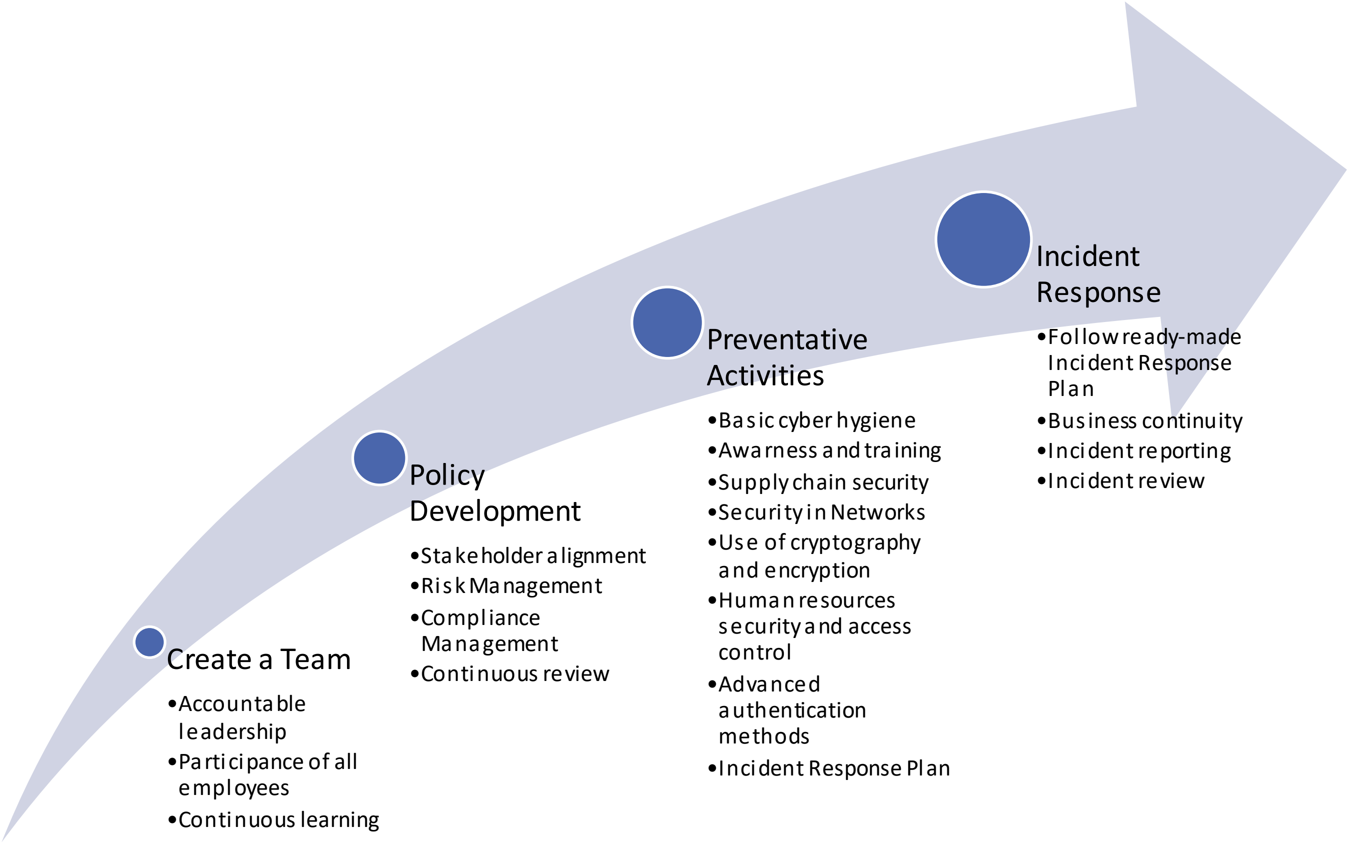


Figure 13 The main steps of Common cybersecurity governance model

6.2.1 Create a Team

The first step in the model is to create a cybersecurity team (Figure 14) which is responsible for:

- Coordinating tasks and resources for cybersecurity measures.
- Relay information to business units and teams.
- Provide guidance.
- Arrange cybersecurity training.
- Audit or arrange audit for cybersecurity measures.
- Report cybersecurity status, for example a yearly review.
- Functions as the first responders in cybersecurity incidents.

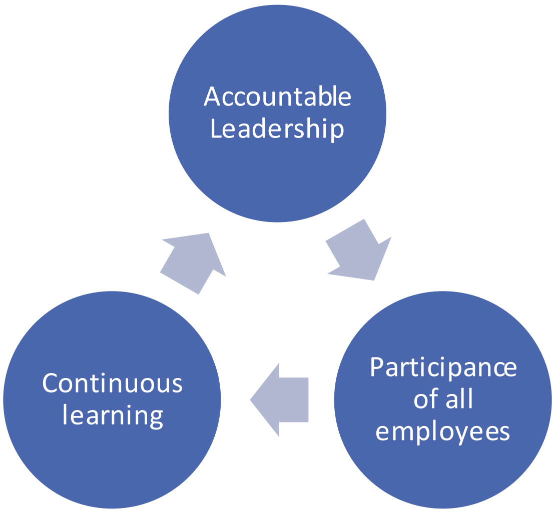


Figure 14 Create a Team

Accountable Leadership:

NIS 2 requires accountability from the senior leadership of the organizations by imposing criminal liability. Therefore, juristically, leaders of the organizations must be part of the cybersecurity management of the organization. Even though the board, the CIO, and the CEO are accountable for cybersecurity, it doesn't mean they are responsible for operational aspects. This can be done by sponsoring a cybersecure culture and providing means and resources necessary for cybersecurity management. Without accountability and responsibility, there are no effective policies or procedures.

Participance of all employees:

At the operational level, all employees are part of an organization's cybersecurity and part of the cybersecurity culture. Each employee is a potential vulnerability, but this can be mitigated with proper awareness and training, see preventative actions -step. Moreover, the cybersecurity team should include employees from all the important businesses and units, hence information relay and positive cybersecurity culture growth is much more effective.

Continuous learning:

A good cybersecurity culture includes continuous learning. Technology is evolving and new technologies are introduced with evolving business environment. Therefore, requirements for new security techniques arise. Bad actors are always looking for new ways to exploit vulnerabilities and new ways to infiltrate networks. For example, at EPES domain, IoT devices and other remote devices expose new vulnerabilities. As technology evolves, so must cybersecurity measures. Continuous cyber learning is essential for staying ahead of skills gap and adapting to new threats.

6.2.2 Policy Development

Policy Development

- Stakeholder alignment
- Risk Management
- Compliance Management
- Continuous review

Figure 15 Policy Development

Cybersecurity policy includes understanding key stakeholders, managing cybersecurity risks, managing cybersecurity compliance, and reviewing actions and statuses.

Stakeholder alignment:

A breakdown of potential stakeholders of an organization can be the customer, the board and executives, employees, vendors and suppliers, and the government and regulators.

The customer can be very sensitive about the protection of their data, thus compliance with the GDPR law is essential. Customer concerns can be alleviated by communicating data privacy and corporation responsibility.

The board and executives are a key sponsor for all company policies including cybersecurity policy. This was already touched on in the first step, but from the cybersecurity policy perspective, they have immense power to influence the culture and ability of forcing change. Boards and executives are aware of risk management regarding the business. Cybersecurity, or better say, lack of it, is a serious risk affecting business. One challenge in cybersecurity from the company perspective is that it doesn't generate immediate value. However, if cybersecurity is neglected, the outcome can be disastrous for the business and for personal lives. Therefore, cybersecurity is one key aspect of risk management.

Employees have operational roles and responsibilities in cybersecurity. Employees are both a cybersecurity threat and a guard in cybersecurity practices. Therefore, employees must implement and adhere to cybersecurity practices of the organization.

Vendors and suppliers are in the supply chain where they are indirectly affecting cybersecurity. As they might have less interest in the organization's cybersecurity, it is paramount that they comply with the organization's cybersecurity standards and practices. This is something that must be considered when procuring new systems, devices, and services.

Government and regulators have interest in the compliance with laws and regulations. By following this model, an organization ensures meeting cybersecurity regulations such as NIS 2.

By identifying stakeholders' needs and expectations, a message can be tailored accordingly, and security goals can be aligned with theirs. This allows a seamless flow of information, encouraging a collaborative environment. Other benefits include improved performance, reputation, trust, and resilience, while reducing risks including breaches, fines, lawsuits, and reputational damage. Active communication with stakeholders can significantly improve the organization's risk management practices.

Risk Management:

To comply with NIS 2, organizations must take measures to minimize cybersecurity risks, which include asset management, vulnerability analysis, and assessing cybersecurity effectiveness. The objective of risk management is to understand risks related to organizational, technical, and operational levels, and how to mitigate the risks involved. Cybersecurity risk management can be seen as probably the most important single task an organization can take in cybersecurity. By conducting risk management, organizations gain valuable insights, not just of risks, but understanding of business operations and requirements of running business by understanding assets involved.

The first step in risk management is to chart different assets an organization has and uses in operation. These assets are various items that are necessary for running business operations such as software, devices, different hardware e.g. network components and servers, data, and systems. Identify assets such as software and hardware and identify where sensitive information resides. In EPES domain, attention must be paid to cyber-physical assets. After assets have been identified, different threats and vulnerabilities can be investigated. Prepare for different types of attacks and analyze weaknesses to different attacks.

In CyberSEAS project, a few tools for asset management were developed such as CVIAT threat assessment and Rating-OT tools.

Compliance Management:

Compliance with relevant cybersecurity standards and regulations such as NIS 2 should be regularly audited to ensure operating in a secure and compliant manner. Compliance management needs to list the relevant standards and conduct internal and/or external audits. An effective cybersecurity governance model should define the necessary standards for different stakeholders as well as timeframe and type of audits to check compliance with the standards.

Continuous review:

Reviewing the performance of the governance model, including reviewing policies, procedures, and controls ensure they remain effective and relevant. The review can enhance the model by learning from incidents and vulnerabilities. This includes conducting post-incident reviews, updating policies and procedures, and adjusting technical controls as necessary. A performance measurement index can help identify gaps in cybersecurity actions. Few helping questions can be asked: What has been done? What needs to be done? How have actions affected performance?

6.2.3 Preventative Actions

Preventative Actions

- •Basic cyber hygiene
- •Awarness and training
- •Supply chain security
- •Security in Networks
- •Use of cryptography and encryption
- •Human resources security and access control
- •Multi-factor authentication
- •Incident Response Plan

Figure 16 Preventative Actions

It is much easier and cheaper to prevent a cyber-attack than face the consequences. There are various methods an organization can take actions to prevent cyber incidents.

Basic cyber hygiene:

Basic cyber hygiene is a practice of maintaining security of systems, devices, networks, and data. Anti-virus and malware software are a preferred method in protecting company and employee PC's. Software updates often include security patches that address known vulnerabilities, while firewalls help to prevent unauthorized access to the system. The main goal of cyber hygiene is to keep sensitive data secure and protected from cyberattacks and theft.

Awareness and training:

A healthy cybersecurity culture needs employees to have awareness for possible cybersecurity related risks. This can be elevated by regular training for cybersecurity threats. Special attention should be given to people, who are working directly with mission-critical equipment or systems. These can be identified in asset management task, see risk management earlier.

Supply chain security:

The objective of supply chain security is to identify, evaluate, and mitigate risks that arise when working with third parties. This includes both digital and physical security of software, services, and products. Attention or due diligence, when necessary, must be performed to the security aspect when procuring third party products and services. At EPES domain, large amounts of devices e.g. IoT devices provide a large surface area for attacks. Vulnerability scans and penetration tests enable early detection of low-level vulnerabilities. Without proper risk assessment and mitigation, third party supply chain can provide indirect cyberattack vulnerabilities.

Security in Networks:

When acquiring network and information systems, organizations should prioritize security. This involves assessing the security features of the products before purchase. Considerations include encryption capabilities, authentication mechanisms, access controls, and vulnerability management. Procurement contracts should explicitly outline security requirements and expectations.

During system development, security should be integrated from the outset. Secure coding practices, threat modelling, and regular security assessments are essential. Maintenance phases should include security updates, patches, and vulnerability assessments. Regular audits and code reviews help identify and address security gaps.

Security measures should cover the entire lifecycle of network systems, from design to decommissioning. This includes secure deployment, monitoring, incident response, and retirement procedures. Regular risk assessments ensure ongoing security alignment.

Manufacturers and vendors must provide timely security updates for their products. These updates address vulnerabilities, improve security features, and enhance overall resilience. Organizations should promptly apply patches to minimize exposure to known risks.

Use of cryptography and encryption:

Cryptography involves techniques for securing information by transforming it into an unintelligible format. It ensures confidentiality, integrity, and authenticity. In the worst case if a data is stolen, cryptography reduces risk of attacker gaining any benefits of the theft and thus provides last line of defence.

Encryption focuses on converting plaintext into ciphertext of which only authorized parties can read the ciphertext. This will ensure the integrity and origin of the data. Commonly encryption is used in data transmission and in data storage preventing unauthorized access.

Effective use of cryptography and encryption enhances data security, protects sensitive information, and contributes to overall risk management.

Human resources security and access control:

Human Resources Security focuses on safeguarding organization's data and resources by managing the human factors associated with security risks. Factors include employee behaviour, awareness, training, and compliance with security policies. Following human factor security measures should be considered: background checks when hiring, training and awareness of security risks and best practices, and employee exit procedures such as access and account deactivation when employee leaves the company.

Access control restricts who can access specific resources, physical or digital. At EPES domain, physical access control is many times mandatory due to health and safety reasons, but also for potential risk of threat agent gaining access to digital systems via physical devices.

Advanced authentication methods:

Advanced authentication methods include multi-factor authentication (MFA), and continuous authentication during the session. MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing a system or application. MFA provides enhanced security as compromising one authentication method does not lead to breach of the system. Continuous authentication monitors user behaviour throughout a session e.g. keystrokes, mouse movements, location, IP address, etc. If anomalies are detected, the session can be disconnected. Organizations should consider what type of authentication method is required in what systems and for what users.

Incident Response Plan:

An Incident Response Plan is crucial for effectively handling security incidents. In Figure 17 is shown a plan. This plan accounts for many of the topics explained in this common governance model and should be incorporated to supplement the overall cybersecurity governance. In brief, the plan includes five steps which enhance cybersecurity and provides guide in case of incident. These steps are preparation, detection, response, recovery, and review. This topic is explored in more details in deliverables D6.6 Data breach management plan and D6.8 Chapter 5 Common procedures and rules for incident response.

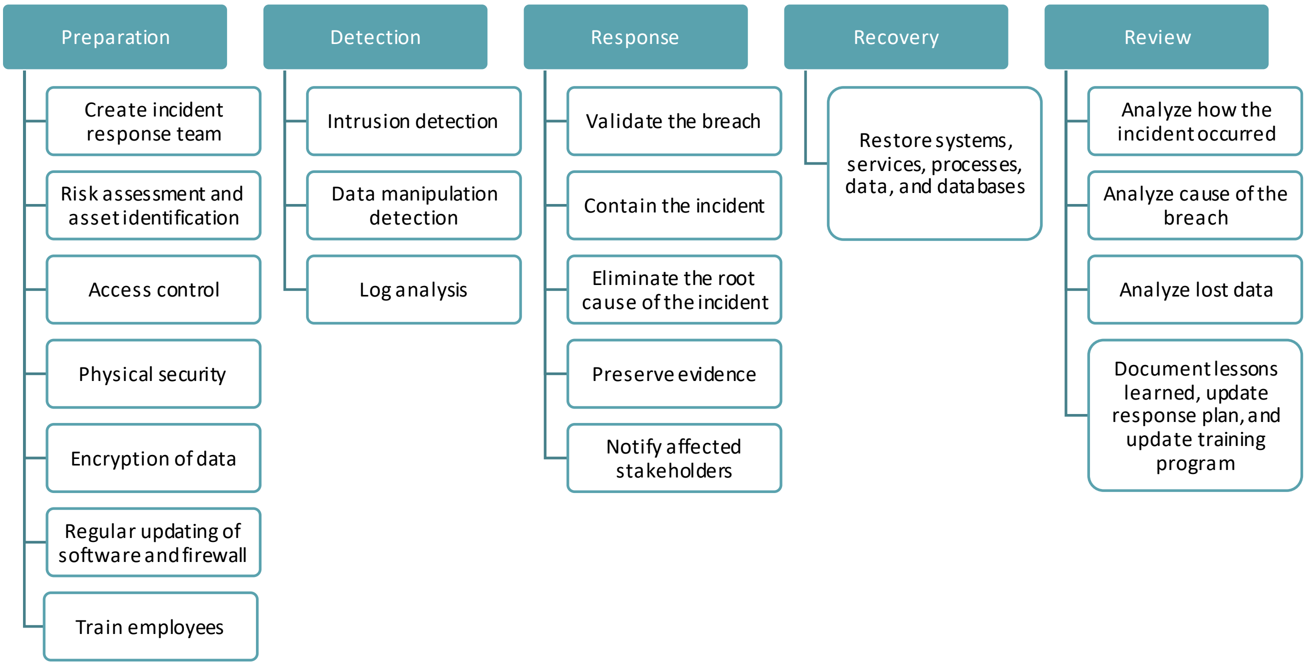

Preparation
Create incident response team
Risk assessment and asset identification
Access control
Physical security
Encryption of data
Regular updating of software and firewall
Train employees
Detection
Intrusion detection
Data manipulation detection
Log analysis
Response
Validate the breach
Contain the incident
Eliminate the root cause of the incident
Preserve evidence
Notify affected stakeholders
Recovery
Restore systems, services, processes, data, and databases
Review
Analyze how the incident occurred
Analyze cause of the breach
Analyze lost data
Document lessons learned, update response plan, and update training program

Figure 17 A Common model of data breach management describing steps

6.2.4 Incident Response

Incident Response

- Follow ready-made Incident Response Plan
- Business continuity
- Incident reporting
- Incident review

Figure 18 Incident Response

Being prepared for cyber incidents is paramount for a proper response. In this step we discover a few key tasks need to be conducted in the case of incident.

Follow ready-made Incident Response Plan:

In prior step, Incident Response Plan was explored as a preparation tool for cyber incidents. Let's consider incident happened, and now is time to execute what was prepared for. In the response step, the first task is to validate the breach or incident. Validate whether the breach has occurred, and it is not just a false flag. If in case of real incident, priority is to block malicious traffic and isolate the system affected by disconnecting the network connection, thus preventing any spread of contamination. Identification of the origin of the incident will help prevent any further attacks.

Even though investigation of the incident might be ongoing, it is important to be open and disclose the incident to the stakeholders affected. Hiding data breach will probably not work in a longer run and after involuntary disclosure, consequences will be much harsher.

Business continuity:

Organizations must plan for how they intend to ensure business continuity in the case of cyber incident. The objective is to have minimal downtime on services and business in general, and to minimize adverse effects of the incident. The recovery plan includes recovery of systems, services, processes, data, and databases. Restore systems affected and data from backups that are not infected. It is advisable to have backups as often as possible. Many companies today have outsourced data services to cloud providers. In this case, cloud providers are crucial to system restoration and effective communication between parties is required. At EPES domain, hardware equipment can also be infected or damaged, which might lead to their replacement or repair. This can lead to a considerable long downtime of service.

Incident reporting:

Cyber incidents need to be informed in a timely manner obligated by NIS 2. Essential and important organizations must have processes for reporting security incidents with significant impact on their services.

NIS 2 sets specific notification requirements:

- Early warning within 24 hours of becoming aware of the significant incident to the competent CSIRT or authority.
- Incident notification within 72 hours of becoming aware of the significant incident.
- Thereafter, an intermediate report may be requested by a competent CSIRT or authority.
- A final report must be provided to the competent CSIRT or authority not later than one month after the submission of the incident notification, unless the incident is still ongoing at that time, in which case a progress report must be provided and the final report within one month of the handling of the incident.

Learn more about reporting to CSIRT in CyberSEAS deliverable D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents.

Incident review:

Final step involves reviewing the incident and taking corrective actions. Review includes analysing the cause of the breach and identifying areas for improvement. Relevant details should be identified such as the timeline, systems affected, and actions taken during the incident. The cause of the incident could be e.g. misconfigurations, software bugs, or human errors. Assess the impact of the incident and analyze the lost or compromised data. Consider factors like downtime, data loss, financial implications, and customer experience. Based on the analysis, update the Incident Response Plan and training program accordingly. It is essential to learn from the incident to prevent future breaches and attacks. Identifying the root cause helps prevent similar incidents.

7 Conclusions (Updated)

This report aimed at providing a set of guidelines for development of a cybersecurity governance model for energy common data spaces. To do so, a brief introduction to energy system and different stakeholders there is followed by the description of energy common data space and its governance model as well as European initiatives for common data spaces. Then, a few EU funded projects dealing with cybersecurity issues have been reviewed. Then, a review over cybersecurity regulatory frameworks on national and EU levels is provided. Guidelines for the development of a cybersecurity governance model for energy common data spaces are described in Chapter 5 where policy development, risk management, compliance management, incident response plan, awareness and training, continuous review, stakeholder alignment, reporting mechanisms and preventive activities are discussed. Finally, in Chapter 6, NIS 2 directive and its requirements for organizations is explored and a common cybersecurity governance model is presented. By following four steps shown in the governance model, an organization is compliant with the NIS 2 directive.

8 References

[1] [Online]. Available: https://www.opendei.eu/about/.

[2] [Online]. Available: https://www.opendei.eu/projects/energy-sector-new/.

[3] [Online]. Available: https://design-principles-for-data-spaces.org/.

[4] "European Commission (November 2020) Proposal for a regulation of the European parliament and of the council on European data governance (Data Governance Act). Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222".

[5] [Online]. Available: https://www.bdva.eu/about.

[6] [Online]. Available: https://www.bdva.eu/TF10-data-spaces.

[7] [Online]. Available: https://www.bdva.eu/I-Spaces.

[8] [Online]. Available: https://www.fiware.org/about-us/#why.

[9] [Online]. Available: https://www.fiware.org/community/fiware-ihubs/.

[10] [Online]. Available: https://www.fiware.org/marketing-material/fiware-for-data-spaces/.

[11] [Online]. Available: https://gaia-x.eu/what-is-gaia-x/about-gaia-x/.

[12] [Online]. Available: https://gaia-x.eu/who-we-are/hubs/.

[13] [Online]. Available: https://gaia-x.eu/wp-content/uploads/files/2021-08/Gaia-X_DSBC_PositionPaper.pdf.

[14] [Online]. Available: https://docs.gaia-x.eu/framework/.

[15] [Online]. Available: https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Policy-Rules_Document_v22.04_Final.pdf.

[16] [Online]. Available: https://internationaldataspaces.org/we/the-association/.

[17] [Online]. Available: https://internationaldataspaces.org/make/hubs-and-competence-centers/.

[18] [Online]. Available: https://internationaldataspaces.org/new-position-paper-governance-for-data-space-instances/.

[19] [Online]. Available: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.

[20] [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf.

[21] [Online]. Available: https://www.beuth.de/en/technical-rule/din-spec-27070/319111044.

[22] [Online]. Available: https://data-spaces-business-alliance.eu/.

[23] [Online]. Available: https://data-spaces-business-alliance.eu/dsba-hubs/.

[24] [Online]. Available: https://dsba-brokering-data-spaces.b2match.io/.

[25] [Online]. Available: https://eu-sysflex.com/.

[26] [Online]. Available: https://eu-sysflex.com/wp-content/uploads/2021/06/EU-SysFlex-D5.4-Data-security-and-privacy-guidelines-and-feasible-cyber-security-methods-for-data-exchange-platforms_FINAL.pdf.

[27] "https://phoenix-h2020.eu/about/," [Online].

[28] "https://success-energy.eu/," [Online].

[29] [Online]. Available: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/Energie/Sonderregelung-Meldepflicht/sonderregelung-meldepflicht_node.html.

[30] [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.html.

[31] [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.html.

[32] [Online]. Available: https://www.bdew.de/media/documents/20210222_BDEW_B3S_Anlagen_zur_Steuerung_und_Bundelung_v1.1_WQNbS5a.pdf.

[33] [Online]. Available: https://cdn.edupedu.ro/wp-content/uploads/2022/01/Monitorul-Oficial-Partea-I-nr.-2Bis.pdf.

[34] EUR-Lex. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[35] ENISA. [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms.

[36] U. G. Security. [Online]. Available: https://www.security.gov.uk/guidance/secure-by-design/activities/assessing-the-effectiveness-of-security-controls.

[37] Lansweeper. [Online]. Available: https://www.lansweeper.com/blog/cybersecurity/a-guide-to-access-control/.

[38] CyberItalia. [Online]. Available: https://www.dlapiper.com/en/insights/publications/law-in-tech/cyberitalia-the-nis-1-directive-and-the-new-nis-2-directive-in-a-nutshell.

[39] P. security. [Online]. Available: https://phoenix.security/nis2-regulation-differences/#:~:text=NIS2%20and%20NIS%201%20what%20are%20the%20differences&text=While%20NIS1%20only%20applies%20to,industries%20and%20digital%20service%20providers..

[40] CyberSEAS research project (GA n.101020560), "Watch Now Webinar: Unpacking Cyber-Resilience for EPES with NIS2 (Woman's Perspective)," 02 March 2024. [Online]. Available: https://cyberseas.eu/watch-now-webinar-unpacking-cyber-resilience-for-epes-with-nis2-womans-perspective/.

[41] U. C.-R. f. E. w. N. 2. [Online]. Available: https://cyberseas.eu/watch-now-webinar-unpacking-cyber-resilience-for-epes-with-nis2-womans-perspective/.