Horizon 2020 Program

ICT-02-2020

Building blocks for resilience in evolving ICT systems

Certifying the Security and Resilience of Supply Chain Services

Project Report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952690.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Description
AIS	Automatic identification system
BP	Business Partner
CA	Conformity Assessment
CC	Common Criteria
CII	Critical Information Infrastructure
CSA	Cybersecurity Act
ENS	Entry Summary Declaration
LNG	Liquefied Natural Gas
MRA	Mutual Recognition Agreement
PCS	Port Community System
PDCA	Plan-Do-Check-Act
RA	Risk Assessment
SC	Supply Chain
SCADA	Supervisory Control And Data Acquisition
SCRM	Supply Chain Risk Management
SCM	Standard Cargo Manifest
SCS	Supply Chain Service
SOG-IS	Senior Officials Group Information Systems Security
ToE	Target of Evaluation
TVRA	Threat Vulnerability Risk Analysis
VTS	Vehicle Transport Service

Executive Summary

This document reports the results of the activities performed in the first phase of CYRENE. The main output is related to the requirements that have been collected from relevant standards and literature review, project pilot partners, as well as external stakeholders.
The document is divided in four parts. In the first one, an overview of the Supply Chains is given, describing both their classification, including three different views (business, technical and sectorial) of the SCs, and their security aspects, consisting of the threat landscape, legal framework, SC security and Risk Management standards and SC risk assessment methodology and tools.
In the second part, an overview of the EU Certification schemes is provided, encompassing the general definition and requirements (policy, legal, standards, methodologies, technical) regarding the security certification.
Moreover, in the third part, the document reports on the methodology used for collecting, analyzing and validating the requirements through the project's Advisory Boards. The feedback obtained from the proposed questionnaire for requirements validation are presented in this part and conclusions are drawn afterwards.
Finally, the fourth part of the report deals with the three Targets of Evaluation (ToEs), namely, the Business, Technical, and Sectorial. Their descriptions and the respective validated requirements are provided in this section.
Two appendixes are included in the document. The first one gives information on a glossary that forms the basis of the concepts used in the project, while the second one gives details regarding the first workshop organized with the Advisory Boards at the end of the first six months of the project.

1. Introduction

1.1 Scope

This document is a record of the requirements that have been collected from several stakeholders, based on which the specifications of certification scheme, the definition of the conformity assessment processes, as well as the development and integration of tools within the CYRENE project will be developed.

The described outputs are the results of the following tasks:

- T1: Conformity and certification assessment scheme state of the art revision;
- T2: Large-scale European Supply Chain requirement gathering, analysis and tracking;
- T3: Legal and ethics requirements;
- T4: Classification of Supply Chains.

During the first task, the activities of CYRENE's phase 1 were initiated, focusing on the definition of a solid basis for setting up the CYRENE Conformity Assessment scheme. An updated state of the art analysis was carried out, consulting scientific papers, related projects, and relevant reference conformity assessment and certification schemes for cyber-security in related domains. In particular, during the task, the CYRENE consortium consulted and built upon the baseline security requirements recommended by ENISA [1]. The existing relevant schemes are mapped to the four CYRENE circles of consideration (as described in *Figure 2*), as well as to the three main aspects of CYRENE certification: business, infrastructure, and individual devices. Based on the described analysis, the task creates a basis for the conformity assessment scheme which grounds the multi-level evidence-driven supply chain risk assessment process.

During T2, in parallel to T1, the CYRENE consortium identified Supply Chains' Conformity Assessment requirements, along with legal/forensic, security and privacy requirements and covered the following aspects: (i) identification of requirements and specific needs of the participating Supply Chain Services, which represent different industry sub-sectors and with different needs with regard to IT security; (ii) substantial engagement of the participating SCs operators (representing different industrial sectors) so as to gain feedback regarding their needs and priorities in the frame of the project; (iii) specification of criteria associated to the nature of their IT system and infrastructure of SCs (such as size, interdependencies with other IT systems, services offered, etc.); (iv) analysis and documentation of the requirements of the various stakeholders, i.e. port authorities and operators, security systems integrators, policy makers etc.) in terms of the handling of multi-order dependencies and cascading effects; (v) identification and classification of dependencies between infrastructures and between SC operators, as well the dependencies among the business inter-organizational, infrastructure, and individual assets/devices.

The output of T3 is the identification, analysis and report of relevant legal and ethics requirements for CYRENE. The regulatory framework applicable to the project is analyzed to define requirements that are not dealt within the previous tasks.

Finally, T4 activities are focused on the specification of the criteria associated to the nature of IT systems and infrastructure of SCs (such as size, interdependencies with other IT systems,

services offered, number of administrators and IT security awareness level, etc.) based on which the categorization of the enterprise target group will occur.

1.2 Document Structure

The rest of the document is structured as follows:

- Chapter 2 presents an overview of the Security of Supply Chains, describing how Supply Chains are classified and the security aspects of the involved Supply Chain Services.
- Chapter 3 gives an overview of the EU Certification schemes, presenting definitions and requirements that address the Security Certification process.
- Chapter 4 presents the Methodology used for requirements elicitation and their validation strategy.
- Chapter 5 presents the CYRENE Conformity Assessment process, including the description of the Targets of Evaluation and their requirements.
- Finally, Chapter 6 concludes the document.

2. Security of Supply Chains

2.1 Supply Chain Classifications

According to Mentzer [2], a Supply Chain (SC) is defined as a globally distributed, interconnected set of entities (i.e., organizations, individuals or/and CIs), processes and services that relies upon an interconnected web of ICT infrastructures and cyber networks to leverage the flows of products, services and information from a source to a customer.

The literature is rich with efforts [3] to classify SCs. Ageron et al [4] developed a classification model that is focused on the practices related to Supply Chains (see *Figure 1*). The model, which is depicted as a pyramid, puts at the top the Managerial Process, on the second level the Information Sharing and Information Technologies, and on the bottom level the Operational process.

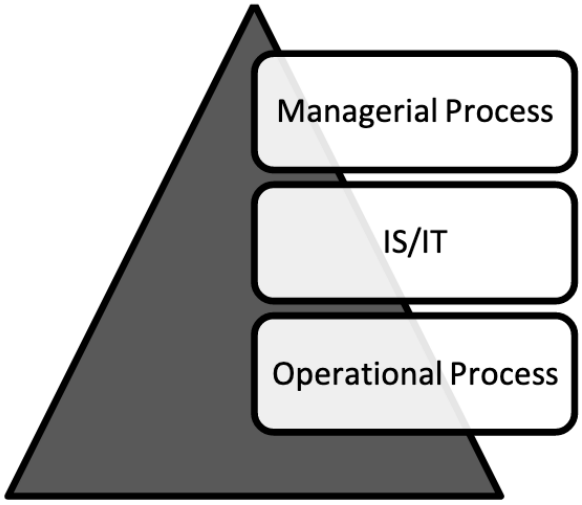


Figure 1 - Ageron et al. Classification model.

Jabbour et al. [5] mapped supply chain practices into four constructs of supply chain management: (i) Supply chain integration for production planning and control support; (ii) Information sharing about products and targeting strategies; (iii) Strategic relationship with customer and supplier; (iv) Support customer order.

Although these works are important and provide clear answers for the purposes of the related research, they failed to consider a conceptual representation of supply chains, which is practical for conformity and certification purposes for Supply Chain Services (SCSs). To address this challenge, CYRENE has developed a conceptual representation of SCSs based on the four circles of consideration. (*Figure 2*).

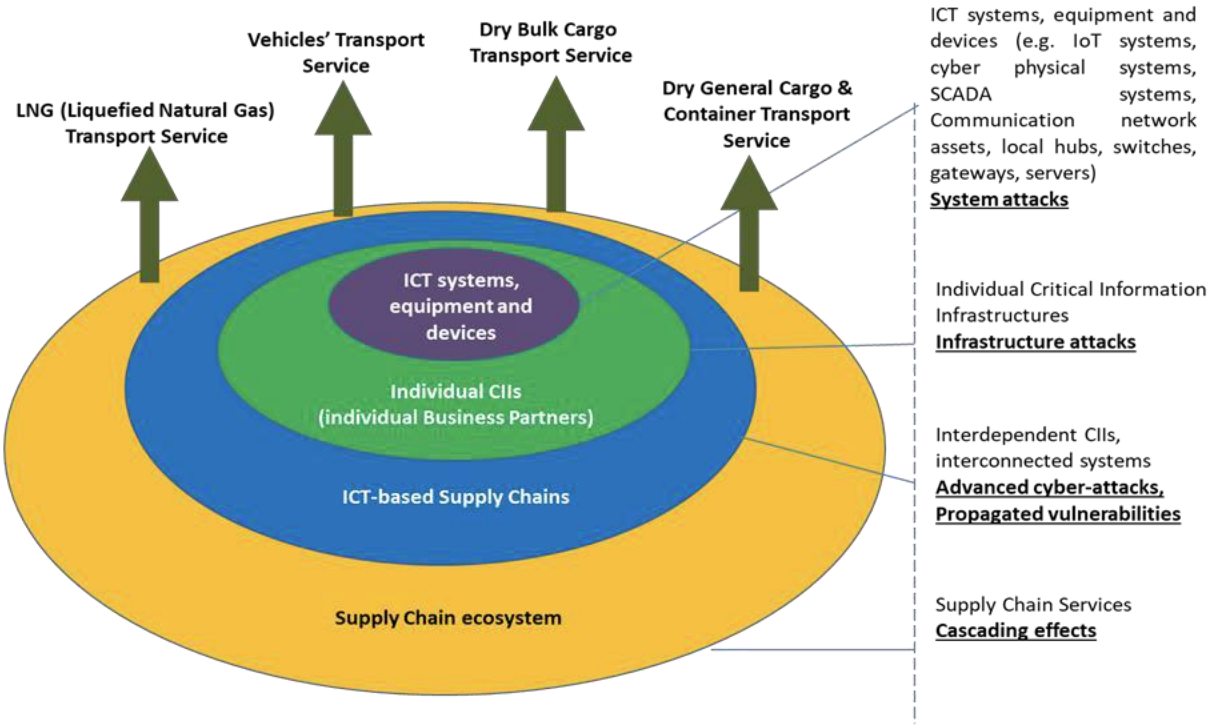


Figure 2 - CYRENE circles of consideration for the CA process.

In such representation, the established SCS interconnections reflect the relationships that exist between the involved entities representing how one process, activity or resource relies upon another. For example, an entity could be dependent on receiving information from another entity or organization as an input to one of its critical business processes.

The first inner circle**,** our starting point, includes all the ICT systems, equipment and devices (e.g. IoT systems, cyber-physical systems, SCADA systems, communication network assets, local hubs, switches, gateways, servers) used by the business partners, which support the operation of the SCSs. The second circle encapsulates the previous one and incorporates the individual Critical Information Infrastructures (CIIs) operated by the individual Business Partners involved in the SCSs. The third circle encloses the two previous ones and represents the Interdependent CIIs composing the ICT-empowered SCSs. Finally, the fourth circle contains all the already mentioned circles, complemented with the Business Perspective of the SCSs such as processes information exchange, business logic, ICT assets, Business Partners, etc. These four circles have been identified and distinguished based on the homogeneity of characteristics (safety, technical requirements, architectures etc.) identified in each one of them.

As mentioned earlier, Supply Chain encompasses entities, assets, individuals, organizations and processes to leverage the flows of products and services to end users. In other words, supply chain provides the required infrastructure and resources for delivering a supply chain service or building a product.

We have mapped the four circles of consideration to three different but interdependent views of SCSs, the *Business view*, the *Technical view* and the *Sector specific view*. This is important since it allows us to define views that can be directly translated to Targets of Evaluation (ToEs), which

represent the main block for the CYRENE Conformity Assessment. It also helps us to investigate a Supply Chain from a different perspective, in order to analyze the effects of business, technical and sector specific aspects on Supply Chain Services. In the next sub-sections, we provide an outline of the three views.

2.1.1 Overall business view

In the context of CYRENE, the business view focuses on the identification, analysis and assessment of any Supply Chain elements that have direct input on the business perspective of an organization. As such, in this view, details of organizational processes, business partners that contribute to such processes (e.g. suppliers), stakeholders, facilities, related business logic (e.g. data and information flows, decision making), and any legal/regulatory restrictions are considered. As a result, all business-driven elements in a Supply Chain which have impact on the Supply Chain Services are taken into consideration.

2.1.2 Technical View - Asset Interdependent SC

The technical view of the SCs includes an asset-based interdependent view of the Supply Chain, which is focused on the ICT assets within the SC used to carry out the activities related to the provision of the SCS. In such view, the SCS elements are all ICT assets (e.g. networks, IoT sensors, communication devices, local servers) hosted by the business partners' infrastructures (and/or their subcontractors) and are utilized for the provision of the SCS.

2.1.3 Sector Specific view - SC snapshot

Business Partners within a SC can belong to different sectors. For example, for the Vehicle Transport Service SC provision, the business partners belong to different industries and sectors (e.g. automotive industry, transport, government).

The sector-specific view of a SC is the view that an individual business partner adopts to analyze the SCS. The sector-specific view of the SC consists of the specific processes that this business partner is participating and his ICT assets that are involved in the provision of the SCS.

The Supply Chain framework is based on components, which are complex designs, consisting of various industry sub-sectors that focus on different IT security levels depending on their needs [6]. Based on that, the SCS can be analyzed according to their sector-specific schemes, which ensure vertical and horizontal security and resilience of Supply Chain Services. This section describes generic Supply Chains classifications that are based on sub-sector specific views.

First, the sub-sector specific classification is based on the three different specific view aspects for the Supply Chains and their components: hierarchical, structural and functional [7]. According to the hierarchical aspect, the parts of a Supply Chain system can be considered as submodules and the system itself can be part of a more comprehensive system, i.e., a supersystem. Second, each Supply Chain sector can be classified based on the set of the sub-sectors' elements and their interconnections. Such classification is based on the sub-sectors' structural architecture, i.e.

connections/relations, elements. Last, each sub-sector can be categorized based on its functional aspect, where the main categorization criterion is the internal status of each sub-sector.

Another sector-specific view of the Supply Chains, according to Mattsson [8], is that companies and Supply Chains can be regarded as open systems, where their components can be linked not only to each other but also to the surroundings, i.e. suppliers, customers, competitors, and the authorities. Such view leads to a more generic description, where the sub-systems in a supply chain can be considered as the functions within the Supply Chain that add value to the final product. Based on that, the sub-systems in a Supply Chain system are the individual companies.

Finally, a really important Sector Specific view is based on the internal and external Supply Chain linkages [9]. Specifically, Mark Barrat and Ruth Barrat proved that internal linkages between sub-sectors are really important as the information flow improves operational performance of the whole Supply Chain. Additionally, this work concluded that organizations need to recognize the combining role of internal and external information-based linkages in order to extend the visibility across the entire Supply Chain.

This section has analyzed the different Supply Chain classifications based on sub-sector view in order to investigate the effects of each sub-sector on Supply Chain services. Also, it has shown the importance of linkages among the sub-sectors as far as the entire Supply Chain visibility.

2.2 Security Aspects of the SCSs

General aspects and requirements (legal, policy, standards, technical) related to the security of the SCs will be addressed in this section.

2.2.1 SCS threat landscape

As the SCSs become more and more complex and technology-dependent, the SC threat landscape is getting broader. Their complexity is directly related to the interdependence among the abundance of sectors, ICT assets and services. Hence, the SCS stakeholders must encounter a variety of cyber/physical threats, either internal, external or diffused, coming from the whole SC. The combination of these threats can create numerous threat scenarios, which may affect the confidentiality, integrity, and / or availability of the SCS's information and ICT systems. Among others, the result of such scenarios may include reduced or unwanted functionality, tampering, theft, counterfeiting or malicious content and may aim at gaining financial, political, military, or even ideological benefits.

ENISA has proposed good practices for cybersecurity in the maritime sector in a report[1] which describes multiple key cyberattack scenarios, targeted at the port ecosystem, concerning both IT and OT infrastructures and able to result in cyber-physical consequences. Each of these real-life scenarios is associated with the impacts that could cause, the assets affected, the stakeholders involved, the details of the attack, as well as the main security measures that could be taken to

[1] Port cybersecurity : good practices for cybersecurity in the maritime sector. ENISA, 2019, [Online]. Available: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector. Accessed: March 15, 2021.

help mitigate the risk. For the purpose of this work three threat scenarios of SCS are presented, as well as the most common individual threats[1] that can lead to such a situation.

2.2.1.1 Threat scenarios in the Supply Chain Services (SCS)

In the following threat scenarios [10][11] it is depicted how a security breach in a specific node of the SCS can cause damage to a larger scale, even to a physical level.

Threat scenario in the Container Management SCS

A terrorist group wants to commit an attack at a port by placing a bomb in a container, which will be detonated before the inspection process of the security authorities, aiming for the greatest number of injuries and deaths. Knowing that the sealed container leaves the company's factory and gets packed at the warehouse of a third-party company before being delivered to the port, they gain access to the third party's IT systems, specifically to the container management system. In this way, they replace the information of a particular shipping container with another one that carries out a bomb, which they make sure it has been placed in the warehouse. After the moving of the malevolent container to the port, they gain access to the container shipping system, which keeps the routing or scheduling of the containers, so that they can change the containers' details of location and maximize the number of victims.

Considering that the containerized freight is almost one third of total trade exchanges measured in monetary value, according to Eurostat 184/2016 statistics, and when kilometres or tonne-kilometres are measured, the percentage of maritime transport in relation to total transported is even higher, it turns out that the impact of realizing such a possibility would be significant.

Threat scenario in the Vehicle Transport SCS

A team of criminals launches a series of cyber-attacks, including phishing information from the port authorities and key officials as well as remote exploitation of software-related vulnerabilities using malware, to steal vehicles from the vehicle terminal of a port. Eventually they manage to compromise a few computers and systems, get access to the vehicles' vast network of interconnected On-Board Units (OBUs) and spoof their geolocation. Having access to the in-port vehicle scheduling processes, they can continue changing the vehicles' route and location to the values of their interest, without the port system administrator being able to detect it. They can also penetrate into the port's surveillance system that controls the CCTV video cameras, so that they gain access and delete video streams that could disclose their malicious activities.

The Vehicle Transport Service is supported by many stakeholders, for example port authorities and shippers, and involves the transfer of a plethora of vehicles and equipment, such as trucks, cranes, container terminals and providers of Dockers. This fact, together with the involvement of actors such domestic and international transportation, IT, warehouse management, order and inventory control, materials handling, and import/export facilitation, make the likelihood of a scenario like this high and its scope wide and complex.

Threat scenario in the LNG Transport SCS

A fake email is sent by the supposed IT company that supports and maintains the ICT infrastructure of a shipping company, requesting the downloading and installation of a software that improves the performance of their systems. In fact, the email is sent by a group of terrorists who, subsequently, download and execute arbitrary code on the victims' systems and gain access. As

a result, the terrorists can exploit vulnerabilities to delve deeper into the network of the oil company's monitoring software, which they can use to break into the system by performing remote tank monitoring, asset tracking, and data reporting services, and empty the oil tank without being detected.
As liquefied natural gas (LNG) is mainly methane, which is odorless, colorless, non-toxic and non-corrosive, in a liquid form for easier storage and transport, its vaporization could cause inflammation, freezing or asphyxia. In addition, a potential explosion of an LNG tanker can be compared to a nuclear bomb's, since it contains more than 100,000 m3 of LNG.

2.2.1.2 Individual threats in the SCS assets

As can be seen from the above-mentioned scenarios, combining individual threats can lead to a variety of impacts, such as cargo and goods stealing, sensitive and critical data theft, illegal trafficking, systems damage or destruction, environmental disaster, or even human injuries and death. In addition, an organization's paralysis, financial loss and costs, kidnapping, fraud and money theft are also included in this long list, and all of the above are usually accompanied by tarnished reputation, and /or loss of competitiveness.
The assets (physical, digital, people, processes, smart objects) used to provide a SCS, hosted and operated by the various SCS business partners involved are called SCS assets.
Examples of potential threats to the digital SCS assets are eavesdropping, interception of emissions or sensitive information, IT/OT assets hijacking, network reconnaissance or traffic manipulation, data poisoning, data manipulation and all kind of nefarious activity and abuse, such as Denial of Service (DOS), brute force, phishing, social engineering or targeted attacks, as well as malware, identity or data theft or abuse, manipulation of information, or even geolocalization signals spoofing or jamming.
Additionally, possible threats to the non-digital SCS assets include unauthorized access to the premises, vehicles or IT/OT end devices, terrorism, hacktivism, coercion, extortion or corruption of employees or stakeholders, piracy or mafia, sabotage, vandalism, natural disasters, environmental damages and theft.
Although in most people's minds a threat may be related to a deliberate act, there is also the likelihood of unintentional damage, which results from data deletion, information leakage, third party security failure, erroneous administration of IT/OT systems, use of unreliable sources or improper penetration testing. An attacker can take advantage of coincidences like all types of outages and natural or environmental disasters, or even force them to carry out their plan. Systems and devices failures and malfunctions, as well as failure or disruption of service providers are also common threats.

2.2.2 Legal framework

The pivotal concepts of the CYRENE regulatory end ethical framework are related to data security and data protection. However, there are similar concepts such as privacy and information security. This chapter briefly sheds light on these mentioned concepts but also on regulation and legislation. The chapter provides preliminary facts that are crucial for the development of a regulatory framework specifically designed for this project.

2.2.2.1 Data Protection and Data Security

Information privacy is a set of rules that governs the collection and use of personal information. It addresses individuals' right to decide about the processing of information related to them by a third party. Information privacy is one of the foundational pillars of privacy protection and personal data protection. Closely related to Information Privacy is the concept of Information Security. Information Security is about preserving the 'security triad' - confidentiality, integrity and availability of information (Densmore, 2019). There are similarities between privacy and security but there are also factors that distinguish them. Therefore, privacy and security could be seen as supplementary concepts but not complementary.

Information integrity is about its authenticity and it relates to accuracy and completeness of personal information. Confidentiality of information is related to limited access to information, whereas availability enables access to information but only to those who are authorized to use this information. To satisfy the standards of the 'security triad', appropriate security controls have to be implemented and security incidents should be prevented. In this way, information security preserves information privacy.

Differences between privacy and security could be found in the fact that implementing information security does not necessarily preserve information privacy. Namely, information privacy serves to protect specific type of information. However, there is no information privacy without the implementation of information security. Therefore, we can have security without privacy, but we cannot have privacy without security (Densmore, 2019).

2.2.2.2 Regulation and Legislation

There is a common mistake with using terms of regulation and legislation in the same sense. They may be similar, but the differences between them should not be neglected. Both regulation and legislation contain provisions with rules, rights, and obligations and it would not be wrong to claim that they regulate certain relations, entities or fields. However, there are at least two distinct lines between these concepts.

The first one concerns the respective sources. Whereas legislation usually refers to statutory law enacted by the legislator (the legislative branch of government), regulation is adopted and promoted by entities that are supposed to develop a self-regulatory system (in order to introduce certain rights/obligations). In other words, legislations are acts adopted by a state, whereas regulations might be adopted by companies, industry associations, formal or informal bodies.

The second distinctive line concerns the relationship between general and specific. Legislators often adopt rules that are general and applicable in many perspectives. Thus, the concrete application of the rules would only be possible if general rules and principles are specified to be used in a specific context. This process is usually carried out by the development of regulation, or more specifically, self-regulation. However, legislation might be a subset of a regulation. This would be the case when states or other legislative instances are allowed to adopt documents that

are formally promoted as regulations, but contain principles and general rules. These principles and rules might be specified by legislations adopted by lower legislative instances[2].

As explained earlier, the scope of this document is to present a specific regulatory framework designed to contribute to the project objectives. Therefore, this document presents specific regulations adapted for a specific purpose. Nevertheless, the document first refers to the principles and rules of various but relevant legislations. In the following sections, these principles and rules are 'custom-made' and are presented as the CYRENE regulatory framework[2].

2.2.2.3 Relevant European Union Law

All actions taken by the EU institutions are based on treaties. These are binding agreements between the EU Member States which set out the EU objectives, the rules for the EU institutions, the decision-making processes and the relationship between the EU and the Member States.

Treaties are the starting point for the EU Law and are known in the EU as primary law. The body of law derived from the principles and objectives of the treaties is known as secondary law. Secondary law includes regulations, directives, decisions, recommendations and opinions.

Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (hereinafter referred to as the Charter) brings together the most important personal freedoms and rights granted by the EU Law into one legally binding document. The Charter was announced in 2000 and came into force in December 2009 together with the Treaty of Lisbon[3].

The purpose of the Charter is to promote human rights within the territory of the EU. Many of the rights existing in the Charter were previously set out in:

- The EU Treaties
- The European Convention on Human Rights
- Case law of the Court of Justice of the European Union
- National constitutions

The Charter has the same legal power as the EU Treaty. This means that it is superior to the legislation of the Member States. The Charter applies when EU countries adopt or apply a national law to implement an EU directive or when their authorities directly apply an EU regulation. In cases where the Charter does not apply, the protection of fundamental rights is guaranteed under the constitutions or constitutional traditions of EU countries and international conventions they have ratified. The Charter does not extend the scope of the EU to matters which are outside its normal competence.

---

[2] Kosti, N., Levi-Faur, D., & Mor, G. (n.d.). Legislation and regulation: three analytical distinctions. *The Theory and Practice of Legislation*, *7*(3).

https://www.tandfonline.com/doi/full/10.1080/20508840.2019.1736369

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

The Charter contains all rights granted by the ECHR. However, the Charter addresses some additional freedoms and rights in order to meet the reality of newly formed issues. One of the newly granted rights relates to the protection of personal data. The Charter ensures that private and family right should be respected granting that 'Everyone has the right to respect for his or her private and family life, home and communications.' In addition, Article 8 regulates the protection of personal data by granting that 'Everyone has the right to the protection of personal data concerning him or her'. In addition, the same article lays down that data processing must be carried out fairly, within the specified purposes, and based on consent or other ground laid down by law. Finally, compliance with the 'rules shall be subject to control by an independent authority.'

Despite academic critics and polemics (Sloot, 2017), the Charter separated data protection from the protection of personal privacy. The additional significance of the Charter lays in the fact that both rights are classified as fundamental rights.

GDPR

The Regulation (EU) 2016/679[4] on the protection of natural persons regarding the processing of personal data and on the free movement of such data (hereinafter GDPR) is the core legislative source of the EU Data Protection Law. The GDPR empowers the EU Data Protection Law by promoting a common set of data protection rules that are implementable in all Member States of the EU. The GDPR is a Regulation and unlike directives, regulations are directly applicable under EU law. In other words, there is no need for their transposition into national laws, and there is no need for national implementation. For that reason, the GDPR is of the highest relevance for CYRENE and represents a common framework for protecting personal data in the EU. To define its scope with regards to CYRENE, it should be noted that the GDPR does not apply to the processing of personal data regarding:

- activities which fall outside the scope of the EU Law,
- certain matters of the EU security and defense policy,
- purely domestic activities and
- cases of data processing carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The GDPR confirms and additionally develops principles promoted by fair information practices. Therefore, the GDPR does not provide novelties concerning promoted principles but rather organizes and specifies them in a different way than it has been the case before. The GDPR promotes six principles, plus the accountability principle that is extracted as the separate one. All of them are relevant in the context of CYRENE.

Lawfulness, fairness, and transparency principle. Lawfulness means that the processing of personal data has to be carried out on the basis of one of the six legal grounds enshrined by the GDPR: consent, the performance of a contract, legal obligation, the vital interest of individuals, public interest and the legitimate interest.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Purpose limitation principle. The purpose limitation principle is embedded in Art 5(1)b of the GDPR. This article foresees that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data minimization. 'Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. To satisfy the requirements of this principle, data controllers have to pass proportionality and necessity tests. That means data controllers should be able to prove that plans regarding the use of a particular scope and a type of data are reasonable to achieve the specified purpose of data processing.

Data accuracy. The GDPR laid down that 'Personal data must be accurate and, where necessary, kept up to date'. Therefore, 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

Storage limitation. Storage limitation principle is about the obligation to keep personal data 'in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.' So, once the purpose of processing is identified, data controllers have to determine the retention period.

Integrity and confidentiality. The principles of integrity and confidentiality are embedded in the GDPR provision stating that personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures'. Concerning the security of personal data, data controllers should take into consideration several factors when determining appropriate technical and organizational security measures. Also, this principle should be interpreted in the context of data controllers' obligation to report a breach of personal data in a relevant way.

Accountability principle. The accountability principle is not a new principle in the data protection framework. Nevertheless, the GDPR clearly defines it. In that way, the GDPR significantly contributes to the existing data protection framework. The essence of the principle lays in the data controllers' obligation to comply with other principles as well as to be able to demonstrate it.

NIS Directive

The Directive 2016/1148 on the security of network and information system (hereinafter NIS Directive)[5] is the first EU legislative initiative exclusively dedicated to cybersecurity. NIS Directive was adopted and entered into force in 2016, whereas the Member States had to transpose this directive into national laws until November 2018. For the effective implementation of the directive, the Member States had at their disposal the "NIS toolkit". This toolkit provides practical information about the best practices, explanations, interpretation of specific provisions, and how they should work in practice.

The general goal of the NIS Directive is to provide legal measures to strengthen the overall level of cybersecurity in the EU. For that purpose, Member States should appropriately equip Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. They should

[5] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32016L1148

collaborate and form a 'Cooperation Group' to support and facilitate strategic cooperation and the information exchange. NIS Directive imposes an obligation to the Member States to effectively cooperate on specific cybersecurity incidents and share information about risks via CSIRT Network. Member States should identify the 'operators of essential services' within business sectors such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. In these sectors, operators should take appropriate security measures and notify serious incidents to the relevant national authority.

Article 23 of the directive requires a periodical review of the directive by the European Commission. As a result of the review process, the new legislative proposal has been presented in December 2020. Proposal for 'NIS 2.0' contains measures for the improvement of cybersecurity infrastructures, and particularly the resilience and incident response capacities of public and private entities, and competent authorities. The new proposal expands the scope of the directive application and includes medium and large companies.

Regulation (EU) 2019/881

Regulation (EU) 2019/881[6] has replaced Regulation (EU) No 526/2013 (Cybersecurity Act) and it represents the regulatory framework for ENISA (the European Union Agency for Cybersecurity) on information and communications technology cyber-security certification. This Regulation foresees a permanent mandate for the European Union Agency for Network and Information Security (ENISA) and the creation of an EU certification framework for ICT products, processes, and services.

It is an undeniable fact that cyberattacks are becoming more sophisticated and they are usually featured by cross-border effects. Therefore, there is an increasing need for coordinated and effective responses as well as appropriate crisis management at the EU level. The goal of Regulation is to empower cybersecurity structures at the EU level by establishing the set of measures that the Member States should develop as well as by strengthening the cooperation among them. The Cybersecurity Act has two major fields focal:

- The first one refers to empowering ENISA by making it a permanent agency of the EU
- The second one is about establishing a European cybersecurity certification framework to ensure the application of a common certification for information and communications technology ("ICT") products, processes and services.

ENISA should assume the key role by assisting the EU Member States (and relevant institutions) to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents, in relation to the security of network and information systems. Moreover, ENISA should support the development and enhancement of the Member States and the EU computer security incident response teams (CSIRTs). Finally, ENISA should promote the exchange of best practices between all Member States.

The Regulation sets out the cybersecurity certification framework. The goal is to enhance the level of cybersecurity in the Union by providing a mechanism to attest the ICT products, processes and services. This attest should comply with advanced determined security requirements. This is

[6] https://eur-lex.europa.eu/eli/reg/2019/881/oj

particularly important for the purpose of protecting the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data and accompanied functions and services.

The EU Member States should establish national cybersecurity certification authorities. These bodies should monitor and enforce the obligations of manufacturers or providers of ICT products, processes or services. In addition, national cybersecurity certification authorities should handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates.

Finally, the European Cybersecurity Certification Group (ECCG) should be established. This body should ensure the consistent application of the European cybersecurity certification framework and monitor the consistent implementation of the cybersecurity program. Also, ECCG should advise and assist the European Commission in matters related to certification frameworks and cybersecurity programs.

The Cybersecurity Act complements the GDPR by providing details related to implementation of appropriate security measures. It also works in conjunction with the NIS Directive to protect critical national infrastructure. However, while the NIS Directive applies only to specific operators, the Cybersecurity Act encourages all businesses to invest in cybersecurity.

2.2.2.4 Ethical issues

Law prescribes what must, can or cannot be done. However, ethics goes beyond what is stipulated by law. Law is based on certain ethical values and it supports fundamental rights and freedoms (Hijmans & Raab, 2018, 1[7]). Moreover, 'laws come and go; the ethics stays'[12].

There is an increasing trend of ethical discussions on data, including personal data. It comes as no surprise due to rapid technological development. New technologies could improve security measures that protect data. However, aspirations towards high security might also misuse information and subsequently jeopardize personal privacy. For instance, the application of a surveillance system in public places might be at cost of our personal privacy. Thus, it would not be wrong for two opposite conclusions to be both correct. Therefore, it is quite important to assess the nature of data intended to be processed as well as the consequences of data processing. Whoever processes data should ensure that relevant legal framework(s) are respected. This is particularly important when sensitive data is processed.

Data processing generates accountability of the entities that processes the data. The essence of the accountability principle lies in the obligation to be compliant with all other data protection principles and to be able to demonstrate it. These requirements are part of the legal responsibility, and it is important to underline that accountability goes beyond legal responsibility. Legal responsibility concerns who is supposed to do what, and it may include legal consequences for the performance or non-performance of duties and tasks that are regulated by certain legislation (such as GDPR).

[7] Hijmans, H., & Raab, C. (2018). Ethical Dimensions of the GDPR. In *Commentary on the General Data Protection Regulation*. Edward Elgar. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3222677

Accountability implies that a responsible agent attempts to respect other principles and demonstrates its compliance, even when this is not explicitly required by law (Hijmans & Raab, 2018, 10[7]). Therefore, accountability imposes both - obligation to behave in a certain way; and preparedness to explain the behavior to relevant stakeholders (e.g. public bodies in a form of regulatory instances as well as individuals).

Processing of data must be limited to the specified purposes and appropriate security measures should be applied. In cases where measures such as anonymization or pseudonymization are not applied, an explanation is needed. This is necessary (inter alia) to make an informed decision about personal data processing. However, there are situations that individuals cannot decide on processing their personal data due to reasons that override their freedoms and rights. The principle of fairness requires an assessment of how processing will affect individuals. If processing negatively affects an individual, then processing will be unfair. However, even unfair processing could be legitimate (e.g. personal data may be collected by tax authorities about an individual who has not paid taxes).

One of the most important ethical issues concerning data processing and protection is transparency. Transparency is not only about providing access to information. It also refers to ways about how information is provided. Delivering info about data processing before processing starts affects individuals' choice concerning the protection of their personal privacy. Therefore, one of the foundations regarding transparency refers to providing information about data processing in a timely manner. A timely manner is a quite general construction, and its specification is context-based.

Transparency means that information about processing activities should be clear, concise, easy to understand and provided in an accessible manner. These requirements are general, and their practical form will depend on a particular context. In practice, that means when data is transferred from one to another country such transfers must comply with the laws of the country in which the data was collected and also facts about the transfer are properly communicated. Also, detailed information on the informed consent procedures related to the processing of personal data must be provided (e.g. in a language and terms understandable by the participants). Moreover, if data processing involves profiling, the data subjects shall be informed of the existence of the profiling, its possible consequences, and how the fundamental rights of the research participants will be safeguarded.

Entities that process data (and particularly personal data) should designate a Data Protection Officer (DPO) – a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with relevant regulation. DPO may evaluate the ethics risks related to data processing activities. This should include an opinion on whether or not a data protection impact assessment should be conducted. The opinion, the risk evaluation and, if applicable, the data protection impact assessment should be conducted. Therefore, accountability includes a risk-based approach. In other words, whoever processes data should assess risks related to the processing. In that way, ethical judgements are made.

2.2.3 SC security standards (families of ISO2800x)

ISO 28000[8] was prepared by Technical Committee ISO/TC 8, Ships and marine technology, in collaboration with other relevant technical committees responsible for specific nodes of the Supply Chain.

This International Standard has been developed in response to demand from the industry for a security management standard. Its ultimate objective is to improve the security of SCs. It is a high-level management standard that enables an organization to establish an overall SC security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since SCs are dynamic in nature, some organizations managing multiple SCs may look to their service providers to meet related governmental or ISO SC security standards as a condition of being included in that SC in order to simplify security management, as illustrated in *Figure 3*.

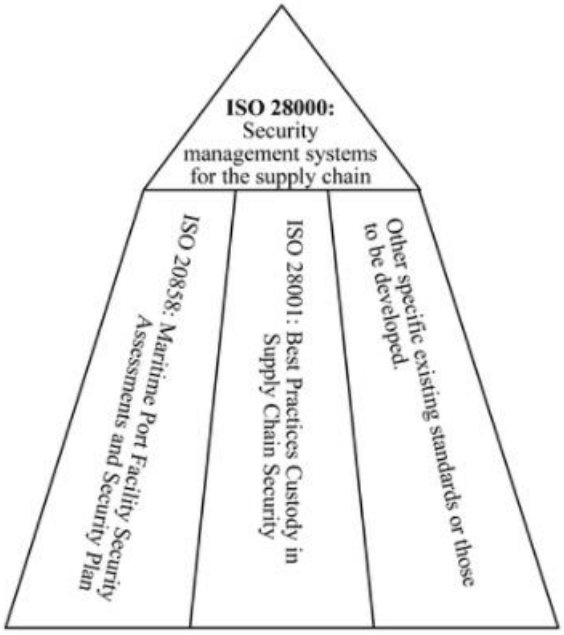


Figure 3 - ISO28000 overview.

This International Standard is intended to apply in cases where an organization's SCs are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with an International Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system with this International Standard may be verified by an external or internal auditing process.

[8] https://www.iso.org/standard/44641.html

The standard focuses on actively managing and reducing risks. Critical security aspects in the supply chain can include financial aspects, manufacturing, information management and logistics, storage in transit and warehousing of goods.

This International Standard is based on the ISO format adopted by ISO 14001:2004 because of its risk-based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this International Standard. It is not the intention of this International Standard to duplicate governmental requirements and standards regarding SC security management to which the organization has already been certified or verified to comply with. Verification may be by an acceptable first, second, or third-party organization.

This International Standard is based on the methodology known as Plan-Do-Check-Act (PDCA), described as follows.

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.
- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve the performance of the security management system.

Moreover, this International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the SC. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that have an impact on SC security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along with the SC.

Finally, this International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or SC that wishes to:

1. establish, implement, maintain and improve a security management system;
2. assure conformance with stated security management policy;
3. demonstrate such conformance to others;
4. seek certification/registration of its security management system by an Accredited third party Certification Body;
5. make a self-determination and self-declaration of conformance with this International Standard.

There are legislative and regulatory codes that address some of the requirements in this International Standard.
It is not the intention of this International Standard to require duplicative demonstration of conformance.
Organizations that choose third-party certification can further demonstrate that they are contributing significantly to SC security.

2.2.4 Risk Management standards (families of ISO2700x)

ISO27000[9] is a set of International Standards that regulate Information Security Management Systems (ISMS). They are used to manage information security risks and controls within an organization. The central principle of the ISO27000 set of standards is to bring information security under overt management control. These standards help organizations to develop and implement a framework for managing the security of information assets as well as to prepare themselves to assess their ISMS. ISO27000 contains vocabulary and requirements for ISMS, Code of practice for information security management, ISMS implementation guidance, measurement for ISMS, information security risk management, and guidelines for ISMS auditing.

ISO27000 family of standards defines requirements for an ISMS, provide direct support, and detailed guidance for the Plan-Do-Check-Act (PDCA) processes and requirements. Sector-specific guidelines are also addressed by ISMS family.

2.2.5 SC risk assessment methodologies & Tools

Supply Chain risk management (SCRM) can be considered the cross-section of Supply Chain management and risk management [13] aiming to minimize the level of uncertainty on the supply chain performance and provide adequate solutions to undertake [14]. SCRM can be identified as the process of applying strategies to capture, estimate, prioritize and mitigate risks [15]. The literature reviews a variety of SCRM definitions focusing on different aspects [16][17][18][9].

Supply Chain Service performance can be jeopardized by common threats (i.e., traditional cyber attack, cyber piracy, espionage, sabotage, etc.) and new rising threats (i.e., APTs, ransomware, botnet) capable of being supported by multiple sophisticated threat agents. In addition, the advent of emerging technologies (i.e., digital twins, IoT, Swarm Intelligence-based techniques, Big Data, adversarial learning techniques, etc.) has posed novel threats to the SC ecosystem. Taking into account the analysis of the latest cyber threat landscape reports coming from dominant EU cybersecurity standardization bodies [19], it can be deduced that SC sophisticated cyberattacks have become a new emerging alarming scenario.

Digital Supply Chains consist of interconnected dispersed nodes, changing dynamically and impeding the chance to adjust to the tremendously evolving threat landscape[10]. Therefore, a combination of both proactive/preventive approaches to size the robustness and reactive strategies to improve the agility can be utilized to address this challenge [20][21].

[9] https://www.iso.org/standard/73906.html

[10] NIST “Case studies in Cyber Supply Chain Risk Management” (2020). Online available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-1.pdf , accessed on 24-2-2021

Additional guidelines have been provided by ENISA on hot SC topics, such as IoT security to illustrate indications and good practices according to existing standards and research[11]. ENISA has also provided a report on guidelines for maritime cybersecurity[12] in an attempt to help port operators adopt good practices for cyber risk assessment, regardless of the risk assessment methodology they have chosen to use.

Considering the multi-level specificities of the modern ICT SCs (i.e. sectoral, cross-sectoral) SCRM strategies [15] should be used to minimize the existence of vulnerabilities and the potential of loss within a Supply (SC) promoting business continuity and security maintenance. Thus, for managing cybersecurity risks that originate from supply chains, organizations need to understand their supply chains, including multiple layers of sub-suppliers[13].

According to SCS stakeholder interviews[10], SCS operators collaboration can facilitate organizations to avoid some of the common pitfalls, early in the maturity journey[10][22]. NIST SP 800-161[14] provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks introducing a multi-tiered, SCRM-specific approach.

In principle, choosing an effective method and a proper tool for risk analysis and risk evaluation proves to be complicated. In recent years, a number of concepts, algorithms and tools have evolved from research, specially designed to protect the IT infrastructure and related systems, mostly utilizing quantitative risk assessment methods based on monetary costs [23]. There are remarkable examples of semi-quantitative risk assessment approaches, such as the Fault Tree Events Analysis [24], the OBEST object-based event scenario tree that combines features of event tree analysis and Monte-Carlo discrete event simulation, which is able to perform a deep analysis on the uncertainty subjects [25]. The difficulty to obtain precise and reliable figures for a quantitative risk assessment is the main reason why the German Federal Office of Information Security (BSI) recommends qualitative risk assessment (e.g. based on risk scoring matrices, etc.) instead of quantitative risk assessment, although the need for the latter has clearly been recognized [26].

In Boiko et al. [27] a qualitative research method is presented for analysing the Supply Chain process and identifying the most effective strategies for information support in Supply Chain environments to eliminate cyber risks. Nevertheless, the qualitative risk assessment does have the appeal of efficiency and is easy to communicate and explain to stakeholders; however, there are no commonly accepted ratings for safety and security that would apply as a standard.

[11] ENISA(2020). “Guidelines for Securing the Internet of Things”. Online available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things , accessed on 24-2-2021

[12] Cyber Risk Management for Ports - Guidelines for cybersecurity in the maritime sector. ENISA, 2021, [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports. Accessed: March 15, 2021

[13] Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2021). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (No. NIST Internal or Interagency Report (NISTIR) 8276). National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8276

[14] NIST SP 800-161 (2015). “Supply Chain Risk Management Practices for Federal Information Systems and Organizations“. Online available: http://dx.doi.org/10.6028/NIST.SP.800-161, accessed on 24-2-2021

Additional complications arise from the need to map the existing infrastructure of an organization onto a fixed terminology with which the chosen risk assessment method works.

There is a variety of past, well-known, outstanding risk management methods and risk assessment tools, such as the ISO 27001-, 27005- and 31000- compliant "EBIOS" method used by ANSSI, the "OCTAVE" method [28], a priori distribution of subjectively estimated probabilities utilizing the Bayesian approach, the Magerit open methodology for risk management and the Mehari risk analysis method [29]. Most of them adopt the commonly known rule "risk = probability x potential damage" [30]. The "BowTie"[15] is a traditional widely used qualitative risk analysis method. The "CORAS" well-known method [31] allows the incorporation of several different risk assessment processes the recognition of the probability of an attack is done a priori to any risk assessment and not automatically. CRAMM [32] is a risk analysis method for all types of information systems and networks, identifying security requirements, detecting contingency requirements and proposing possible solutions. The STORM-RM [33] is a collaborative and multi-criteria risk management ISO27001-based methodology promoting organization users to participate in the various risk assessment and treatment phases combining risk computation with the AHP algorithm. The Collaborative Cyber/Physical Security Management System (CYSM) approach [34] explores the significant criticality of ports' infrastructure and the complexity of the interrelationships among the internal and external systems and infrastructures.

Oliveira et al.[35] provides an extended research on SCRM profile works of the last fifteen years to discover key-players in the SCRM research field and conclude that there is a lack of consensus among authors undertaking a description of SCRM steps. In addition, there is limited work on developing stable SCRM solutions of well-defined process descriptions from a managerial perspective. On this account, there is a compelling need for continuous improvement in the SCRM cyber plane in terms of investigating solutions capable of holistically and dynamically assessing an organization's exposure to Cyber Supply Chain threats and taking into account cross-functional risks [15]. A set of key practices that any organization of any size, scope, and complexity can use to manage cybersecurity risks associated with their supply chains is provided in Cyber Supply Chain Risk Management (C-SCRM) approach[10]. Ensuring cyber-resilience seems to be a critical capability that needs to be improved in order to successfully identify, assess, and mitigate cyber supply chain risks. This can be achieved through creating explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions. Organizational accountability is a principle that is highlighted in this report and could be guaranteed through a C-SCRM program. For this reason, it is critical to know by whom the data and infrastructure are accessible. Security requirements should be communicated not only to suppliers, but also to suppliers' sub-suppliers. The C-SCRM approach also proposes establishing protocols for vulnerability disclosure and incident notification for better managing cyber supply chain risks.

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers [36] building strategies between two or more players which aim to maximize their payoff and minimize their loss. The application of game theory (i.e. the Minimax approach) in risk management elegantly aims to presume the attacker's behavior to be optimal in the most unfavorable way for its victim. The appeal of game-theory lies in the fact that, no matter how the adversary actually behaves, it provides the worst-case scenario and, in this manner, a

[15] https://www.researchgate.net/publication/298916210_The_bowtie_method_A_review

sharp assurance for the risk can be provided [37]. Thus, game theory has gained ground in the field of cryptography and the security of IT infrastructures in the past years.

There are various strategies in the literature which give a guaranteed payoff under any behaviour of the adversary, regarding scalar and multi-dimensional payoffs [38][39]. Cox (2005) [40] provides a clear connection between game theory and risk analysis claiming that they are deeply complementary and mutually reinforcing. He considers that risk analysis can support game theory by providing probabilities of different consequences for pairs of attacker-defender strategies. Conversely, game-theoretic methods and concepts can improve current risk analyses of adversarial actions. Rajbhandari and Snekkenes in their research work [41] explain how game theory can interact with the classical risk management. Specifically, they provide a full description on how the steps of the classical management model ISO/IEC 27005 can be mapped and utilized in a game-theoretical model.

Responses to SC risks are in a variety of cases supported by payoffs and risk mitigation strategies as already presented indicatively. Ceryno et al in their research work [42] state that modern risk models require validation upon real cases and a deeper risk analysis and risk treatment exploration. They continue that there is a lack of research relying on empirical data obtained from face-to-face interviews of SC stakeholders and a unanimous SCRM definition is not yet provided.

Methodologies for dependency modelling, simulation and analysis have been recently categorized in the following broad categories [43]: (i) empirical approaches, (ii) agent-based approaches, (iii) system dynamics-based approaches, (iv) economic theory based approaches, (v) network based approaches, and (vi) others. Empirical methods focus on the impact assessment and/or the risk related with the dependencies between Cis [44] and their potential cascading effects. A limitation of empirical approaches is the difficulty in capturing statistical data related to the likelihood of the examined threats. Network-based approaches [45][46] focus on the flow of products or services exchanged between CIs and try to model this flow based on graphs. Other methods can be categorized as hybrid, including characteristics of both empirical and network-based methods [47]. A key role in the analysis of such various methods, mainly empirical, network-based and hybrid ones has the graph theory.

Attack Trees or Attack Graphs approaches are well-established, promoting threat scenarios during the risk assessment process[16]. In recent years, attack models are a primary tool in risk assessment of SC heterogeneous and interconnected systems (i.e. SCADA, AIS systems). They are conceptual diagrams providing possible conceivable attacks, where the root of the tree illustrates a potential exploit and the leaves provide the various actions to achieve that goal aiming to point out optimal attack paths (kill chains)[17]. Shin et al. in their respective research work [48]

[16] Bodeau D.,J., McCollum, C., D., Fox, D.,B. (2018) "Cyber Threat Modeling: Survey, Assessment, and Representative Framework", The Homeland Security Systems Engineering and Development Institute (HSSEDI) & MITRE Cooperation. Available online: https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf (Accessed on 19 March 2021)

[17] Nagaraju, Vidhyashree, Lance Fiondella, and Thierry Wandji (2017). “A survey of fault and attack tree modeling and analysis for cyber risk management”. In: 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–6.DOI: 10.1109/THS.2017.7943455. URL: http://ieeexplore.ieee.org/document/7943455/

utilize the theory of random graphs to model interdependent networks and provide a theoretical analysis of the cascading effects.

Most research work of cascading failures in SC networks refers only to single network models because it is difficult to represent real-world multiple agent network systems of SCs [49]. A remarkable research work on these grounds is the Medusa approach [50][51] proposing multi-order dependencies between stakeholders involved in the maritime supply chain, where cyber threats are estimated in terms of scrutinizing the cascading scenarios modelled by dependency graphs. The efforts described above can be a starting point to leverage research on the impact of risks in supply chains. Notwithstanding, there is still a strong need to investigate methods that focus on SC risk impact analysis and how to facilitate SC stakeholders better comprehend cascading effects of potential attacks in a vertical manner.

3. EU Certification

The general definition and requirements (policy, legal, standards, methodologies, technical) regarding the security certification will be reviewed in this section.

3.1 Security Certification - EU requirements

3.1.1 Cybersecurity Act - The European certification legal instrument

The EU Cybersecurity act[18] aims to coordinate a number of certification schemes (e.g., ISO 15408/18045, NCSC) in order to boost the digital single market, scale up the response to cyber-attacks, improve cyber resilience and increase the trust for consumers of ICT products, services and processes within the union.

The Cybersecurity Act provides a framework for certification schemes based on the following standards: ISO/IEC 15408, ISO/IEC 18045 and ISO/IEC 17065. These complementary standards constitute the basis for all cybersecurity evaluation schemes in the cybersecurity act.

According to the cybersecurity act, ENISA, the European Union Cybersecurity Agency, is assigned a central role to establish, support and implement the EU cybersecurity certification framework. The framework indicates the following requirements for each certification scheme:

- A certification scheme is designed to achieve a number of security objectives including confidentiality, integrity, availability, accountability, non-repudiation of stored, transmitted and processed data. Design goals of the scheme also include post-incident recovery, business continuity and identifying known vulnerabilities and dependencies.
- A certification scheme may specify one or more assurance levels including basic, substantial and high. These assurance levels shall be associated with the risk level related to the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.
- A certification scheme may allow for conformity self-assessment to those ICT related products, services and processes that present a low risk corresponding to assurance level ‘basic’.
- A certification scheme includes a number of other elements such as: scope (products, services and processes), references to standards (international, European and national standards), evaluation criteria, conditions for marks or labels, rules concerning vulnerability disclosure, validity period, conditions for mutual recognition with third countries.
- A certification scheme provides supplementary cybersecurity information. It includes the guidance and recommendations to assist end-users with the secure configuration, availability of cybersecurity-related updates, and a reference to online repositories listing publicly disclosed vulnerabilities that are related to ICT products and services.

[18] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

In the context of the Cybersecurity Act, Supply Chains are recognized as “global” and the introduction of certification schemes should lead to reducing market fragmentation.

Furthermore, the Cybersecurity act gives tasks and provides resources to ENISA in order to assist EU member states in dealing with cyber-attacks. This will be accomplished by enhancing the EU Member States with an efficient information sharing through the network of Computer Security Incident Response Teams (CSIRTs) and raising cybersecurity awareness through exercises and trainings.

3.1.2 Security Certification standards addressing EU requirements

EU Cybersecurity certification requires formal evaluation of products, services and processes against a defined set of criteria in order to provide assurance that the products comply with specified requirements and standards. Each standard specifies one or more level(s) of assurance (basic, substantial or high), based on the level of risk associated with the intended use of the product, service or process.

ISO/IEC 15408[19] and ISO/IEC 18045[20] are a pair of international standards for IT systems security evaluation and certification. ISO 17065[21] International Standard focuses on requirements for the competence, consistent operation and impartiality of the certification bodies evaluating and certifying products, processes and services.

CYRENE focuses on creating solid links and significantly influencing a number of initiatives in the areas of cybersecurity, data protection and software standardization. Specifically, CYRENE combines ISO standards in order to build a Conformity Assessment Process for ensuring the security and resilience of Supply Chain services.

3.1.2.1 ISO/IEC 15408

ISO/IEC 15408 is a guide for the development, evaluation and/or procurement of IT products with security functionality. It establishes the general concepts of IT product security evaluation, specifying the requirements for the security functions of IT systems and the assurance measures applied to them during a security evaluation. The standard consists in three parts.

The first part, i.e., ISO/IEC 15408-1 [52], provides an overview of all parts of ISO/IEC 15408 standard. In more details, it defines the general concepts and the principles of IT security evaluation. It establishes the core concept of the Target of Evaluation (ToE) scheme and refers to the evaluation criteria. It focuses on the basic security concepts necessary for IT products evaluation. Also, it defines the permitted functional operations for the functional and assurance

19 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408

20 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-18045

21 https://www.iso.org/standard/46568.html

components, which are defined into ISO/IEC 15408-2 and ISO/IEC 15408-3. Finally, it describes the key concepts of protection profiles (PP), it gives guidelines for the specification of Security Targets (ST) and the organization of the components throughout the model.

The security functional requirements, which are described in ISO/IEC 15408-1, establish a comprehensive catalogue of security functional components that serve as standard templates. These templates are described analytically in ISO/IEC 15408-2 [53] and are a standard way of expressing the functional requirements for ToEs (Targets of Evaluation). The templates are organized using a hierarchical structure of classes, families and components. ISO/IEC 15408-2, also, provides guidance on specifying custom security requirements, where no suitable predefined security functional templates are in place.

Last, the ISO/IEC 15408-3 [54] describes a set of assurance components, which serve as standard templates for expressing and covering ToEs assurance requirements. The assurance components are organized into a set of components, families and classes. Also, ISO/IEC 15408-3 presents the Evaluation Assurance Levels (EALs), which define a scale for rating ToEs assurance levels.

3.1.2.2 ISO/IEC 18045

ISO/IEC 18045 [55] is a companion standard to the evaluation criteria for IT security defined in ISO/IEC 15408. This standard defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the corresponding criteria and the evaluation evidence. The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions, i.e. sponsors and/or developers. It is considered as a “companion” document, which is helpful mainly for security professionals, which are involved in evaluating compliance with ISO/IEC 15408. Finally, this standard does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is no generally agreed guidance yet.

3.1.2.3 ISO/IEC 17065

The overall goal of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfills specified requirements. ISO17065 standard [56] contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies. Certification bodies operating under this International Standard do not have to offer all types of products, processes and services certification. In this International Standard, the term “product” can be read also as a “process” or “service”.

This International Standard specifies requirements that should be met to ensure that certification bodies operate certification schemes in a competent, consistent, and impartial manner. This International Standard can be used as a criteria document for accreditation or peer assessment or designation by governmental authorities, scheme owners and others. The requirements should be considered as general criteria for certification bodies operating product, process, or service certification schemes. Of course, they may have to be adjusted and/or empowered when specific industrial or other sectors make use of them.

3.1.3 The European Cyber Security Certification Schema (EUCC)

Securing network and information systems in the European Union has been deemed as a key objective in an effort to keep the EU online economy functional and secure. ENISA[22] contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for tomorrow's cyber challenges.

The EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.

This scheme will improve the European Union Internal Market conditions for ICT products, and as a result also have positive effects for ICT services and ICT processes relying on such products.

The purpose of the EU cybersecurity certification (EUCC) framework is to establish and maintain trust and security in cybersecurity products, services and processes. Drawing up cybersecurity certification schemes at EU level aims at providing criteria to carry out Conformity Assessments to establish the degree of adherence of products, services and processes against specific requirements. Users and service providers alike, need to be able to determine the level of security assurance of the products, services and processes they procure, make available or use.

The EU cybersecurity certification framework lays down the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more level(s) of assurance (basic, substantial or high), on the basis of the level of risk associated with the envisioned use of the product, service or process. It serves the purpose of providing notice and assurance to users about the level of conformity against stated requirements. EU cybersecurity certification schemes serve as the vehicle to convey such requirements from the EU policy level to the industry service provision level and further to the users and conformity assessment bodies.

Cybersecurity certification requires the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance; as such cybersecurity certification plays a key role in increasing trust and security in products, services and processes.

As per Article 52.6 A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security

[22] ENISA EUCC Cybersecurity Certification: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.

A European cybersecurity certification scheme may specify several evaluation levels depending on the rigor and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components. Certification under this scheme shall cover the assurance levels 'substantial' and 'high' of the CSA.

A user of certified products or an applicant to certification shall decide against which security objectives he/she decides to evaluate the ICT product(s) and select the applicable requirements, either in a Protection Profile or a Security Target of the individual ICT product. ENISA may provide associated guidance for this selection, based on risk assessment methods or tools.

3.1.4 R&D certification projects and EU initiatives

The European Commission declared cybersecurity as a top priority of the digital and connected Europe and cybersecurity presents an important part of the Commission's research and innovation funding framework programmes, Horizon 2020 and its successor Horizon Europe. CYRENE will make a direct contribution to the strengthening of the EU's cybersecurity capacity through collaboration with the winning pilot projects of the 2018 and 2019 Horizon 2020 cybersecurity call. In this section, we have listed several projects dealing with various aspects of cybersecurity in supply chains.

FISHY[23] is one of the projects aiming to design and develop a solution for cyber resiliency provisioning supporting security assurance and certification management, trust management, data and privacy management and the proper orchestration of their related functional components. An evidence-based security assurance and certification methodology identifying security claims and metrics will be developed which draws similarity to the CYRENE approach. FISHY will make validation and demonstration of the framework on three use cases from different sectors, including agriculture, manufacturing and transportation. Taking into account that CYRENE will also validate its Conformity Assessment process on pilot use cases dealing with the

[23] https://fishy-project.eu/

manufacturing and transportation sector, those use cases from the FISHY project may be used as external Supply Chain pilot scenarios.

Most companies developing ICT solutions require the integration or synergy of other ICT components developed by third parties. This can represent a high security risk, making the verification of potential vulnerabilities more difficult. The EU-funded BIECO project[24] is working on a holistic framework composed of a set of tools and methodologies that will address the challenges related to vulnerability and risk management, resilience and auditing of complex systems on the level of the ICT supply chain. On the other side, CYRENE will improve the trust of the consumer through the development of an innovative certification schema and a clear and structured Conformity Assessment across all levels of a Supply Chain provision.

Cloud computing is an essential element of innovative economies. Despite trust-building efforts, the adoption of cloud computing is limited. A lack of security and transparency is the reason for the slow uptake. European cloud service providers (CSPs) still face multiple challenges for certifying their services. The EU-funded MEDINA project[25] will work to counter this trend. It will propose a framework for achieving a continuous audit-based certification for cloud service providers, complying with the EU Cybersecurity Act. The project will also address the definition and assessment of technical and organizational measures, security testing, machine-readable certification language and audit evidence management. Medina framework will be based on European Cybersecurity Certification Scheme for Cloud Services (EUCS). Currently certification schemes are expressed using natural language so MEDINA proposes to transform this certification language into a machine-readable expression. Results of this effort may be utilized on the schema which will be developed inside the CYRENE approach and which is also based on EUCC as that EUCS schema.

Parallel with the demand for autonomous Cyber-Physical Systems (CPSoS), grows the need for advanced certification mechanisms that can improve their security posture without compromising their safety. Existing validation methods require exhaustive offline testing of every possible state scenario prior to fielding the system. The EU-funded ASSURED project[26] is introducing an innovative, formally verified runtime assurance framework for securing CPS Supply Chains. The main objective of the project is to develop highly automated middleware for the secure configuration, management of edge devices, processes and safety-critical software components. The ASSURED project will identify and implement a reactive, runtime risk assessment model which will enable the dynamic assessment and forecast of individual, cumulative and propagated risks, taking into account the representation of assets along with their dependencies, the associated threats and vulnerabilities and the potential cascading effects. The ASSURED framework will mainly focus on certification of supply chains including IoT devices while CYRENE will take into consideration certification of individual devices but also, certification of whole infrastructure and assets of the Supply Chain as well certification of business perspectives of Supply Chain.

[24] https://www.bieco.org/

[25] https://cordis.europa.eu/project/id/952633

[26] https://www.project-assured.eu/

CONCORDIA[27] addresses the current fragmentation of security competence by networking diverse competencies into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Center. CONCORDIA is trying to build a community of strong cooperation between all stakeholders, understanding that all stakeholders have their KPIs, bridging among them, and fostering the development of IT products and solutions along the whole supply chain. Technologically, it projects a broad and evolvable data-driven and cognitive E2E Security approach for the ever-complex ever-interconnected compositions of emergent data-driven cloud, IoT, and edge-assisted ICT ecosystems.

The SPARTA[28] proposal brings together a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Strongly guided by concrete and risky challenges, it will set up unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centers. Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry. CYRENE will collaborate with CONCORDIA and SPARTA for knowledge transfer as well as to strengthen the EU's cybersecurity capacity.

CyberSec4Europe[29] aims to boost defenses within the vertical sectors of digital infrastructure, finance, government, transport, health, and smart cities. The project utilizes practical experience gained during CyberSec4Europe to develop a specialized roadmap and recommendations for the implementation of network competence. CyberSec4Europe project has identified seven key research and innovation demonstration cases covering a wide spectrum of prominent research areas in both the public and private sectors. Among the demonstration cases are Supply Chain security assurance and maritime transport which are of special interest to CYRENE.

ECHO[30] is one of the projects supported by the European Commission with the objective of connecting and sharing knowledge across multiple domains to develop a common cybersecurity strategy for Europe. The project will develop a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents. One of ECHO's main objectives is the development of ECHO Security Certification Scheme: Development of sector specific security certification needs within the EU Cybersecurity Certification Framework from ENISA. CYRENE will make key advances comparing to ECHO. Specifically, it will contribute to a comprehensive cybersecurity conformity assessment framework for SCs viewed as a whole, i.e., a complex system with business, infrastructure, and individual devices levels.

The secure SerIoT platform is a key step that can be used to implement secure IoT platforms and networks anywhere and everywhere. The SerIoT project[31] develops, implements and tests a

[27] https://www.concordia-h2020.eu/

[28] https://www.sparta.eu/

[29] https://cybersec4europe.eu/

[30] https://echonetwork.eu/

[31] https://seriot-project.eu/

generic IoT framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network. The aim of the SerIot platform is to recognize suspicious patterns, evaluate them and finally to decide on the detection of a security leak, privacy threat and abnormal event detection, while offering parallel mitigation actions that are seamlessly exploited in the background. Large-scale pilots can test SerIoT technology in various use cases including intelligent transport and surveillance, flexible manufacturing within Industrie 4.0 and other emerging domains such as food chain & logistics, m-Health (both at Home & in Hospitals business scenarios) and energy (smart grid). CYRENE will consider security solutions developed in SerIoT, specifically regarding the protection of IoT devices and communications, as these are important sub-components of the CYRENE Conformity Assessment framework.

In addition, there exists a set of EU bodies and initiatives related to cybersecurity improvement and certification schemes development, that are of interest.

DIGITALEUROPE[32] represents a regulatory environment, the leading trade European association, that concerns digitally transforming industries. Its goal is to contribute to both the development and implementation of relevant EU policies, as well as to shape industry policy positions on relevant legislative matters. It implies a wide variety of businesses, corporations and national trade associations and partnerships with European institutions. One of its policy areas is cybersecurity, with a focus on the proposed Cybersecurity Act, with the aim to create a harmonized EU market for cybersecurity certification schemes, and on the implementation of the Directive on the security of network and information systems - the NIS directive[33]. The NIS directive is the first representative of EU cybersecurity legislation, with the aims to enhance cybersecurity across Europe and create and strengthen a Computer Security Incident Response Team (CSIRT) Network. The NIS directive is a central deliverable within the EU Cyber Security Strategy, that tends to harmonize a framework for evolving of three different aspects of cybersecurity.

The Digital Agenda for Europe (DAE)[34] defined the key enabling role that the use of ICTs had to play in order to make Europe succeed in its goals. The Digital Market Strategy is built on three pillars: providing better access for consumers and businesses to digital goods and services across Europe, creating the right conditions for digital networks and services to flourish, and maximizing the growth potential of the digital economy.

The European Cyber Security Organization (ECSO)[35] is a fully self-financed non-for-profit organization. ECSO is the privileged partner of the European Commission for the implementation of the Cybersecurity Public-Private Partnership (PPP), and it also unites European Cybersecurity stakeholders. The main aims of ECSO include the coordination of the development of the European Cybersecurity Ecosystem, the support to protecting European Digital Single Market and the contribution to the advancement of European digital sovereignty and strategic autonomy. ECSO has collaborations with different European Agencies and Bodies, such as ENISA.

[32] https://www.digitaleurope.org/

[33] https://enisa.europa.eu/topics/nis-directive

[34] https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe

[35] https://ecs-org.eu/

Regarding Public Private Partnerships (PPPs), the representatives that are relevant as collaborators include: Big Data Value Association (BDVA)[36], ARTEMIS industry association[37] and ECSEL Joint association[38].

European Competence Network of Cybersecurity Centers of Excellence[39] strives to retain and develop the cybersecurity technological and industrial capacities of EU. Its goals include securing EU Digital Single Market and strengthening and sustaining the cybersecurity competence of Europe. It comprises four EU pilot projects: CONCORDIA, ECHO, SPARTA and CyberSec4Europe, with the aim to prepare the European Cybersecurity Competence Network.

The ENISA[40] is oriented towards achieving a high common level of cybersecurity across Europe. ENISA contributes to EU cyber policy and cybersecurity certification schemes, and also plays a key role in supporting the collaboration between cybersecurity stakeholders and institutions and agencies. The EU Cybersecurity Act[41] establishes an EU-wide cybersecurity certification framework, and also strengthens the role of ENISA, as it grants a permanent mandate to the agency. ENISA has also announced the creation of the Stakeholders Cybersecurity Certification Group (SCCG)[42]. Its aim is to focus on strategic issues regarding cybersecurity certification, to assist in preparation of the Union rolling work programme and also to create market-driven certification schemes.

The regulation on electronic identification and trust services for electronic transactions in the internal market - eIDAS Regulation (Regulation (EU) N°910/2014)[43] provides a predictable regulatory environment for enabling secure and seamless electronic interactions. It creates a European internal market for electronic trust services.

The GSMA IoT Security Guidelines and Assessment[44] represents a European standard organization. It is oriented towards a set of IoT Security Guidelines, supported by an IoT Security Assessment scheme. It promotes best practices for the security of IoT services and a mechanism for security measures evaluation.

[36] https://www.bdva.eu/

[37] https://artemis-ia.eu/

[38] https://www.ecsel.eu/

[39] https://cybercompetencenetwork.eu/

[40] https://enisa.europa.eu

[41] https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

[42] https://ec.europa.eu/digital-single-market/en/stakeholder-cybersecurity-certification-group

[43] https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[44] https://www.gsma.com/iot/iot-security/iot-security-guidelines/

CEN-CENELEC-ETSI Cyber Security Coordination Group (CSCG)[45] is dedicated to provide strategic advice in the field of IT security, Network and Information Security (NIS) and cybersecurity (CS). It was created in 2011. In 2016, it was converted to CEN-CENELEC Focus Group on Cybersecurity. The aim is to prepare a European roadmap on cybersecurity standardization, while providing active support on global initiatives on cybersecurity standards.

3.1.5 Examples of Certificates

A certificate contains the most relevant information for the identification of the product and the assurance level obtained. It should include a unique identifier established by the issuer of the certificate, information related to the certified ICT product and its manufacturer or provider, information related to the evaluation and certification of the ICT product.

The certificate is only related to the cybersecurity certification requirements of the product at the moment of issuance of the certificate. It is not related to the product itself. It only expresses that the cybersecurity related material and information of the product meets the requirements of this certification related information.

There may exist different options to claim that a product, system or services complies with cybersecurity certification requirements. Some examples of certificates can be:

- self-declaration without any assessment,
- self-declaration based upon a self-assessment or a voluntary third-party assessment,
- accredited certificate based upon a third-party assessment (in-house or external),
- certificate issued by a National Authority based upon a third-party assessment (external).

Common Criteria certifications enable an objective evaluation to validate that a particular product or system satisfies a defined level of robustness. It not only provides assurance that the process of specifying and implementing a secure solution has been rigorously conducted, but also that the solution has reached the expected level of trust for final use.

In order to obtain Common Criteria certification, vendors have to complete several steps. First, they must provide a Security Target description including an overview of the product and its security features as well as an evaluation of potential security threats and a self-assessment. Second, organizations must find an independently-licensed laboratory to evaluate their product and determine if it meets security properties to a satisfactory level. If the product passes the evaluation, certification of the security properties of the product is issued by various Certificate Authorizing Schemes. These certificates are recognized by all the members of the CCRA and groups such as SOG IS[46].

[45] https://www.cencenelec.eu/standards/Sectorsold/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

[46] https://sogis.org/

Various examples of certificates issued by a National Authority with claims of compliance against Common Criteria may be found online[47]. One of them relates to mobile ID software solution developed by company Thales[48]. This software enables citizens to securely log on to public and private eServices and to smoothly prove who they are online while guaranteeing data protection and privacy. The Gemalto Mobile ID software has demonstrated a level of resistance to the most advanced security penetration tests against mobile applications. Security tests on the Gemalto mobile ID software were performed by the internationally renowned testing laboratory "Brightsight" under the supervision of the NSCIB (Netherlands Scheme for Certification in the Area of IT Security), in cooperation with of The Netherlands Ministry of Interior and Kingdom Relations.

3.2 Conformity Assessment (CA)

3.2.1 Basic Concepts and Requirements

The basic concept of the Supply Chain Conformity Assessment process is based on the general frame, within the scope of the conformity definition, which contains several abstract categories based on the EU Commission single market for goods regulation[49] . In order for a product to be placed in the market, several conformity assessment steps need to be followed. These steps include a demonstration that all of the legislative requirements are met by the product testing, inspection and certification of the product, and making sure that the procedure for each product is specified in the applicable product legislation.

The same steps are also required for SC, not from a product perspective, but that of a collection of processes, products and services. CYRENE will evolve conformity assessment processes by meeting the same steps having a supply chain as a constant instead of an individual product, and based on the steps taken, new requirements will derive from the entities involved.

A preliminary step in that procedure is to identify the non-specific requirements, initially described in the first phase of the CYRENE. As proposed, the CYRENE requirements phase is building upon the proposed baseline security requirements that are included in the ENISA report [9][9]. Such security requirements are: (a) Security by design; (b) Least privilege (c) Strong authentication (d) Asset protection (e) Supply chain integrity (f) Documentation transparency; (g) Quality management (h) Service continuity (i) Conformance to law (j) initial planning of operational and technical measures and controls.

Following the abstract requirement sections, a more detailed view of the processes should contain the following specifications.

[47] https://www.commoncriteriaportal.org/products/

[48] Gemalto Advanced Whitebox PKI SDK for Android v1.0.1.300, https://www.commoncriteriaportal.org/files/epfiles/Certification%20Report%20NSCIB-CC-230855-CR.pdf

[49] https://ec.europa.eu/growth/single-market/goods/building-blocks/conformity-assessment_en

- Security by design – the SC provider shall design and pre-configure the delivered product so as that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations;
- Least privilege – the SC provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable
- Strong authentication – the SC shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed;
- Asset protection – the SC shall provide an adequate level of protection for critical information assets during storage and transmission;
- Supply chain integrity – the supply chain provider should provide means to ensure that the SC is genuine, cannot be tainted during operation, and its integrity is warranted throughout the SC's lifecycle. Currently this requirement can be technically fulfilled only partly;
- Documentation transparency – the SC provider shall offer comprehensive and understandable documentation about the overall design of the SC, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible. Providing one or more use case scenario(s), can be really helpful for the documentation transparency procedure;
- Quality management – the SC provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes;
- Service continuity – the SC provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure;
- Conformance to law – the SC provider shall accept that all contracts (including those with subcontractors) are conforming to the legal requirements in place;
- Data usage restriction – the SC provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.

CYRENE will take into consideration the aforementioned general requirements and extend them to provide more specific requirements for conformity assessments.

3.2.2 Target of Evaluations (ToE) - Security & Assurance Requirements

3.2.2.1 ToE Description

In this section we provide the basic concepts and interrelation of the terms which are necessary for certification processes. The specification of these terms in the CYRENE will be provided in D.2.2.

As shown in the Glossary (Appendix A – Glossary and Examples), according to the ISO15408 a ToE is a set of software, firmware, hardware and/or process which is subject to a security evaluation in which it is assessed against security requirements (conformity assessment).

Conformity assessment of the ToE is defined as the procedure followed to evaluate whether specified requirements relating to the ToE have been fulfilled[50]. Thus, according to ISO/IEC 15408-1[51] and ETSI TS 102 165-1 v5.2.3 (2017-10)[52], it is required to clearly define what the ToE is and specify its security aspects.

ToE shall be the ICT product (equipment, device, asset, process or service) as a whole or the elements of the ICT product. As far as ISO/IEC 15408 is concerned, the precise relation between the ToE and any IT products is important in only one aspect: the evaluation of a ToE containing only a part of an IT product should not be misrepresented as an evaluation of the entire IT product.

For the purposes of this project, ToE is defined as an interconnected set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end-user across the modes of transport. Thus, in the case of CYRENE, a ToE is a Supply Chain Service (SCS**)** that may involve many SCS business partners (vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, authorities and other entities) that contribute to reach the end user[8] (provision of the SCS).

3.2.2.2 Security environment

The security environment includes all the security aspects of the environment in which the asset is intended to be used. For the purposes of this project, the security environment contains any aspects related to the security of the processes, assets, techniques, and technologies associated with the ToE, i.e. the supply chain service[53].

The key elements of the security environment are the following[51]:

- *Security assumptions*: the intended use of the implementation of the ToE;
- *Assets*: the assets that are to be protected, i.e., the ToE itself; the components that comprise the ToE and all the assets with which the ToE under analysis will interact with;
- *Threats and threat agents*: a set of threats (threat scenarios) that are relevant to the secure operation of the ToE; the threat agents that will be used to enact the identified threats;
- *Organizational security policies*: a security policy is expressed by a set of controls that address all the security functional requirements to be implemented by a ToE.

In our case the above issues will be specified in D.2.2 for the CYRENE case where the ToE is a SCS.

[50] https://eur-lex.europa.eu/eli/reg/2019/881/oj

[51] https://www.iso.org/standard/50341.html

[52] https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[53] ENISA report (2015) “Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward”, v.1.1, August 2015. Online available: https://www.enisa.europa.eu/publications/sci-2015

3.2.2.3 Security objectives

A set of security objectives need to be satisfied by the ToE in response to the defined security problem. The security objectives that are to be fulfilled by a ToE should be clearly defined and evaluated in the conformity assessment process.

Different definitions for the security objectives have been presented in the bibliography. Based on ISO 28000:2007, a security objective is defined as a specific outcome or achievement required for security in order to comply with the security management policy. It is essential that such outcomes are linked either directly or indirectly to the provision of products, or services delivered by the overall business to its customers or end-users. The ETSI TVRA methodology defines the security objectives of both the asset and its environment. These objectives are expected to cover the assumptions, identified threats and policies that need to be addressed as described in *3.2.2.2 Security environment*.

An indicative example of security objectives to be set for the SCS-ToE, as defined in this project, could be to ensure the integrity of all SCS processes or the authenticity of the SCS data exchanged between the SCS-business partners.

3.2.2.4 Security requirements

The distinction between security objectives and security requirements is of great importance. An objective is the expression of what a security system should be able to do in very broad terms while a requirement is a more detailed specification of how an objective is achieved. More than one requirement could be fulfilled in order to meet one objective. In ETSI TVRA methodology, indicative examples are presented in order to better apprehend this distinction between these two similar terms.
The security requirements consist of two categories of requirements:

a) the security functional requirements (SFRs)
b) the security assurance requirements (SARs)

Security Functional Requirements (SFR)
Security functional requirements are a set of requirements specified in the basic security standard and an indication of where in the standard the detailed requirement can be found. In CC, SFRs are defined as the translation of the security objectives for the ToE into a standardized language. The implementation of functional requirements addresses threats of counterfeited or tainted products and components.

Security Assurance Requirements (SAR)
Based on CC, SARs provide a description of how assurance is to be gained that the ToE meets the SFRs [ISO/IEC 15408-1:2009 (CC)]. Evaluation Assurance Level (EAL) is a scale for measuring assurance for component ToE. In ETSI TVRA methodology, asset security assurance requirements provide an indication of the EAL that an implementation of the base security standard could be expected to meet.
From the Evaluation service level summary as specified in ISO/IEC 15408, Vulnerability Analysis is the assurance class that will be used in this project. This assessment deals with threats and

could allow to testing if attackers are able to violate the SFRs. In particular, the Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the ToE. The assessment of development vulnerabilities is covered by the AVA_VAN assurance family.
Cases where the security problem description mentions threats where the threat agent is very capable, and a low (or no) Vulnerability analysis (AVA_VAN) are included in the SARs.

3.2.3 Methodologies for CAs

In order to apply the Threat Vulnerability Risk Analysis (TVRA), a specific method has been developed, which consists of a systematic re-evaluation of undesirable events that need to be prevented in a given system.

In order to succeed in doing this evaluation, one needs to identify the assets that compose the system and the associated weaknesses, as well as the threats and the threat agents that might attack the system. After that, the procedure to follow includes a modelling of the likelihood and the impact of the potential attacks on the system's vulnerabilities so as to determine the risk to which the system is exposed.

A system includes assets such as physical, human and logical ones. Those identified assets may have weaknesses that can potentially be attacked by threat agents who enact a threat. This results into breaking some of the initially defined security objectives. When the TVRA is applied, several countermeasures are put in place, whose goal is to protect the assets against threats related to vulnerabilities, by reducing the risk.

The TVRA method repeatedly identifies the assets of a given system and the relationships between them. For each one of the assets, a weakness might be established and an assessment of how practical an attack is to be mounted as well as its potential resulting risk. The method process is explained in 10 steps, as follows:

1. ***Identification of the Target of Evaluation (ToE) resulting in a high-level description of the main assets of the ToE and the ToE environment and a specification of the goal, purpose and scope of the TVRA***
   At first, it is essential to clearly define the scope, purpose and goal of the analysis. The Target of Evaluation (ToE) and its environment must be described, representing a "system under standardization". This description might as well include information of the system architecture, its relevant applications, information flows and possible attack surfaces.
2. ***Identification of the objectives resulting in a high-level statement of the security aims and issues to be resolved***
   What matters at this stage is to identify the security objectives in terms of user protection to be given. If those objectives are unknown, it is highly difficult to come up with security requirements and the TVRA would not be fruitful. For most of the telecommunication services, there is a series of technical security issues in which these objectives can be categorized into:
   - Fraud charging
   - Privacy protection
   - Service availability guarantee

3. ***Identification of the functional security requirements, derived from the objectives from step 2***
   Based on the system objectives identified in step 1, this step aims at identifying the functional security requirements that can be either security or assurance requirements. For this step, it might be wise to use the ISO/IEC 15408-2 [i.28] requirements.
4. ***Systematic Inventory of the assets as refinements of the high-level asset descriptions from step 1 and additional assets as a result of steps 2 and 3***
   For step 4, the assets are classified and it is vital to identify the nature of the assets that the system includes as well as the complexity of the technology comprised in their construction. The assets are identified in three categories:
   - physical assets, such as equipment
   - human assets and
   - logical assets (information stored in and handled by the physical assets)

   We can consider that an asset is at risk when a weakness related to it exists and a viable threat is present. The gravity of the vulnerability will depend on the value that is attributed to the asset and the probability of the weakness to be abused by a threat. The evaluation must be repeated until no assets can be identified. The relations of the asset have to be identified in what concerns its affiliation to the system and to other assets (parent-child-sibling relationships that might exist).

   What really is important is to calculate the impact on the system after a successful attack. The asset impact can be of different level of severity (low, medium, high) according to the harm the attack has on the system, as seen in *Table 1*.

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

Table 1 - Impact on assets after a successful attack.

5. ***Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result***
   The identification process begins with the determination of the weaknesses and the process of locating them, what threats could take advantage of the weaknesses and what is the potential harm due to these attacks. A vulnerability within the system occurs only when a threat can be associated to a weakness.
   A Weakness is a potential point of attack. Nevertheless, all weaknesses do not provide the possibility of viable attacks. The weaknesses on which a realistic attack can be done, are considered to be vulnerabilities.
   Vulnerabilities are the potential attack surfaces that need to be identified and examined.

A successful attack needs a well-elaborated attack method. A successful attack method needs to be practical and in order to evaluate its practicality, the following factors shall be analyzed in order to determine the weight of the attack potential that is needed to take advantage of a vulnerability:

- System knowledge.
- Time.
- Expertise.
- Opportunity.
- Equipment.

Threat agents need to be identified as well. Threat agents consist of entities that act maliciously on the system's assets. The extent to which a threat agent is motivated and capable of mounting a successful attack, differs according to the agent.
The threat agent's capability combined with their motivation, gives us the level of the threat. We define capability of the threat agent, the level of technical sophistication of the threat, and motivation the extent to which the agent wants to attack and compromise a given asset or a group of them. *Table 2* shows the mapping of both:

Motivation	Capability				
	Very Little	**Little**	**Limited**	**Significant**	**Formidable**
Very low (indifferent)	Negligible	Negligible	Low	Low	Low
Low (curious)	Negligible	Negligible	Low	Low	Moderate
Medium (interested)	Negligible	Low	Moderate	Severe	Severe
High (committed)	Low	Low	Moderate	Severe	Critical
Very high (focused)	Low	Moderate	Severe	Critical	Critical

Table 2 - Mapping of motivation and capability of threat agents.

6. ***Quantifying the occurrence likelihood and impact of the threats***
   The attack factors mentioned in step 5 shall be summed (i.e., Time + Expertise + Knowledge + Opportunity + Equipment) to obtain an overall attack potential rating. The attack potential value is then mapped to a vulnerability rating. The vulnerability rating is thereafter combined with the threat level to obtain the occurrence probability/likelihood.
7. ***Establishment of the risks***
   As said above, for every asset of the system, the vulnerabilities are identified after having determined their weaknesses and related threats. The probability of each vulnerability is calculated as described in step 6. One shall also calculate the risk associated to each vulnerability and for this, the impact of intensity, and classification of risk, have to be considered.
8. ***Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk***

Security Countermeasures are basically new assets added to the system aiming to reduce the calculated risk the system might go through. In a few words, countermeasures are put in place in order to reduce the probability of an attack and/or its impact. Security countermeasures are mainly logical assets but can also be human or physical.
Given the fact that there might exist various alternative countermeasures, they have to be at first identified and then compared to each other in order to choose the most beneficial in terms of cost, and overall impact.
Every new countermeasure and its associated physical asset, bring new vulnerabilities to the system and for this, the TVRA shall be applied including the countermeasures in the ToE.

9. ***Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8***
   As stated above, there might be a number of possible countermeasures and for this, an analysis must be conducted in order to choose the most beneficial of them. The chosen countermeasures need to mitigate the attack measures that result in added security and attack protection. Other than that, countermeasures are evaluated according to the standards design, their implementation, the operation, their regulatory impact, and the related market acceptance.
10. ***Specification of detailed requirements for the security services and capabilities from step 9***
    During this final step, security requirements are to be identified both for the assets and their environment, where applicable. Functional security requirements identified in step 3 and the security services and capabilities of the countermeasures and security requirements identified in step 8 and analyzed in step 9, are used and refined at this stage. Guidelines for the specification of detailed requirements are given in ETSI TR 187 011 [i.2].

3.2.4 Standards for CAs

Overtime, ISO, and IEC have developed many standards that may help to set up a proper conformity assessment system. The website of ISO provides an overview of international standards and guides for conformity assessment. There are international and also EU specific standards that the CYRENE conformity assessment procedure will be based upon.

ISO/IEC 17000:2020[54] provides the vocabulary and general principles for international conformity assessment based on a functional approach. Any form of conformity assessment reflects the following functions: selection, determination, review, and attestation.

ISO/IEC Guide 17067:2013[55] recommends good practices for all elements of conformity assessment, including normative documents, bodies, systems, schemes, and results. It is intended for use by individuals and bodies who wish to provide, promote, or use ethical and reliable conformity assessment services. Next, international standards have been developed for

[54] https://www.iso.org/standard/73029.html

[55] https://www.iso.org/standard/55087.html

the different categories of conformity assessment bodies and their activities, (*Table 3 - Conformity standards*).

ISO/IEC 17021:2006[56] contains standards and criteria for the competence, consistency and impartiality of audit and certification of all forms of managements systems (e.g., quality managements systems or environmental managements systems), as well as the bodies that provide these services. Certification bodies adhering to this International Standard are not expected to provide certification for all forms of management systems. Management system certification is a third-party conformity testing practice. As a result, third-party conformity testing bodies conduct this task.

ISO/IEC 17024:2012[57] contains principles and requirements for a body certifying persons against specific requirements and includes the development and maintenance of a certification scheme for persons.

ISO/IEC 17020:2012[58] indicates requirements for the competence of bodies performing review and for the impartiality and consistency of their inspection activities.

Conformity assessment body	Standard or guide
Conformity assessment body	Standard or guide
Testing and Calibration laboratories	ISO/IEC 17025:2005
Certification bodies for: - product certification - management system certification - certification of persons	ISO/IEC Guide 17067:2013 ISO/IEC 17021:2006 ISO/IEC 17024:2012
Inspection of bodies	ISO/IEC 17020:2012

Table 3 - Conformity standards.

In the context of CYRENE, standards shown in *Table 3 - Conformity standards* that concentrate on the quality and management (and not security) will be taken into account in Cyrene proposal for the SCS security certification scheme (that will be based on the ISO15408).

[56] https://www.iso.org/standard/29343.html

[57] https://www.iso.org/standard/52993.html

[58] https://www.iso.org/standard/52994.html#:~:text=ISO%2FIEC%2017020%3A2012%20specifies,to%20any%20stage%20of%20inspection

3.2.5 Conformance monitoring

This paragraph deals with measures put in place in order that a certified system/product can still be considered as certified over time, after the initial acquisition of the certificate.

Up to 2020 (where the European Certification Scheme was proposed by ENISA), there was not an official procedure or set of requirements established by the SOG-IS scheme to that end. Such a mechanism will thus have to be officially developed and established. The work can be based on existing procedures related to the approach of maintenance in the SOG-IS scheme.

Until a monitoring mechanism is established, this process can be initiated by the risk owner as a way of compliance monitoring by conducting voluntary assessments.

There is although a proposed approach by the SOG-IS MRA participants who suggest the following:

- the Conformity Assessment Bodies (CABs) to establish a validity period of 5 years for each certificate
- the CABs to work on evaluation methods so that the initial certificate can retain some of its validity on future updated versions where it can be proven that the updates were carried out according to a set of pre-defined requirements
- Manufacturers/developers to:
    - Carry out impact analyses of all modifications added to the product or the system over its lifecycle
    - Monitor common vulnerabilities and exposures (CVEs) that may apply to the system and submit an impact analysis when necessary, to the competent CAB
    - Showcase the actions taken in order to maintain levels of security, also reporting to the competent CAB
    - Manage customer complaints and keep record of corrective actions
- the CABs to periodically review issued certificates based on a security assessment of an ITSEF (Information Technology Security Evaluation Facility) which considers the impact analyses of the accumulated changes since the latest evaluation carried out
- the CABs to withdraw certificates in case there is evidence that the commitments/requirements are not respected or in case a security assessment has failed and no corrections can be applied.

4. Methodology

This chapter gives an overview of the methodology followed for the elicitation and analysis of requirements as well as their validation with the project's Advisory Boards.

Figure 4 summarizes the requirements engineering process.

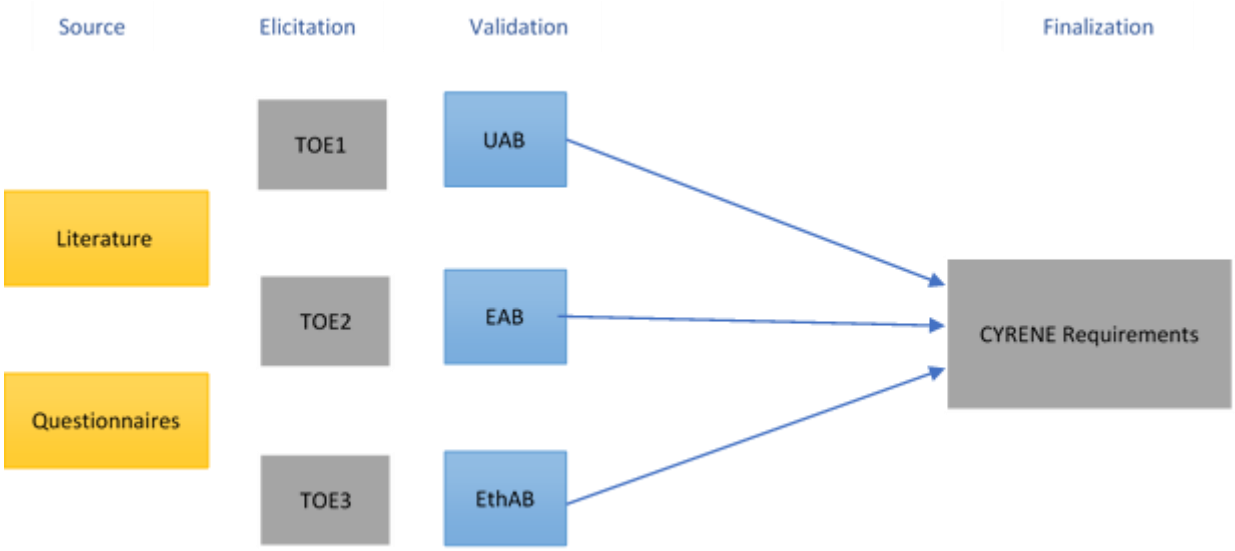


Figure 4 - Overview of requirements elicitation and validation process.

The first column on the left includes the investigation of the Standards (SotA) by means of literature overview and interviews to experts and stakeholders. This process, that leads to the elicitation of the three CYRENE ToEs, is described in paragraph 4.1.

The validation of requirements is performed by involving three different Advisory Boards (User, External and Ethical) and then leads to the finalization of Cyrene requirements.

In the next two subsections, the methodology used for requirements elicitation and validation is better explained.

4.1 Methodology for requirements elicitation

The methodology used for the requirements elicitation is summarized in *Figure 5* and described below.

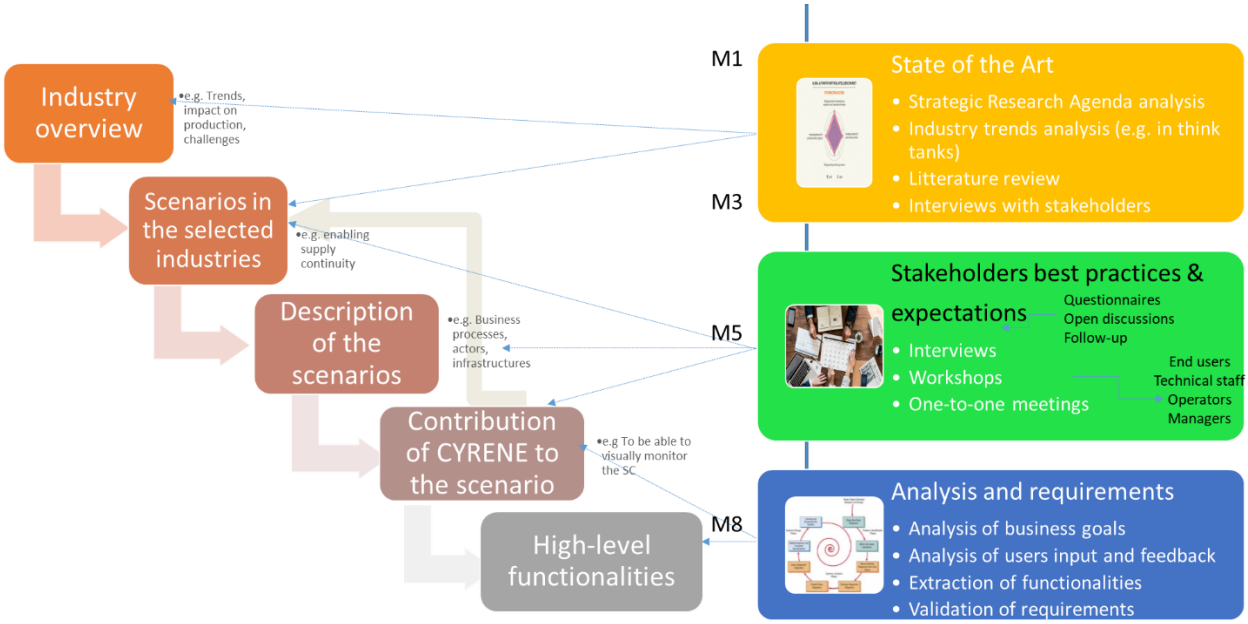


Figure 5 - Overview of the methodology for requirements elicitation.

The requirements elicitation process has been performed during the first eight months of the project.
It started with the “Industry overview” step. The general situation regarding the outlook of the industry (e.g.: trends in cybersecurity in IoT, etc.) is examined, through an analysis of the company strategic agenda, the industry outlook as hypothesised by consultancy firms or think tanks (e.g.: Gartner, Allied Market Research) and through dedicated interviews with key stakeholders providing their specific expertise (e.g.: the impact of connected cars on cybersecurity). This results in an overview of the existing services in the Industry and a forecast of their evolution and the required systems.

After this first result, there are two other steps, where the process is iterated several times, before arriving to a definition of high-level requirements. During these phases, end-users, technical staff, operators and managers are involved.

The “Scenarios in the selected industry” steps narrows the analysis to the specific cybersecurity scenarios in Supply Chains, and to the processes managed by the stakeholders involved.

Then, in the “Description of scenarios” step, the AS-IS situation is presented, describing the actions performed by the people involved during their daily activities, and which tools they use to face the cybersecurity issues encountered. In particular, as it will be better described in the Chapter CYRENE Conformity Assessment , Business processes, actors, and infrastructures involved in the considered scenarios are described in detail and modelled.

The last step of this iterative process is the one that sets the ground for the elicitation of the requirements and is called “Contribution of CYRENE to the scenario”. In fact, this phase is the one when the objectives of the project are presented to the stakeholders, trying to match the user needs with CYRENE layers that could satisfy these needs.

Different iterations of these three steps are usually performed in order to identify other scenarios and adding more details in order to better understand the AS-IS situation and to validate requirements. In particular, in CYRENE, the elicitation of the three ToE requirements (business, technical, sectorial, as will be detailed in chapter 5) has been made involving end users, technical staff, operators and managers from the pilot partners, by means of interviews and one-to-one meetings.

The conclusion of the iterative process (presentation and questions as shown above, feedback, dedicated meetings and deep dives) then led to the “High-level Requirements” step. The business goals emerged from the previous phases are analysed here, in order to list the business needs of the final users. Moreover, matching the results of this analysis with the inputs and feedbacks of the discussion points mentioned above, it is possible to extract the high-level requirements, translating the business needs into relevant functionalities of the system.

4.2 Methodology for requirements validation

After the previous process, that led to listing the ToEs’ requirements, the requirements were validated through the three Advisory Boards: User Advisory Boards, Ethics Advisory Boards and External Advisory Boards.

The validation followed the organization of a workshop at the end of month 6 of the project, where the members of the Advisory Boards were invited. Details and results related to the workshop material, organization and results are better explained in Appendix B – Validation of CYRENE ToEs.

Project material was shared with the Advisory Boards some days before the event, including a first version of the current report, project presentations and a questionnaire. In particular, the questionnaire (see more details in the Appendix B – Validation of CYRENE ToEs), addresses mainly the following aspects:

- “How ICT threats impact on your daily work?”
- “How do you face the problems you encounter?”
- “Which tools/measures are you using to identify, monitor and mitigate risks?”

The workshop was structured in the following way:

1. Presentation of CYRENE: slides were presented to the participants in order to introduce them to project main objectives.
2. The discussion started then from these points in order to have feedbacks from the Advisory Boards on the requirements and their validation.

At the end of the workshop, all participants were asked to give their answers to the questionnaire.

Moreover, the questionnaire was also submitted to wider audience of stakeholders contacted by the project partners, in order to have additional feedback.

4.3 CYRENE Questionnaire for enriching the requirements with feedback collected by external stakeholders

CYRENE organised on 31st of March 2021 the 1st CYRENE Workshop. Its preparation was taken care by the Privanova (PN) Team. During the workshop, the partners presented an overview of the project, the security aspects of supply chains in general and also grounded their presentations with the Supply Chains (SC) as Targets of Evaluation (ToEs). Except for the discussion and collection of feedback by the Advisory Board members, the consortium shared the CYRENE Questionnaire as well, in order to be filled within a defined time frame.

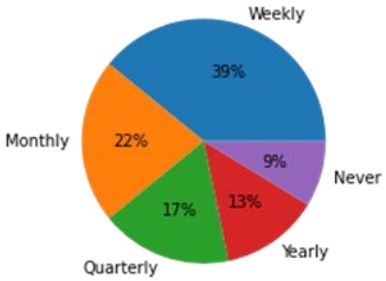
The CYRENE Questionnaire was a campaign which was held between the 31st of March 2021 and finalised on the 10th of May 2021. Some high level insights of the questionnaire on the infographic dimension of the 23 total collected results include that 69,5% of the participants are private companies, while 4,4% are non-profit organisations and 26,1% are public authorities. Among the private companies, 4,3% are coming from the automobile sector, while the public and non-profit sectors are representing port authorities. The majority of the companies are representing large IT companies, supply chain providers, software houses, system integrators and technology providers, maritime ICT domain, healthcare service providers and consultancy services. The rest of the participants represent research organisations and universities. Among the participants, 30% are coming from small companies, 21% from medium ones and 49% from large ones. Last but not least, the professional background of the participants is dealing with the OT and IT systems and devices surveillance services, project management, blockchain and B2B platforms, chief technology operation, ICT security policy making, systems maintenance and security automation operations, GDPR and ISO27001 compliance, cybersecurity services and research activities on cybersecurity certification, testing, evaluation and mitigation actions.

4.3.1 Feedback from the questionnaire

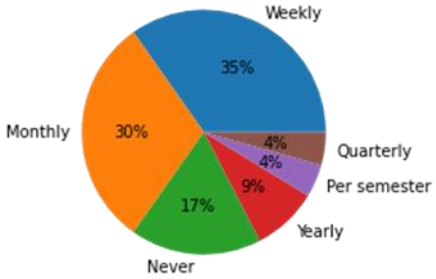
In this paragraph, the most significant results of the questionnaire are presented. In fact, some relevant questions asked to the stakeholders are shown with the related infographic description including tables and graphs and then the results are summarized.

Figure 6 depicts the statistics of the question *"In case you perform any tasks related to ICT Systems Security, please specify the cybersecurity activities and their frequency that are applicable to your organisation."*

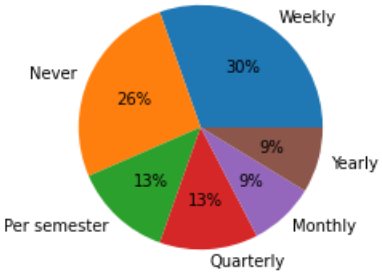
Big Four



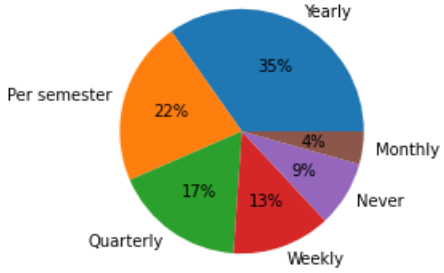
Secure / Encrypted Remote Access to enterprise networks



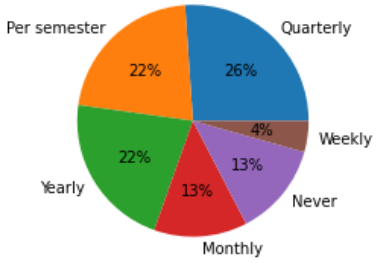
Multifactor Authentication



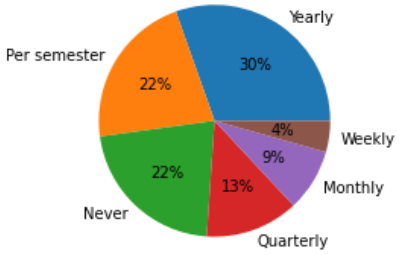
Employees training and awareness



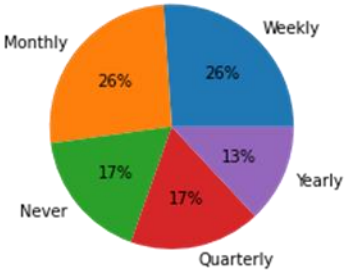
Adoption of certified products, services and processes



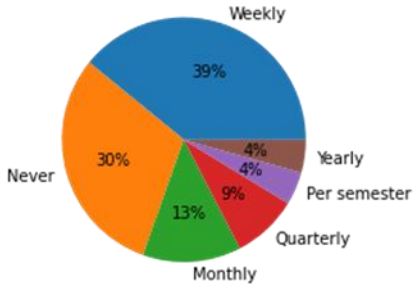
Risk Assessment procedures



User Identity Management



Virtualisation services



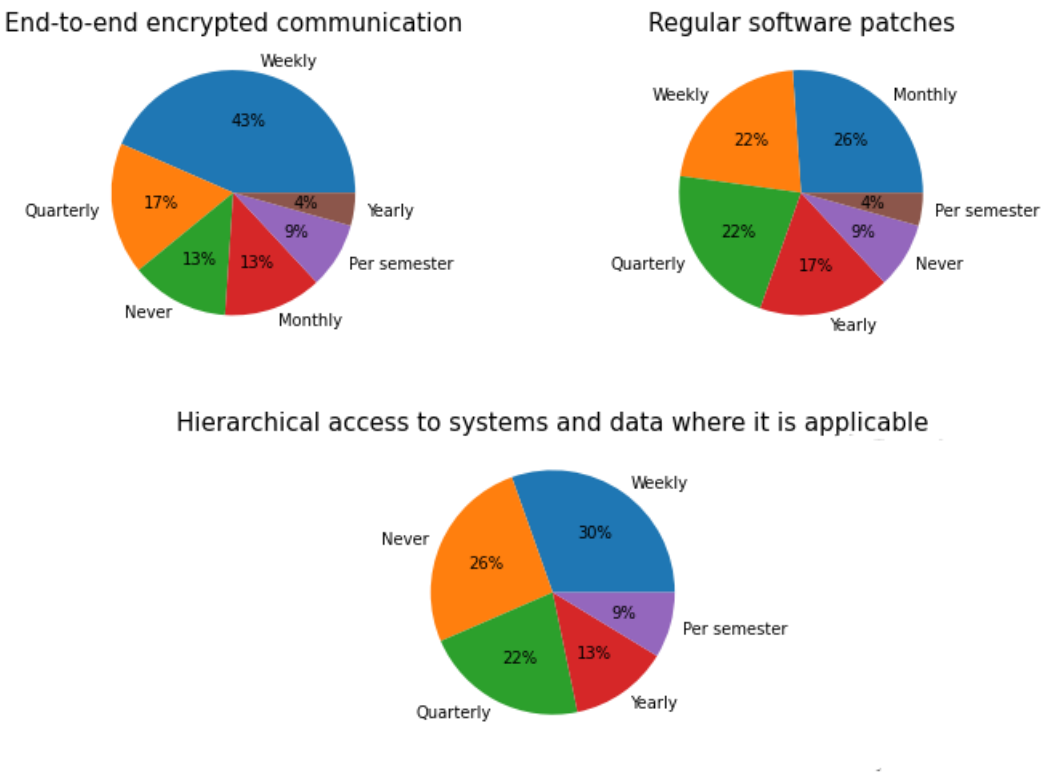


Figure 6 - Cybersecurity activities frequency.

Table 4 summarizes the statistics of the question *"Please identify the set of Supply Chain (SC) Services that are critical for your organisation in terms of business importance and scale them accordingly."*

Supply chain service	Total score (max score is 115)
Solutions provider	63
Components/Peripherals provider	61
Third party services	60
Transportation	57
Public Authority	56
Local / Global Agent's services	54
Outbound Logistics	52
Inbound Logistics	49
Warehouse	44
Retailer	34

Table 4 - Business importance of SCS.

Table 5 summarizes the statistics of the question *"What Security Standards and proven guidelines has your organization adopted?"*

Standards	Number of respondents
ISO / IEC 27001	11
ISO 9001	8
I do not know / It does not concern	7
ISO 28001	4
NIST Framework for the Improvement of Critical Cybersecurity Infrastructures	3
ISO / IEC 27002	3
ISO / IEC 27035	3
ISO / IEC 15408	1
ISO / IEC 27005	1
ISO / IEC 18045	1
NIST SP800-30	1
NIST SP800-61	1

Table 5 - Security standards and guidelines adopted.

Figure 7 summarizes the results of the question "*Are you aware of the EU Cybersecurity Certification Framework for ICT products and services?"*

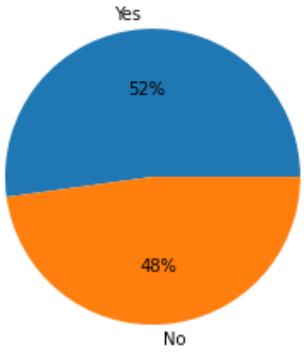


Figure 7 - Awareness of EU Cybersecurity Certification Framework for ICT products and services.

Figure 8 summarizes the result of the question *"How does your organization address the following cybersecurity issues in the Supply Chain Services you are involved in?"*

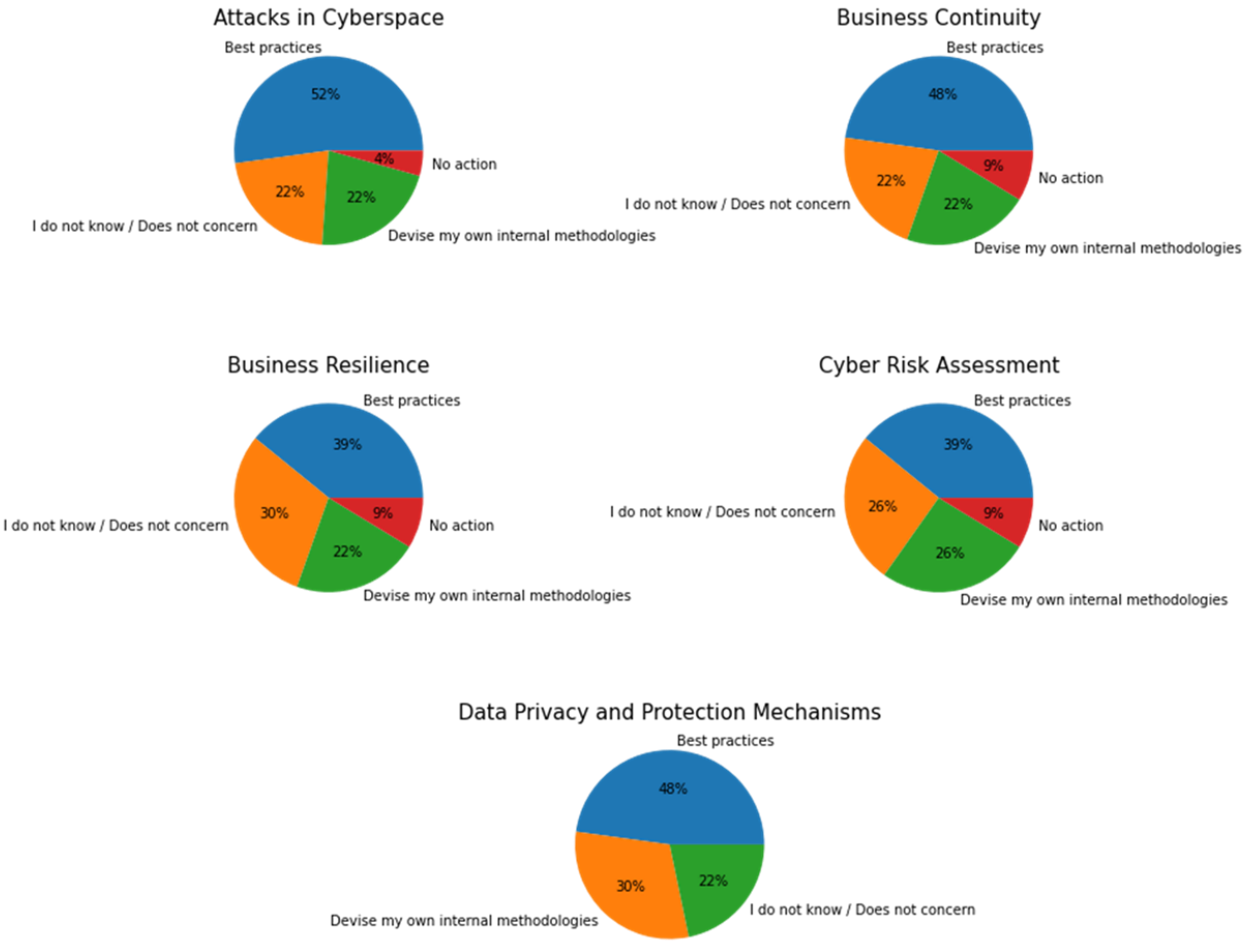


Figure 8 - Measures to address cybersecurity issues.

Figure 9 summarizes the results of the question *"Does your organization provide an effective cybersecurity management plan for the Supply Chain Services you are involved in?"*

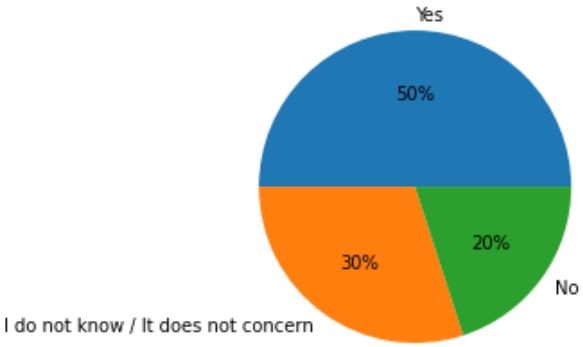


Figure 9 - Effective cybersecurity management plan applied to SCS.

Figure 10 summarizes the results of the question *"Are you aware of the content of the security standards and best practices that your organization has adopted and implemented?"*

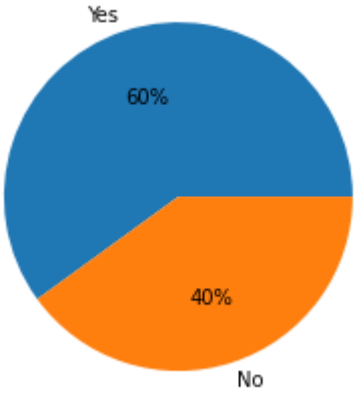


Figure 10 - Awareness of security standards and best practices adopted.

Figure 11 summarizes the result of the question *"Choose the Security Procedures and Policies that apply to your organization"*

Malware Detection Software / Policies	14.0
Policies / Procedures for Backup and Disaster Recovery	14.0
Information security procedures	14.0
Access Control Policies / Procedures	13.0
Business Continuity Policies / Procedures	11.0
Cyber-incident management procedures	11.0
Network Access Policies / Procedures	10.0
Security Monitoring Policies / Procedures	10.0
Problem management procedures	10.0
User Identification Policies / Procedures	5.0
I do not know / It does not concern	3.0
Policies / Procedures for inteconnecting the Affiliated / Collaborating Organizations	2.0

Figure 11 - Security procedure - Number of respondents.

Figure 12 summarizes the results of the question *"Does your organization comply with the legal and regulatory principles and EU directives regarding the security of Supply Chain Services and the protection of Personal Data?"*

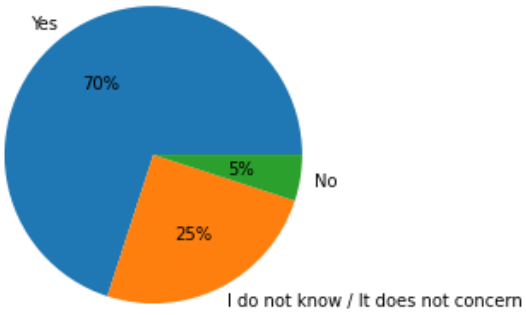


Figure 12 - Compliance with legal and regulatory principles and EU directives.

Figure 13 summarizes the results of the question *"Have you experienced any cybersecurity issue in the last 3 years?"*

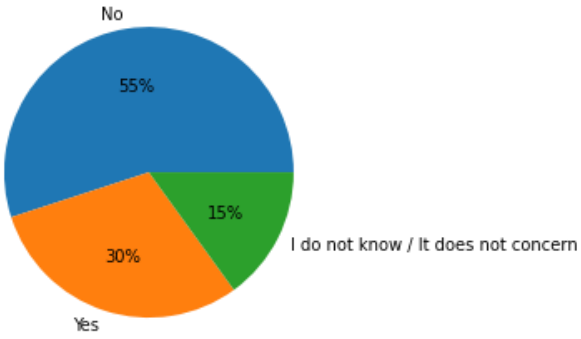


Figure 13 - Experience of cybersecurity issues in last years.

Figure 14 summarizes the results of the question *"Regarding potential security incidents to the services, information systems, and infrastructure used by your organization, please evaluate what is the probability to experience a threat in the future."*

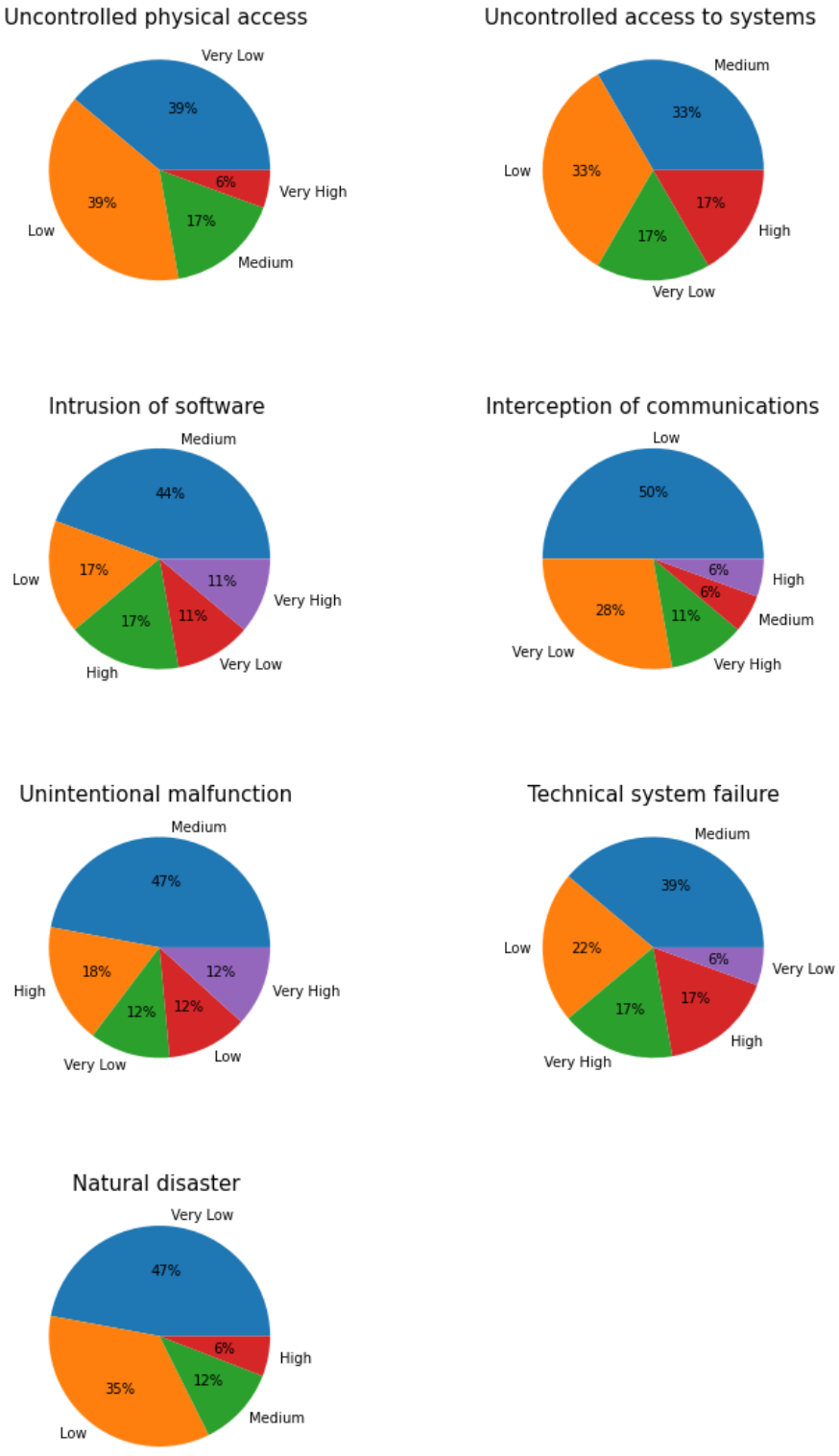


Figure 14 - Probability of threats in the future.

Figure 15 summarizes the results of the question *"To whom do you report for issues related to risks and security threats and how often?"*

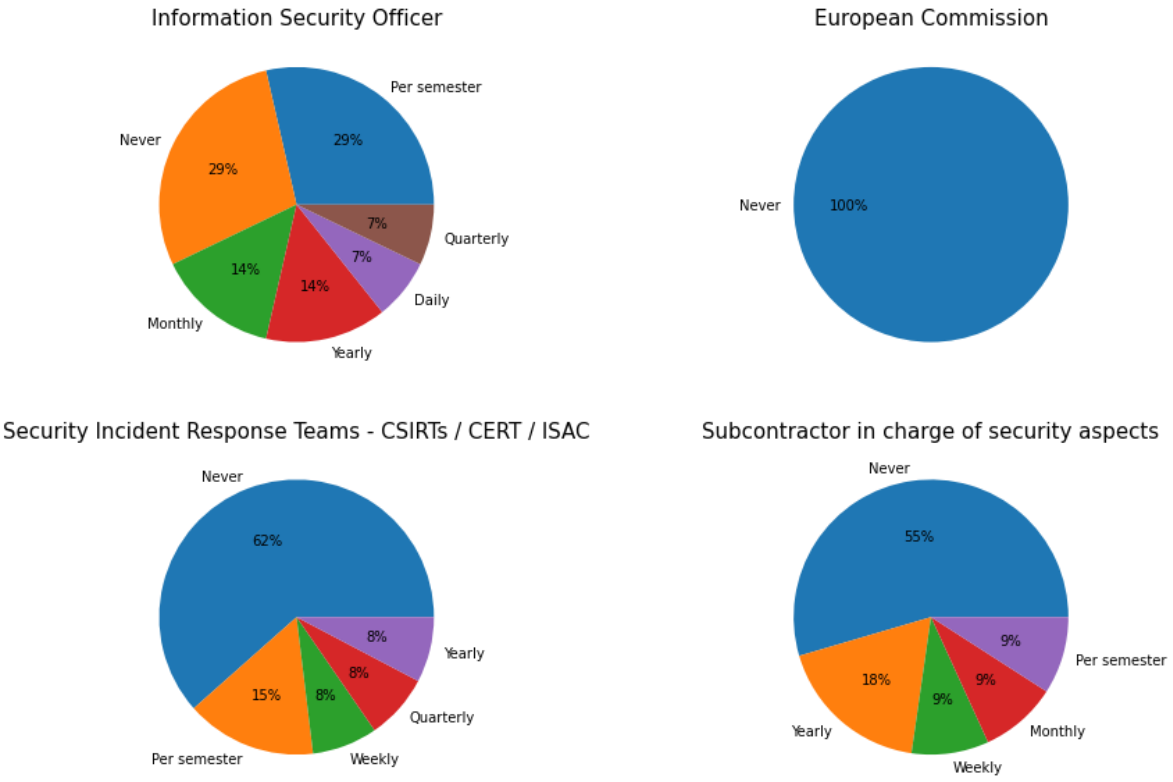


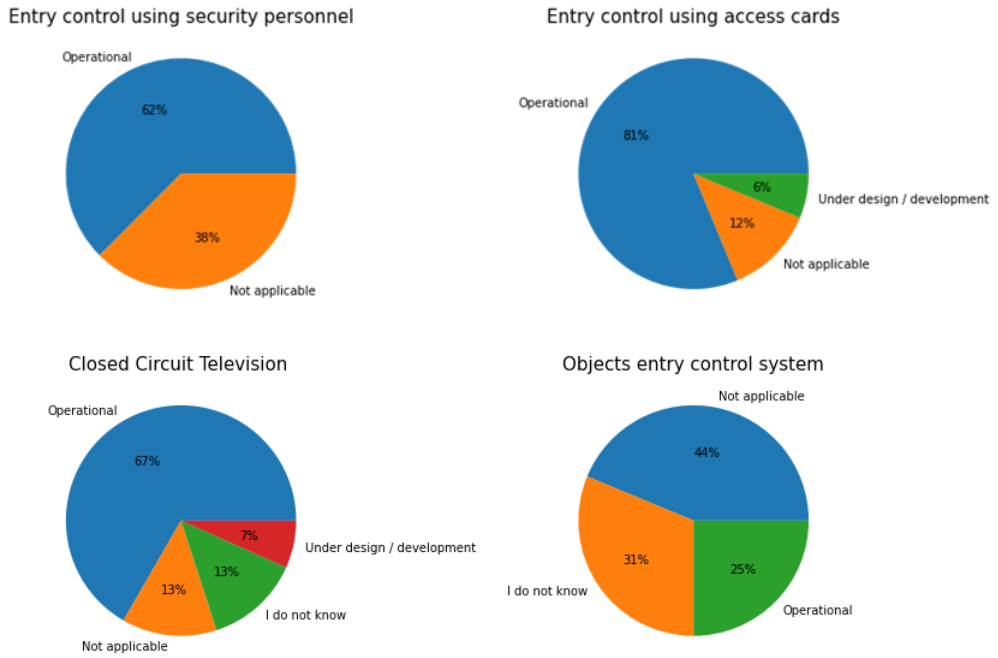
Figure 15 - Addressee of risks and security threats.

Figure 16 summarizes the results of the question *"What are the most important tools (e.g. human or technical resources, processes, etc.) required for secure service delivery?"* (maximum score is 115).

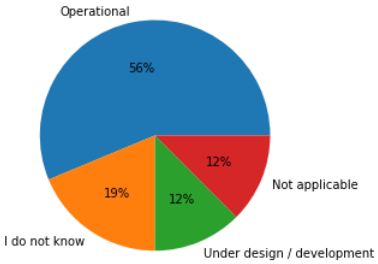
Organizational & Individual Tools: Awareness	63.0
Organizational & Individual Tools: Trainings	62.0
Organizational & Individual Tools: Collaborative Means	57.0
Organizational & Individual Tools: Mitigation Skills	55.0
Organizational & Individual Tools: Risk Assessment	55.0
Organizational & Individual Tools: Experienced Human Resources	55.0
Technical Tools: Intrusion Detection Mechanisms	54.0
Organizational & Individual Tools: Assessment Means	52.0
Organizational & Individual Tools: Mindful Set	50.0
Technical Tools: Information Systems	49.0
Organizational & Individual Tools: Predictive Means	48.0
Technical Tools: Data Analysis Systems	48.0
Technical Tools: Decision Support Systems	47.0
Technical Tools: Mobile Devices	46.0
Organizational & Individual Tools: Open Information	45.0
Technical Tools: Mobile Platforms	41.0

Figure 16 - Relevant tools for secure service delivery.

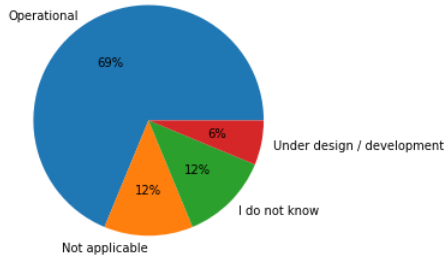
Figure 17 summarizes the results of the question *"Which of the following ICT Systems security measures apply to your day-to-day operations?"*



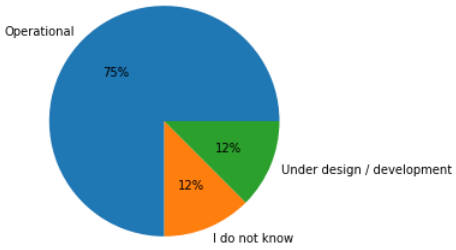
Building / Data Centre fire safety system



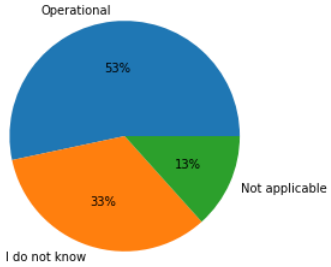
Data Centre air conditioning system



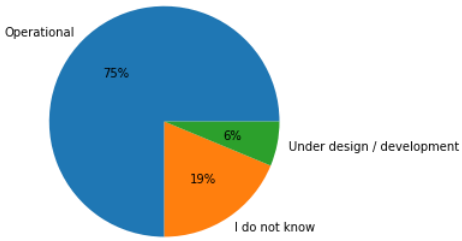
Use of dual / backup systems



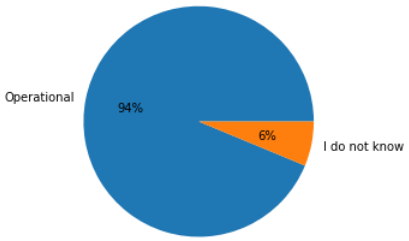
Use of alternative network connections



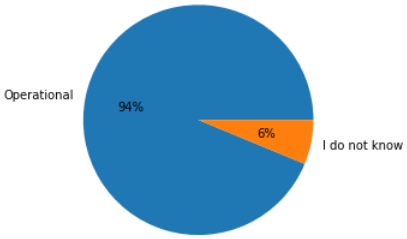
Processes for maintenance and systems control



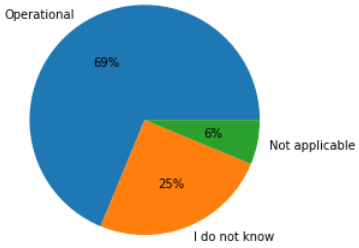
Backup files



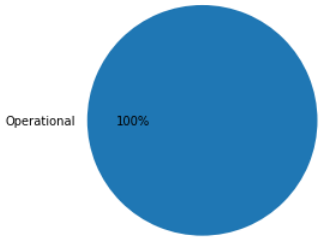
Automated backup file system



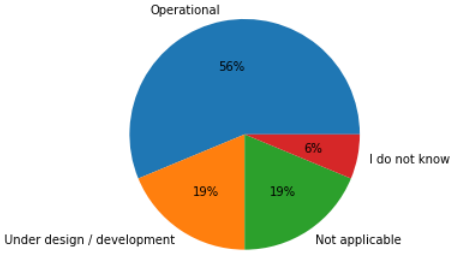
Secure backup storage



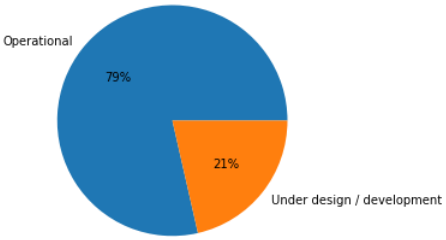
Use of unique credentials



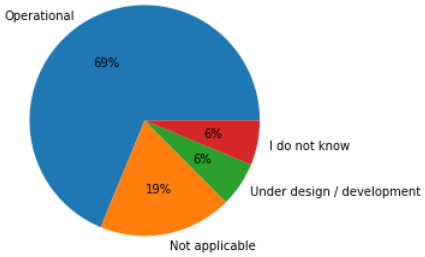
Use of certificate tokens to access systems



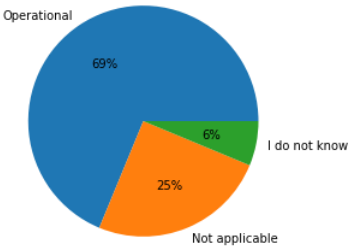
Logging access and actions



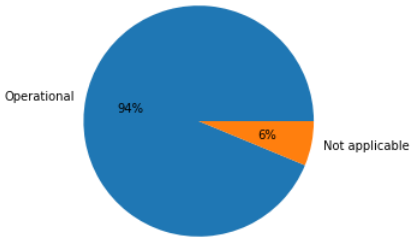
Encryption of sensitive information



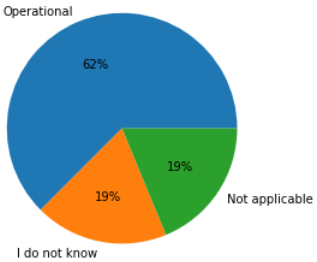
Communications encryption



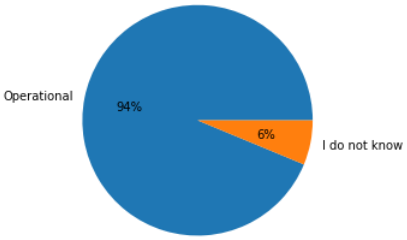
Use of antivirus system



Use of filtering techniques in web applications



Systems update



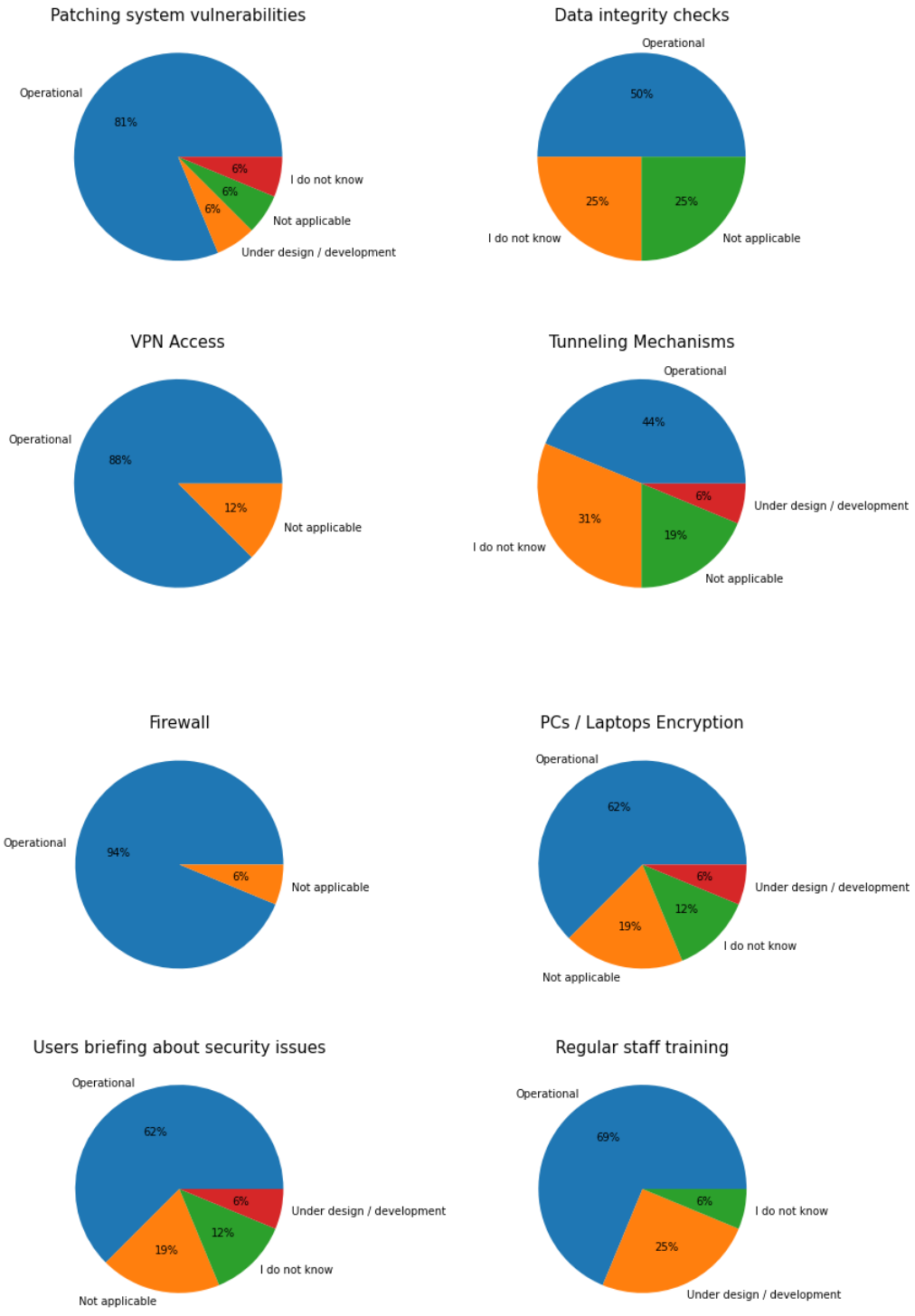


Figure 17 - ICT Systems security measures applied to daily operations.

Figure 18 summarizes the results of the question *"Do you perform periodic audits to inspect user activity on the Organization's network?"*

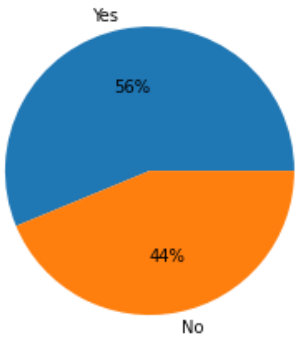


Figure 18 - Perform of periodic audits.

Figure 19 summarizes the results of the question *"Has an external certified analyst been assigned the analysis and evaluation of threats and vulnerabilities, as well as the execution of penetration tests (vulnerability scanning / penetration testing) in the infrastructure of your Organization? If so, how often do you carry out such checks and when was the last time?"*

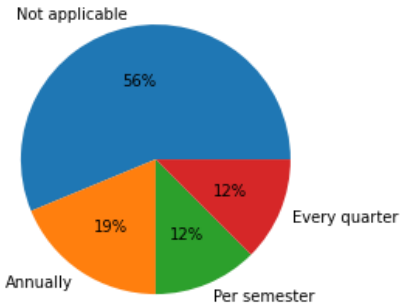


Figure 19 - Analysis and evaluation of infrastructure security performed by external certified analyst.

4.3.1.1 Conclusions from the questionnaire

The answers to the questionnaire give us interesting information regarding the security in Supply Chain and in general in the organizations involved.

The main results that we can extract and that have been presented as graphs are summarized as follows:

- The frequency for cybersecurity activities is very heterogeneous and very different from one participant to another.
- All listed SCSs are considered critical, in terms of business importance, in particular the solutions providers, the components/Peripherals providers and the third-party services, as from *Table 4*.
- Most of the participant states that their companies have adopted ISO / IEC 27001 and ISO 9001, while most of them doesn't have total knowledge if other standards are adopted.

- About half of the people interviewed have knowledge about EU Cybersecurity Certification Framework for ICT products and services.
- Most of the people declares they usually utilize best practices to solve the listed cybersecurity issues they can encounter in the SC, from Business continuity issues to Attacks in cyberspace.
- 50% of people think their companies provide an effective cybersecurity management plan for the Supply Chain Services they are involved in.
- The majority in fact knows company best practices to be used in these cases and the most commonly used Security Procedures and Policies. Most utilized Security Procedures and Policies in organizations are Malware Detection, Backup and Disaster Recovery, Information security and Access Control, as from *Figure 11 - Security procedure - Number of respondents*.
- From *Figure 12 - Compliance with legal and regulatory principles and EU directives Figure 12*, 70% of people answer that his/her company follows the EU directives regarding the security of Supply Chain Services and the protection of Personal Data, while most of the rest are not aware.
- In general, people think that the most probable threats are the following: uncontrolled access to the systems, intrusion of software, unintentional malfunction and technical system failure.
- In case of risks, most of them reports to the information security officer.
- The tools that are considered as the most important for secure service delivery are, from an organizational and individual point of view, the awareness, the trainings and the collaborative means, mitigation skills, risk assessment and experienced human resources and, as technical tool, the intrusion detection mechanisms, as from *Figure 16*.
- ICT Systems security measures listed are applied to day-to-day operations from the majority and in one case from all of the participants to the questionnaire.
- Only a slight majority performs periodic audits to inspect user activity on the organization's network.
- 56% of people declare “Not applicable” as answer to the question related to the analysis and evaluation of infrastructure security performed by external certified analyst.

To conclude, even considering the limitations of the sample, it is important to stress that:

- An assessment that involves all the SCSs providers is needed, since they are all considered important from a business point of view for the organization. Moreover, this implies that the communication between all the participants of the SC should also be secure, in order to ensure integrity and confidentiality of all the data transmitted, and also that the actors involved in the communication are authorized.
- The people involved have no deep knowledge of security standards and policies adopted by their organization nor all of them perform cybersecurity activities frequently. As a result, it is necessary to provide a software solution that supports end-users in their daily operations, allowing auditing all the activities of the SC, identifying vulnerable or compromised assets, performing an analysis of the risks of threats and an impact assessment. All these features will support the decision-making process, by proposing and evaluating different mitigation strategies, therefore being very relevant to the Conformity self-Assessment of ICT related products, services and processes.

5. CYRENE Conformity Assessment

Within a Conformity Assessment (CA) process, the Target of Evaluation (ToE), as mentioned in 3.2, is considered as "a set of software, firmware, hardware and/or process possibly accompanied by guidance" (ISO/IEC 15408-1:2009, see Appendix A – Glossary and Examples.

The CYRENE ToE is the SCS and the CYRENE CA methodology (that will be described in D3.1 "Conformity Evaluation Process & Multi-Level Evidence-Driven Supply Chain Risk Assessment") is oriented to evaluate the SCS-ToE against the security requirements, i.e., the CYRENE CA aims to examine whether specified security requirements related to a given SCS have been fulfilled.

CYRENE CA methodology applies to every SCS in any sector. The CYRENE CA methodology will give the opportunity to SC stakeholders to evaluate their SCSs under all or one of the three different perspectives: the SC business view, the technical view and the sectorial view.

To illustrate this, we will develop the CYRENE CA methodology in the scope of three SCS-ToEs; namely, ToE I: CYRENE business SC, ToE II: CYRENE technical SC, ToE III: CYRENE sectoral SCS, which will be thoroughly analysed in the coming sections. This is carried out in terms of decomposing the SCS to its generic components: SCS processes, business partners involved in the provision of the SCS and highlight the infrastructure they utilize to execute their tasks within the SCS performance. For each ToE, the CYRENE CA methodology can be applied capturing the different aspects of the SCS under the particular viewpoint and examining only the SCS components that matter in this viewpoint.

SCS-ToE I (business view) will be evaluated to the identification, analysis, assessment and mitigation of process-related threat scenarios that concern the SCS-ToE I. It views the SCS under evaluation from a business perspective, entailing SCS processes, business partners information exchange, business logic, etc. to assess their conformity according to the specific ToE I requirements, described in section 5.2.1. Thus, in this ToE the business environment enfolds the SCS processes and business partners participating in these processes. Therefore, the components of the SCS-ToE I under evaluation here are all SCS processes, business partners, data that operate in the provision of the underlined SCS. Digital assets are out of the current scope of the evaluation and will not be subjected to this ToE I.

SCS-ToE II (holistic technical view) provides a technical-asset interdependent view of the SCS and is set to detect and analyze threats, identify and mitigate risks, examining the SCS processes, the business partners involved and the ICT infrastructure together with the individual SCS assets. The latter are hosted and operated by the business partners and are necessary for the provision of the SCS. Thereby, it focuses on assessing the conformity of these SCS components with respect to the ToE II requirements that are specified in section 0. The components of the SCS-ToE II considered under this type of evaluation are: SCS processes, business partners, data and all SCS assets (digital and physical) that participate in the provision of the entire SCS.

SCS-ToE III (individual technical view-snapshot) considers a sector-specific view of the SCS. The boundary of the SCS-ToE III is within the scope of one of the business partners involved in the SCS. The components of the SCS-ToE III considered under this evaluation here are the processes and SCS assets that one of the business partners host and operate in order to participate in the entire SCS.

These three differently adopted views reflect the following CYRENE SCS Circles of consideration which have been described in section 2.1. CYRENE adopts three different views in order to capture the entire SCS ecosystem, since the SCS usually are described either from a business perspective or a technical perspective or a snapshot of the entire SCS.

The CYRENE conformity assessment methodology and the multi-level evidence-driven supply chain risk assessment of CYRENE will be thoroughly described and analysed in D3.1 and is designed in order to assess any SCS independently of the viewpoint.

CYRENE will undertake as an example of its SCS-ToE the Vehicle Transform Service (VTS) and it will assess it by adopting the three (3) different views described above, as it will be presented in the next section. The “Vehicle Transport Service” is a complex SCS, including critical sectors, such as the Automotive Industry and the Maritime Transport Industry. It has been selected because the industries involved impose a high financial and business impact for the EU.

The current section targets at identifying the three ToEs and recognizing their business environment (section 5.1). Technical specifications and further analysis of ICT infrastructures and assets of the VTS that may be included in ToE II and ToE III and will be further analysed in D3.1. Once the business environments of the three ToEs are identified, the requirements for self-conformity assessing the CYRENE ToEs are presented (section 5.2).

5.1 Targets of Evaluations (ToE)

CYRENE has adopted as an example of a SCS-ToE the Vehicle Transport Service (VTS) which is a SCS incorporating different business sectors and industries (e.g., maritime, automotive, transport, tourism).

CYRENE described the VTS-SCS from three different angles (as mentioned in the previous section): VTS-ToE I: business SC, VTS-ToE II: technical SC, VTS-ToE III: sectoral SC. In sections 5.1.1, 5.1.2, 5.1.3 , all these three (3) different views will be analysed and illustrated in detail.

The Vehicle Transport SCS is considered as a massively complex system with numerous players for the manufacturing, shipment and delivery of various types of vehicles. It supports composite processes (i.e., domestic and international transportation, communications and information technology, warehouse management, order and inventory control etc.), which enfolds an aggregation of industry sectors, such as maritime transport and automobile industry. It includes several interactions and tasks among the various entities engaged (stakeholders and actors) having different goals and requirements entailing vehicles manufacturing and storage facilities to assembly plants, i.e., inbound logistics (automotive industry), vehicles distribution, i.e., vehicles transport via port origin and port destination (maritime transport industry) and the final delivery to the importer. The performance of the Vehicle Transport SCS is accomplished through the provision of the Vehicle Transport Service (VTS) which is considered the CYRENE SCS-ToE.

According to the above presentation of the three ToEs:

-VTS-ToE I, includes the SCS processes of the VTS and the business partners interacting to meet these processes.

-VTS-ToE II consists of SCS processes of the VTS, the involved business partners along with the operating SC assets that are involved and participate in the operation and provision of the SCS. In the current report only a high level infrastructure representation is provided. Asset models including technical specifications and security details will be analysed in D3.1, where the CYRENE CA methodology will be thoroughly presented and described.

-VTS-ToE III reflects sector-specific processes of one business partner (in CYRENE the business partner is the Centro Ricerche FIAT ScpA and its World Class Manufacturing Research and Innovation (WCM R&I) department that has the goal to increase flexibility, quality, productivity, safety and ergonomics, energy and security of the logistics and manufacturing processes for FIAT Chrysler Automobiles (FCA)) and its SCS assets that hosts and uses in order to participate in the entire VTS. In the current report only a high level infrastructure representation is provided. Asset models including technical specifications and security details will be analysed in D3.1, where the CYRENE CA methodology will be thoroughly presented and described.

In the coming sections 5.1.1, 5.1.2 and 5.1.3, the business environment of the three ToEs is gradually displayed according to the following structure:

- **Identification and description of SCS business processes of the ToE.**
  In this section a brief description of each identified business processes of the SCS (the VTS) along with the business goal is provided. The process description follows the table format shown in *Table 6*:

ToE SC Process x (A general description of the business process and its business goal)
…….

Table 6 - SC process description template.

- **Identification and description of the business partners involved in the SCS processes of the ToE.**

  Within this section the identified SCS processes of each ToE are further analysed into their embedded steps recognizing all the business partners participating together with their interactions and their business roles to fulfil these processes. The current description adopts the table format described in *Table 7*:

ToE SC Process x analysis (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the SC process x (Record business partners' entities)
BP_1, BP_2, BP_3, … BP_i
Description (Process analysis describing how the business partners are involved in the SC process)
…….

Table 7 - SCS Business Partners description template.

- **ToE's infrastructure description** (if applicable)

  As ToE I is targeted into the business process evaluation, the current section is applicable only to VTS-ToE II and VTS-ToE III. Through this section, the ICT infrastructures of the cyber assets, the identified business partners utilize to perform their tasks within the underlined SC processes of the ToE are described and presented in a high-level overview. This is met according to the table format described in *Table 8*:

ToE infrastructures of the SCS Process x (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
BP_1	……
BP_2	……
BP_3	
BP_i	……

Table 8 - ToE's infrastructure description template.

- **Business process model generation**
  To help the conformity assessor better comprehend the SCS processes, their workflows and the business partners and assets engaged across these flows, a process diagram is developed, visualizing each identified SCS process of the ToE.

  Example
  For the VTS process "Standard Cargo Manifest" the following business process diagram is developed utilizing the BPMN 2.0 business process modelling notation.

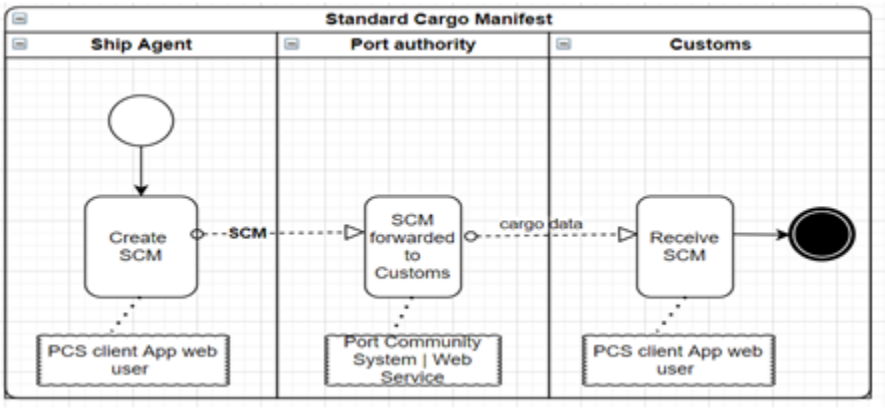


Figure 20 - "Standard Cargo Manifest": a business process model example.

The above figure shows the business process model of the “Standard Cargo Manifest” (SCM) process of the VTS. In particular, the process’s steps are visualized within the depicted workflow (Step1: Create SCM, Step2: SCM forwarded to Customs, Step3: Receive SCM) while the business partners involved in each step are represented into the three pools (swimlanes). Hence, in the current business process diagram the Ship Agent creates the SCM via the Port Community System (PCS) web application, the Port Authority forwards through its web service the SCM to the Customs to check and the Customs receives the document via the PCS web application and undertakes this responsibility

5.1.1 ToE I: Business view of the VTS-SCS

The current ToE falls under the CYRENE business SCS perspective. The underlined SCS is the Vehicle Transport Service (VTS) as defined in the introduction of section 5.1. “ToE I” sets the scope to evaluate all process-related threat scenarios of the VTS. The current section encompasses the business environment of ToE I: VTS processes and involved business partners. The processes under examination are dominant SCS processes that concern the overall VTS. Such SCS processes derive from an aggregation of industry sectors, such as automobile industry, maritime transport and logistics industry. The VTS-SCS is based upon the following four (4) business phases:

A. Vehicles Purchase Phase;
B. Shipment Phase;
C. Pre-arrival Phase and Vessel Arrival,
D. Vehicles Unloading and Delivery Phase.

The SCS phases encompass major SCS processes for the VTS provision as described below.

A. Vehicles Purchase Phase

The *Vehicles Purchase Phase* engages all the procedures an importer does for a vehicle purchase from an automobile Industry of the VTS. The SC processes of this phase are identified in terms of the importer’s activities and interactions with the automobile industry to proceed with a purchase order of vehicles. The automobile manufacturer (e.g., FIAT Chrysler Automobiles (FCA)) realizes sectorial vehicles components supplying and manufacturing processes. For instance, they purchase and consume components from several auto parts suppliers in the vehicle assembly and auto parts (that can be several thousands of components of different variants and part numbers), which are assembled for the vehicle during the production of the automobiles. The current ToE considers an overview of the VTS. Therefore, such sector-specific processes are not identified and examined in the current ToE. The Vehicles Purchase Phase consists of the Vehicles Order Dispatch process and the Contract Agreement on the Vehicle Purchase process:

- A1. Vehicles Order Dispatch process
- A2. Contract Agreement on the Vehicle Purchase process

B. Shipment Phase

The *Shipment Phase* encapsulates all the shipping formalities that lead to the maritime transportation of the vehicles from the port of origin to the destination port. It incorporates the Chartering Agreement Preparation & Negotiation, the Ship Formalities Arrangements and the Shipping Arrangements processes:

- B1. Chartering Agreement Preparation & Negotiation process
- B2. Ship Formalities Arrangements process
- B3. Shipping Arrangements process

C. Pre-arrival Phase

The *Pre-Arrival Phase* possesses distribution chain procedures that have to be arranged by the importer through a corresponding representative (agent) and the port, engaging various formalities regarding the vessel docking and stevedoring of the vehicles at the designated port car terminal of the port and the agent's interactions with other entities to accomplish these tasks, such as interactions with the Customs Authority. The phase encapsulates the Port Call Request, Standard Cargo Manifest, Entry Summary Declaration (ENS), Loading and Discharge List processes:

- C.1 Port call request process
- C.2 Standard cargo manifest process
- C.3 Entry Summary Declaration (ENS) process
- C.4 Loading and Discharge List process

D. Vessel Arrival, Vehicles Unloading and Delivery Phase

The *Vessel Arrival, Vehicles Unloading and Delivery Phase* includes a series of tasks among the key-players of the VTS that lead to a specific goal or produce a final result, referring to the delivery of the vehicles to the end customer (namely the importer in the current use case). This is instantiated by the completion of the vessel arrival procedures to the destination port and the vehicles unloading of the Car Carrier Vessel at the designated port car terminal. The current phase is supported by the Discharge vehicles, Customs declarations, Transportation order processes.

- D1. Discharge vehicles process
- D.2 Customs declarations process
- D.3 Transportation order process

Within the next two sections, the SCS processes are identified (section 5.1.1.1 Identification and description of SCS business processes of ToE I), the business partners are recognized and it is described how they are involved in each VTS process step (section 5.1.1.2 Identification and description of SCS business partners of ToE I and corresponding SCS business process models) and eventually the business process models are developed for each corresponding SCS process.

5.1.1.1 Identification and description of SCS business processes of ToE I
In this section, the recorded VTS processes for each SC phase, abovementioned, are specified.

A. Vehicles Purchase Phase

- A1. Vehicles Order Dispatch process

ToE "Vehicles Order Dispatch" process (A general description of the business process and its business goal)
The process aims to satisfy the end customers' requirements for automobile purchase and it refers to all the procedures undertaken for the preparation of the vehicles purchase order request.

Table 9 - "Vehicle Order Dispatch" process description.

- A2. Contract Agreement on the Vehicle Purchase process

ToE "Contract Agreement on the Vehicle Purchase" process (A general description of the business process and its business goal)
The SC process "Contract Agreement on the Vehicle Purchase" of the VTS relates to the procedures undertaken, in order to issue and sign a contract agreement between the interested parties towards a vehicles' purchase request.

Table 10 - "Contract Agreement on the Vehicle Purchase" process description.

B. Shipment Phase

- B1. Chartering Agreement Preparation & Negotiation process

ToE "Chartering Agreement Preparation & Negotiation" process (A general description of the business process and its business goal)
The process aims to highlight all the procedures undertaken for ship chartering including the negotiation actions.

Table 11 - "Chartering Agreement Preparation and Negotiation" process description.

- B2. Ship Formalities Arrangements process

ToE "Ship Formalities Arrangements" process (A general description of the business process and its business goal)
The current process describes some activities taken before the vessel reaches the local port to load or unload the vehicles. Critical activities in the current process are the Customs Clearance request, the docking permission and the control of the vessel's course during the authorization process.

Table 12 - "Ship Formalities Arrangements" process description.

- B3. Shipping Arrangements process

ToE "Shipping Arrangements" process (A general description of the business process and its business goal)

The process engages all the activities required to be implemented before the vehicles are distributed from the port of origin to the destination port via carrier vessel sea transport. The goal of the process is to fulfil all the prerequisites, in order to deliver the vehicles on time from one port to another, such as to prepare the respective documents and forms for the shipment, manage ship arrival procedures and control regional procedures.

Table 13 - "Shipping Arrangements" process description.

C. Pre-Arrival Phase

- C.1 Port Call Request process

ToE "Port Call Request" process (A general description of the business process and its business goal)
The SC process "Port Call Request" of the VTS can be described as the activities taken before the vessel reaches the local port for requesting port call including the nautical services (pilot, tugboats, and mooring).

Table 14 - "Port Call Request" process description.

- C.2 Standard Cargo Manifest process

ToE "Standard Cargo Manifest process" (A general description of the business process and its business goal)
The current process describes some activities taken before the vessel reaches the local port for declaring all the goods in the vessel.

Table 15 - "Standard Cargo Manifest" process description.

- C.3 Entry Summary Declaration (ENS) process

ToE "Entry Summary Declaration (ENS) process" (A general description of the business process and its business goal)
The current process describes some activities taken before the vessel reaches the local port for declaring all the goods on the vessel when accessing to the European customs area.

Table 16 - "Entry Summary Declaration (ENS)" process description.

- C.4 Loading and Discharge List process

ToE "Loading and Discharge List process" (A general description of the business process and its business goal)

The current process describes some activities taken before the vessel reaches the local port for informing the good to be loaded and discharged.

Table 17 - "Loading and Discharge List" process description.

D. Vessel Arrival, Vehicles Unloading and Delivery Phase

- D1. Discharge Vehicles process

ToE "Discharge Vehicles" (A general description of the business process and its business goal)
Once the car carrier vessel arrives at the destination port and the loading and the vehicles discharge list is sent to the Terminal Operator of the destination port on proper time and all preparation processes have been set, activities for discharging the vehicles from the vessel to the port take place.

Table 18 - "Discharge Vehicles" process description.

- D.2 Customs Declarations process

ToE "Customs Declarations" process (A general description of the business process and its business goal)
The Customs declarations is a mandatory process when importing goods with the Tax Agency's Custom. In this regard, the goods owner or its representative needs to submit the Single Administrative Document for goods from countries outside the EU or the corresponding document (e.g., Proof of Union Status). This is necessary before the goods can leave the customs compound, in this case the port.

Table 19 - "Customs Declarations" process description.

- D.3 Transportation Order process

ToE "Transportation Order" process (A general description of the business process and its business goal)
Road transportation is an important part of the logistics in the container transport chain, including a variety of actors. The interested parties in order to control the transportation flow and obtain a common knowledge of the operations, there is a documentation flow in parallel running with the physical flow of goods, i.e., the ordered vehicles. The current process describes the documentation required for the road transportation of the vehicles to the delivery to the end customer, namely the importer.

Table 20 - "Transportation Order" process description.

5.1.1.2 Identification and description of SCS business partners of ToE I and corresponding SCS business process models

In the current section, the SCS processes identified in section 5.1.1.1 Identification and description of SCS business processes of ToE I are further analysed into consequent steps and the business partners involved in these processes for the provision of the VTS are specified along with their business roles.

After presenting the SCS processes of the VTS along with the business partners involved, business process diagrams are developed for each identified process. These business process model visualizations aim to help the reader better comprehend the process workflow and the involved parties. The business process models are represented using the BPMN 2.0 modelling specification and are depicted after each business partners identification table for the corresponding specified SCS process.

A. Vehicles Purchase Phase

- A1. Vehicles Order Dispatch process

ToE "Vehicles Order Dispatch" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)
Importer, Automobile Industry
Description (Process analysis describing how the business partners are involved in the SC process)
The "Vehicles Order Dispatch" order is a process executed between the Importer (and the Automobile Industry. The importer sets the order for the Automobile Industry according to the end customers' demands. In particular, the following actions take place: Step 1. The Importer prepares a purchase order via his Ordering System that contains orders for a number of automobile Industries. Step 2. If the Automobile Industry does not approve it (e.g., lack of stock), the purchase order is returned to the customer (importer) for revision. If the Industry approves the task order, module generates a copy of the approval letter and e-mails it to the costumer (importer) together with the order file. The Manufacturer (Industry) deal with these procedures through an electronic commerce system (e.g.: a Part On line Catalogue and Ordering System). Step 3. The Importer enters funding information and uploads appropriate supporting document attachments in the Part On line System (whether it is available to interact directly on line).

Table 21 - Business partners involved in the "Vehicles Order Dispatch" process.

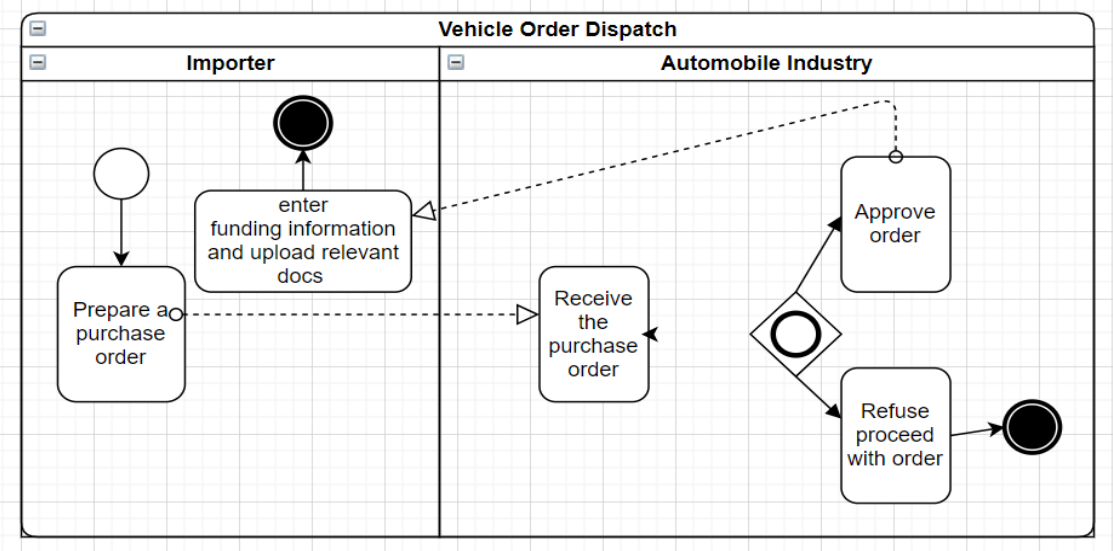


Figure 21 - Business process model for the "Vehicle Order Dispatch" process.

- A2. Contract Agreement on the Vehicle Purchase process

ToE "Contract Agreement on the Vehicle Purchase" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)
Automobile Industry, Importer
Description (Process analysis describing how the business partners are involved in the SC process)
The process is performed between the Industry and the Importer and it is activated as soon as the Vehicles Order Dispatch process is fulfilled. The business partners involved follow the subsequent steps enlisted, below, to deal with the process: Step 1. The Automobile Industry receives the funding documents. Step 2. The Automobile Industry prepares a pre-contract agreement and sends it to the Importer. Step 3. The Importer delves into the terms of the pre-contract and with the cooperation of a lawyer, a financial consultant and an insurance consultant sends a report to the Industry for amendments. Step 4. Then the Automobile Industry arranges a meeting with the Importer in order to negotiate for the contract. Step 5. During the meeting, they discuss with specialized officers about all the amendments required to get both parties satisfied. Step 6. Once both Importer and Industry have agreed upon the terms and conditions of the contract like pricing, documentation, freight charges, currency etc. and signed the contracts the latter proceeds to complete the order.

Lawyers and the Accounting Department of Industry issue all the appropriate formalities of the deal (invoicing, tax office declarations etc.) and send to the Importer the related documents. The Automobile Industry involved parties issues the associated documentation via enhanced technology platforms (i.e., ERPs) and database management systems. Fiscal transactions are operated through e-government services provided by a Taxation Information System. Fund transfers are achieved through wire transfers, direct deposits, ATM transactions and e-banking services via electronic, interactive communication channels. When the purchase procedures come to an end the Automobile Industry has to arrange the delivery of the vehicles to the Importer with Maritime Transportation at a specified time.

Table 22 - Business partners involved in the "Contract Agreement on the Vehicle Purchase" process.

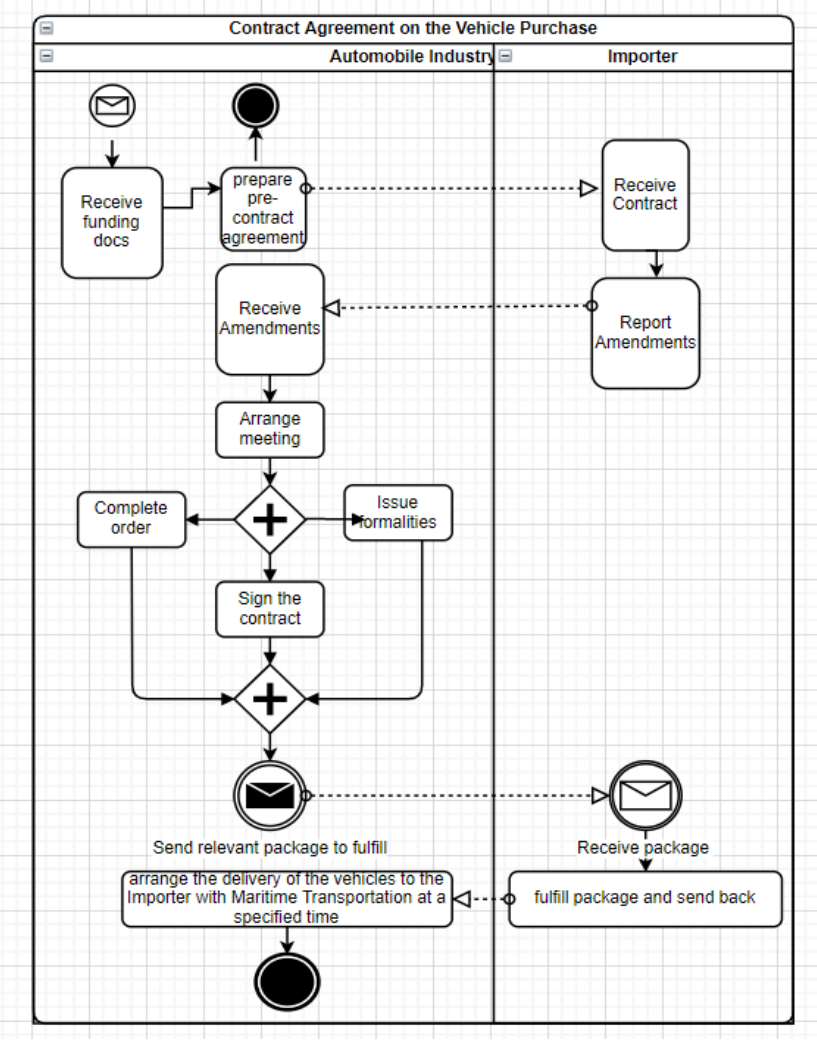


Figure 22 - Business process model for the "Contact Agreement on the Vehicle Purchase" process.

B. Shipment Phase

- B1. Chartering Agreement Preparation & Negotiation process

ToE "Chartering Agreement Preparation & Negotiation" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Charterer (Automobile Industry), Ship Owner, Shipbroker
Description (Process analysis describing how the business partners are involved in the SC process)
The Automobile Industry is seeking to contract with the Ship Owner for delivering the vehicle to the destination port defined by the Importer. To accomplish this goal the following activities take place: Step 1. Initiation of Chartering Agreement procedures. The Chartering Agreement (known as charter party) is a binding agreement between the Ship Owner and the Charterer (in the current scenario the Automobile Industry is the Charterer) indicating the certain conditions in which a vessel is rented regarding the vehicle transport. The most important clauses of a charter party are those defining the time-period allowed for loading and unloading the vessel and determining who undertakes the responsibility for the expenses involved. The Automobile Industry and the Ship Owner must come to a chartering agreement. More specifically, there are four principal methods of chartering a tramp ship summarized below: • Voyage charter, is the most common type according to which chartering refers to a given price for the transport of a certain vehicle for a one-way voyage between specific ports • Time charter, depends on hiring the vessel for a certain period of time • Bareboat or demise charter, is rarely used, described as an arrangement of hiring a vessel for a specified period without crew, insurance, stores or any other provision. As a result, the Charterer is entirely responsible for the vessel's legal and financial supporting • "Lump-sum" contracts are settled on a lump-sum basis, agreed upon a total and global price for simple and well-defined scope projects which are hardly possible to change. Step 2. After continuing negotiations between the interested parties, the charter party agreement is set reflecting the following main aspects: • time offers • counter (may be one, two or several counters exchanged) • recap of terms (partially fixed on subjects) • clean recap (final revision) • execution of charter party Step 3. The Automobile Industry informs the Shipbroker (an entity that acts as a negotiator between the Automobile Industry and the Ship Owner) about the specified shipment agreement conditions and terms dealt with the Importer. Step 4. The Ship Owner reports the Shipbroker on cargo related details, declaring the actual vehicles carrying capacity of the vessel.

Step 5. The Ship Owner and the Automobile Industry are under extended discussion through the Shipbroker, exchanging several counter offers until both parties lift the subjects on vessels.

Table 23 - Business partners involved in the "Chartering Agreement Preparation & Negotiation" process.

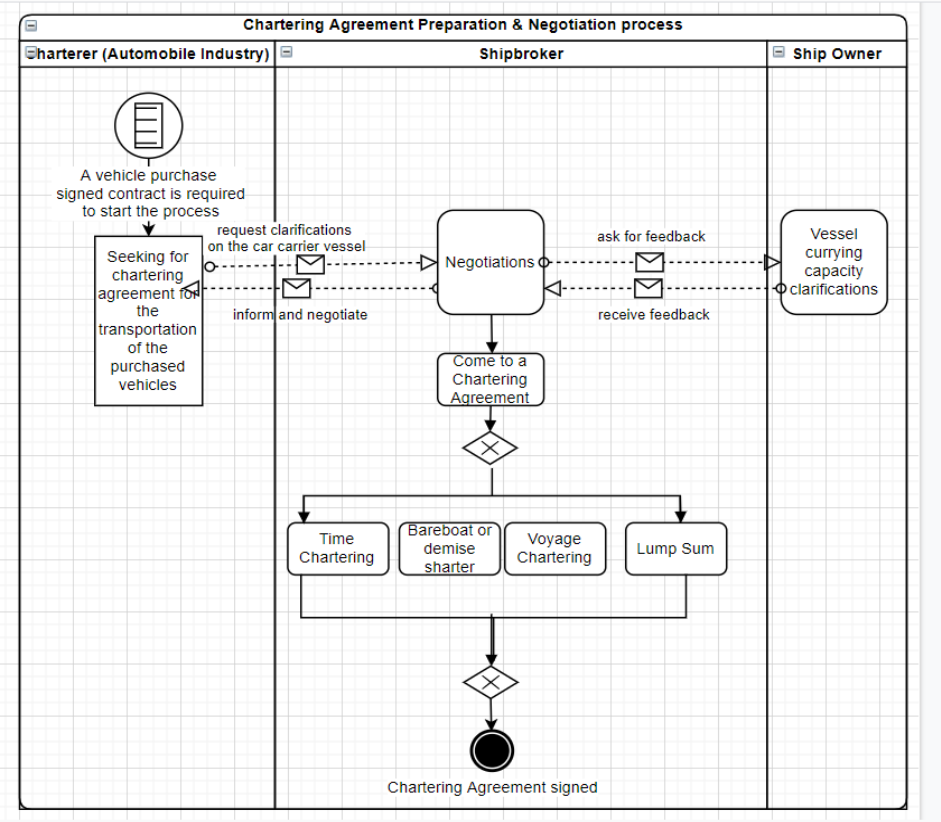


Figure 23 - Business process model for the "Chartering Agreement Preparation & Negotiation" process.

- B2. Ship Formalities Arrangements process

ToE "Ship Formalities Arrangements" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Customs, Port Authority
Description (Process analysis describing how the business partners are involved in the SC process)
Vehicles import/export in Maritime transport is subject to local Customs' audit. Only Local Customs can legitimate the vehicles shipment across the origin and destination port. According to this, the Ship Agent undertakes the responsibility to deal with the appropriate formalities arrangements for gaining from the Local Customs the permission to proceed with the vehicles' shipment. Customs Clearance is considered the documented permission

given by the Customs to import or export vehicles. Customs Clearance proves that all Customs duties have been paid and shipment procedures have been approved. To execute the process the following activities are undertaken:

Step 1. The Ship Agent submits the ship's associated documentation to the Customs requesting Customs Clearance. Typical formalities must have been fulfilled at the customs office for import/export activities including:

- the lodging and acceptance of the customs declaration;
- the declaration verification n and the supporting documentation; the physical examination of vehicles;
- measures for vehicles identification and controls on whether they are conformed to satisfy the appropriate conditions or restrictions;
- payment for import/export procedures and other charges (e.g., VAT, excise duties);
- release of vehicles for the customs procedure concerned.

Step 2. Once the Ship Agent obtains the Custom Clearance approval, he submits a request to the Port Community System (PCS) of the Port Authority to grant permission for the vessel to dock at the port. The Ship Agent's request is submitted via the corresponding online service of the PCS.

Step 3. The Port Community System (PCS) checks the Customs Clearance document authentication by data verification services requesting information from the Custom information system via an Electronic Data Interchange system (EDI) and reports the result. During the authorization processes, Port Authority observes via the Automatic Identification System (AIS) the vessel's course to ascertain that the marine transportation meets the primary consignment's specific requirements. Information on vessel position and an Arrival/Departure timetable is requested from the Port Authority via the Vessel Traffic Service. Vessel Traffic Service is a Port's Authority marine-traffic monitoring system, identifying vessel e-tracking and traffic services operations. The Port Authority uses the "MarineTraffic" intermodal web platform to retrieve information for the vessel's course, its geo-coordinates location and the vessel traffic in the adjacent sea area and control remotely the vessel's movement in case traffic on the water is high.

Step 4. The Port Authority provides permission for the vessel to dock, only if the following prerequisites occur:

- The vessel has not deviated from its route,
- The vessel's voyage has followed the regulatory compliance policies
- Marine traffic does not prevent the vessel from approaching the Port.

Step 5. As long as the above prerequisites are satisfied, the Local Agent must be informed from the Port Authority about the docking arrangements at a specific time before the vessel arrives at the local port to load (or unload) the vehicles.

Step 6. Before the vessel reaches the local Port consults the marine traffic live map and informs the Ship's Administration about the current sea traffic. Port Authority expert personnel monitor the vessel's movement and conducts it via AIS equipment to enter safely the port to dock. In particular, the internal communication between the Port Authority and the Local Agent is satisfied by utilizing AIS transponders broadcasting information via marine radar antennas VHF radio waves. In this manner, they can corporate in order to avoid a potential collision and to improve sea navigation.

Step 7. The Ship Agent makes the arrangements with the Public Administration (management of the ship formalities) regarding the authorisation process, ranging from the entry of the ship into the local port to the vehicles loading onto the vessel for shipping them to the

destination Port. The shipping arrangements are realized through data exchange using logistics infrastructures and port integrated systems. During the authorization process, shipping operations are monitored and controlled through networking technology of SCADA and AIS systems.

Table 24 - Business partners involved in the "Ship Formalities Arrangements" processs.

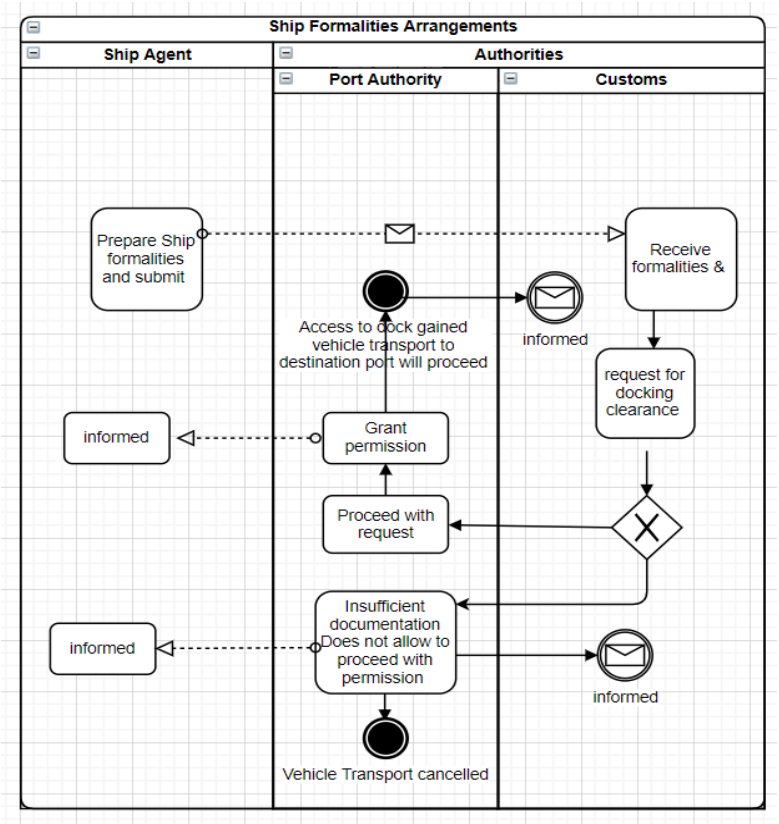


Figure 24 - Business process model for the "Ship Formalities Arrangements" process.

- B3. Shipping Arrangements process

ToE "Shipping Arrangements" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Local Agent, Insurance Company, Vehicles Transport Company, Importer
Description (Process analysis describing how the business partners are involved in the SC process)

The Ship Agent (representing the Ship Owner) is obligated to deliver the vehicles on time. A breach of contract can easily occur either for unreasonable delay or for unjustifiable departure from the usual and reasonable route. To achieve this, the following activities are implemented:
Step 1. The Ship Agent undertakes the responsibility to send all the pertinent documents (e.g., the Manifest document of the vessel, the docking clearance document) to the Importer's Local Agent.
Step 2. The Local Agent undertakes the responsibility for the ship arrival and controls the regional procedures:

- he communicates the Insurance Company to make an assessment report of the vehicles physical status and their transportation's service quality
- he employs a Vehicle Transport Company and arranges to receive and load the vehicles from the vehicle terminal at the destination port at a specified time.
- he deals with the relevant shipping formalities (exchanging information through logistics infrastructure, multi-modal platforms and communicating via telematics)

Step 3. The Local Agent informs the Importer about the status of the aforementioned procedures.

Table 25 - Business partners involved in the "Shipping Arrangements" process.

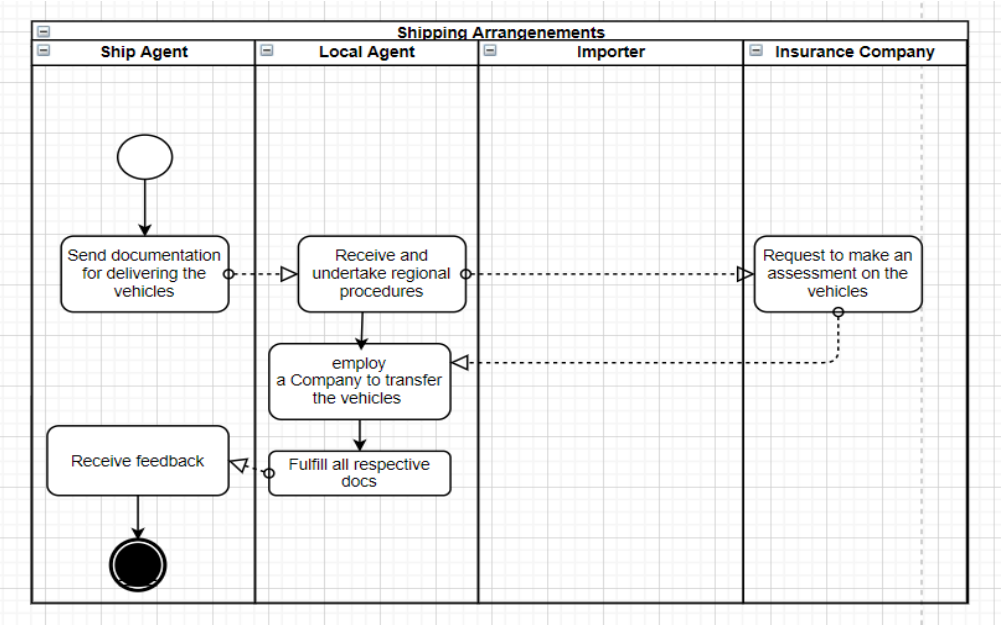


Figure 25 - Business process model for the "Shipping Arrangements" process.

C. Pre-Arrival Phase

- C.1 Port Call Request process

ToE "Port Call Request" Business Partners

(Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)

Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Port Authority, Customs, Terminal Operator
Description (Process analysis describing how the business partners are involved in the SC process)
The port calls process is a request from the Shipping Line or its Ship Agent to the Port Authority and the Harbourmaster's office, requesting a berth, giving details of the call and the vessel authorized. To achieve this, the following activities are implemented: Step 1. The Ship Agent sends the Port Authority data including the port of arrival, name of vessel, the carrier, previous and following ports of call. Once the port call corresponding authorisations for these requests are received the Ship Agent provides more information about passengers and crew, waste, berth requirements, expected operations (pilot, tug-boats, and mooring), and other relevant data. Step 2. Vehicles import/export in maritime transport is subject to local Customs' audit. By sending the request of port call, automatically opens a Customs registry for the customs clearance of goods that must be loaded or unloaded from the vessel. Step 3. The port calls information is used by Port Authority and the Terminal Operators to manage their resources accordingly preparing equipment, personnel, etc. All these communications are done using the Port Community System (PCS), which provides the users a client application to launch the service rapidly and be able to fulfil the requirements to send documentation electronically to the involved entities.

Table 26 - Business partners involved in the "Port Call Request" process.

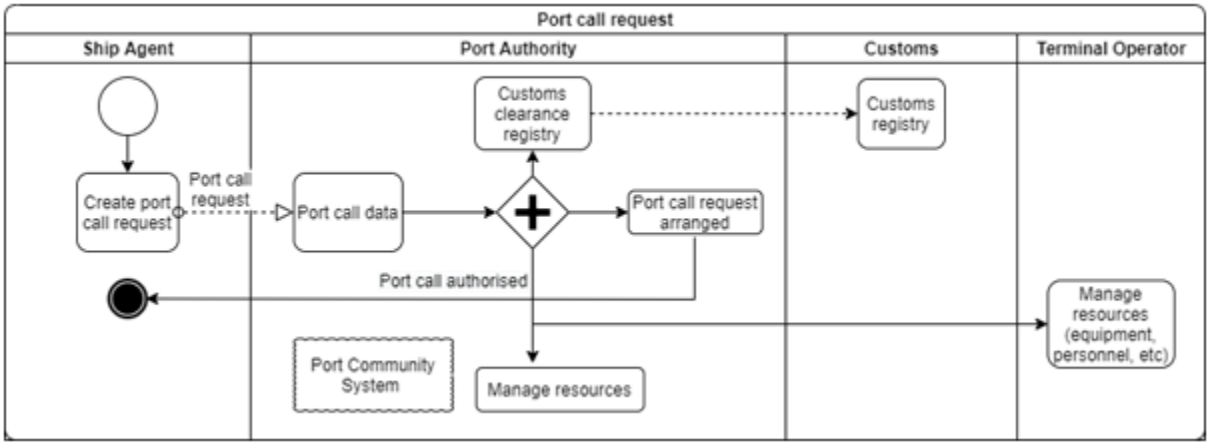


Figure 26 - Business process model for the "Port Call Request" process.

- C.2 Standard Cargo Manifest process

ToE "Standard Cargo Manifest" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)

Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Port Authority, Customs
Description (Process analysis describing how the business partners are involved in the SC process)
The Standard Cargo Manifest is the document that includes all the information related to a ship and the cargo transported in a ship for a particular trip and which is intended to be discharged/loaded during its port call. In this way, the information contained in a Summary Declaration is mainly divided into two sections: • Information related to the ship, trip and port call: this section includes the data referring to the name of the ship, flag, etc., indicating the ports of origin, destination that delimit the corresponding trip. In addition, it incorporates information for Customs, such as the concept of regular line, simplified transit procedures and the operations and actors involved in them. • Information related to the Cargo transported: this section contains three blocks of data, those related to the level of Bill of Lading, (B/L), those related to the consignment (a consignment is characterized by having a single tariff code and be integrated into a single Bill of Lading), and those that refer to equipment. Also at the starting level, it contains data related to the customs situation and clearance. Step 1. The Ship Agent, as the representative of the shipping Line, undertakes responsibility for sending the Standard Cargo Manifest at least one day before the arrival of the ship. Step 2. The message is received by the Port Authority. Step 3. The Standard Cargo Manifest is forwarded to the Customs. These communications are done using the Port Community System (PCS), which provides the users a client application to launch the service rapidly and be able to fulfil the requirements to send documentation electronically to the involved entities.

Table 27 - Business partners involved in the "Standard Cargo Manifest" process.

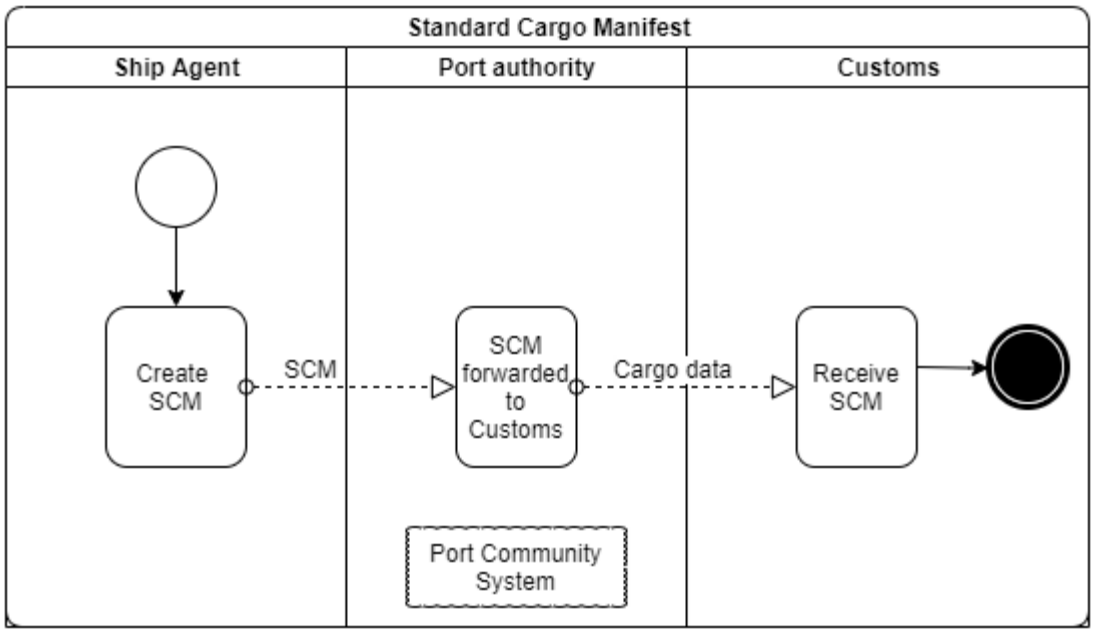


Figure 27 - Business model for the "Standard Cargo Manifest" process.

- C.3 Entry Summary Declaration (ENS) process

ToE "Entry Summary Declaration (ENS)" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Customs, Port Authority
Description (Process analysis describing how the business partners are involved in the SC process)
The Entry Summary Declaration (ENS) is a mandatory document which includes all the information related to the cargo transported in a ship. It is needed only when arriving to the first European port. The information in the document is quite similar to the Standard Cargo Manifest, although in this case contains all the cargo in the vessel and not only the cargo to be discharged to a specific port. Step 1. The Ship Agent, as the representative of the shipping Line, is engaged to send the ENS at least one day before the arrival of the ship together with the Standard Cargo Manifest. Step 2. The message is received by the Port Authority. Step 3. The message is forwarded to the Customs. These communications are done using the Port Community System (PCS), which provides the users a client application to launch the service rapidly and be able to fulfil the requirements to send documentation electronically to the involved entities.

Table 28 - Business partners involved in the "Entry Summary Declaration (ENS)" process.

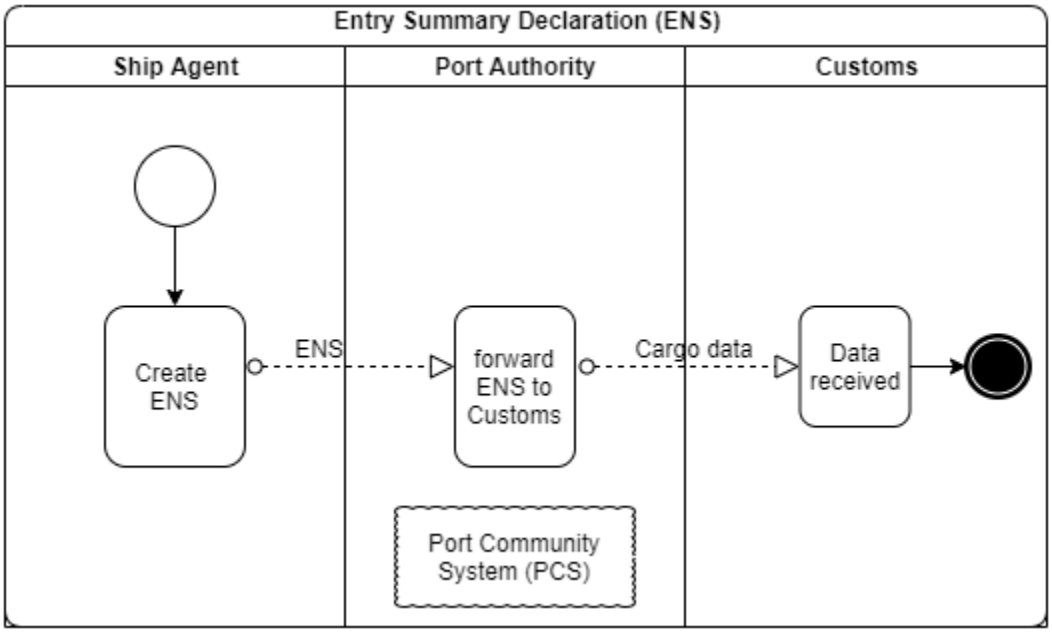


Figure 28 - Business process model for the "Entry Summary Declaration (ENS)" process.

- C.4 Loading and Discharge List process

ToE "Loading and Discharge List" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Ship Agent, Terminal Operator, Port Authority
Description (Process analysis describing how the business partners are involved in the SC process)
The loading and discharge list is a document which contains all the vessel loading and discharge containers, cars, or goods. The main information included in the document is the container type, dimensions, weight, temperature, seal, dangerous goods information, etc. Step 1. The Ship Agent sends the loading and discharge list to the Terminal Operator at least 12 hours before the arrival. Step 2. The Terminal Operator needs this information to manage all the resources needed for the process. Step 3. The Ship Agent receives a confirmation from the Terminal Operator of the loading and discharge of these containers when it is accomplished. These communications are done using the Port Community System (PCS), which provides the users a client application to launch the service rapidly and be able to fulfil the requirements to send documentation electronically to the involved entities.

Table 29 - Business partners involved in the "Loading and Discharge List" process.

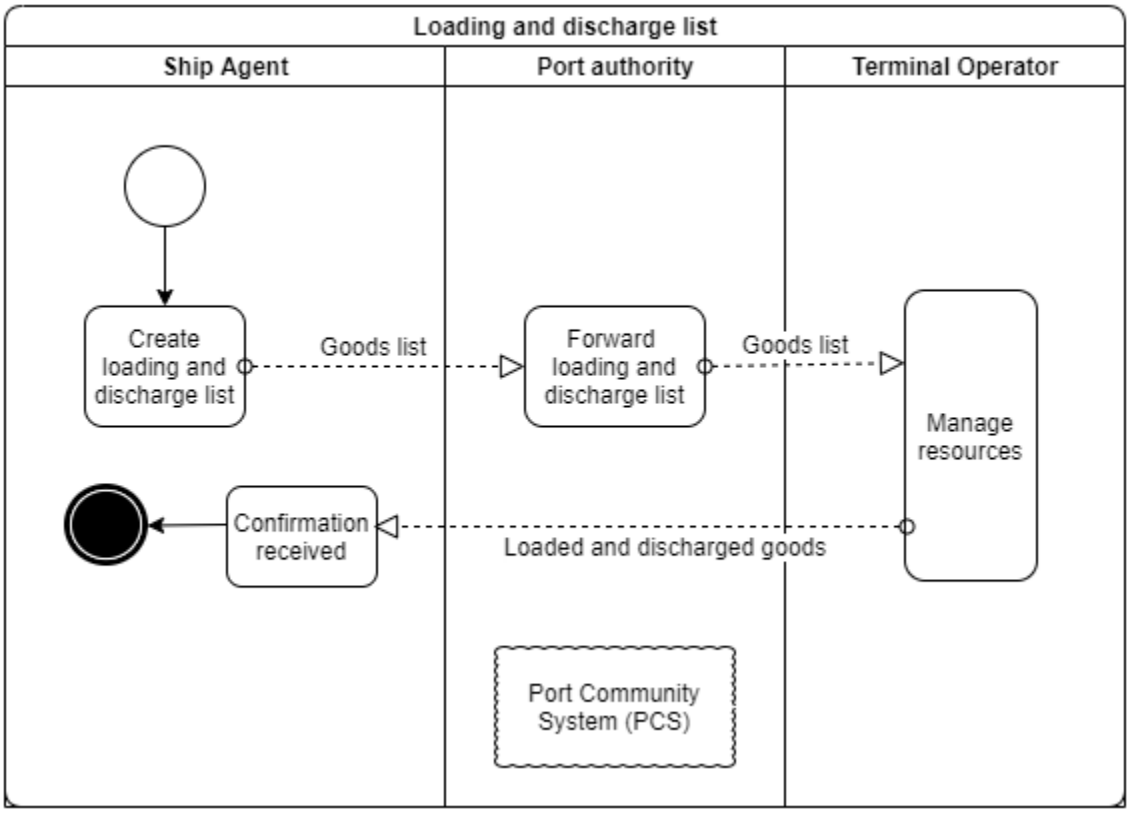


Figure 29 - Business process model for the "Loading and Discharge List" process.

D. Vessel Arrival, Vehicles Unloading and Delivery Phase

- D1. Discharge Vehicles process

ToE "Discharge Vehicles" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Terminal Operator (Docker)
Description (Process analysis describing how the business partners are involved in the SC process)
Once the vessel is docked in the port, the discharge of vehicles begins: Step 1. Dockers get on the vessel and discharge the vehicles driving towards the terminal yard. Step 2. Dockers have a mobile device connected to the TOS (Terminal Operating system) for receiving indications of the vehicles to be discharged and the area in the terminal yard to be parked.

Step 3. With this information terminal operators managers are aware of the situation of each vehicle and are able to manage the resources and the space.

Table 30 - Business partners involved in the "Discharge Vehicles" process.

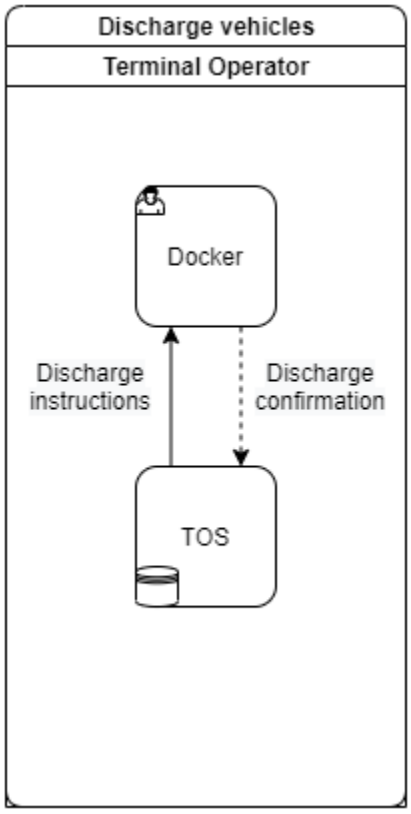


Figure 30 - Business process model for the "Discharge Vehicles" process.

- D.2 Customs Declarations process

ToE "Customs Declarations" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Freight Forwarder, Customs, Port Authority
Description (Process analysis describing how the business partners are involved in the SC process)
The Customs declarations is a mandatory process when importing goods with the Tax Agency's Custom. For that the goods owner or its representative needs to submit the Single Administrative Document for goods from countries outside the European union or the corresponding document (e.g. Proof of Union Status). This is necessary before the goods can leave the customs compound, in this case the port. The Single Administrative Document

includes the type of import, content, type of goods, value, currency, invoice, transport documents, origin, destination, weight, etc. Step 1. Before the truck arrives at the port to pick up the vehicles, the Freight Forwarder has to submit the Single Administrative Document to Customs. Step 2. Whether predefined conditions are met, the Customs authorises the request and the response is sent to the PCS in order to be available for involved stakeholders, including the automatic gate system in the port allows the trucks to leave the port. This process is done directly through the Customs system.

Table 31 - Business partners involved in the "Customs Declarations" process.

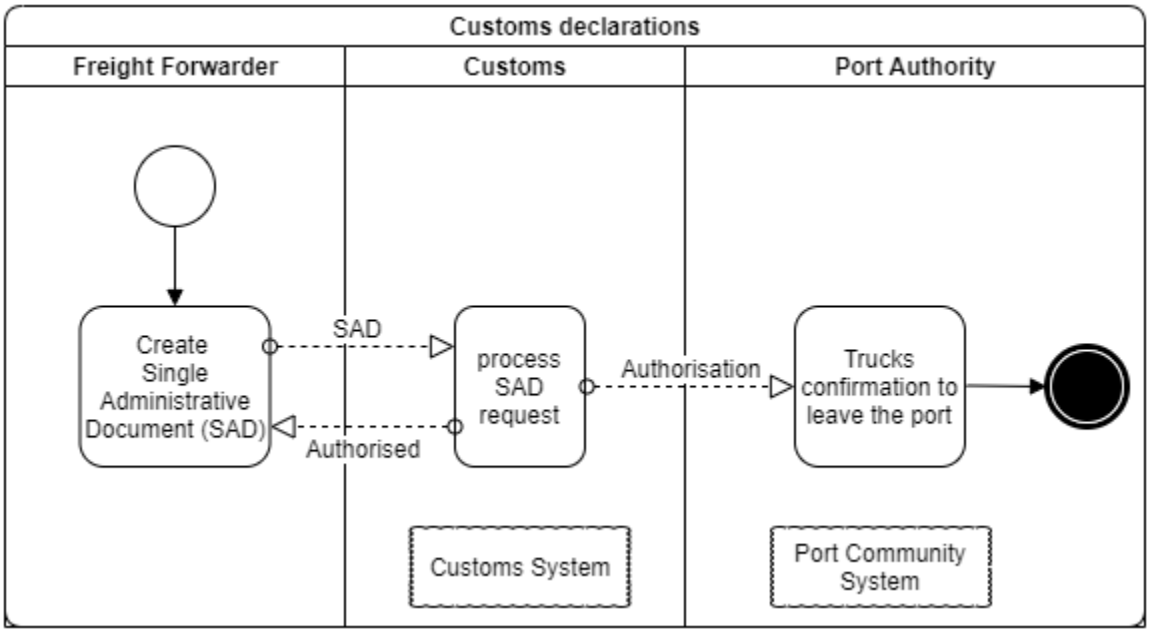


Figure 31 - Business process model for the "Customs Declarations" process.

- D.3 Transportation Order process

ToE "Transportation Order" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) participating in the process (Record business partners' entities)
Freight Forwarder, Ship Agent, Terminal Operator, Haulier Company
Description (Process analysis describing how the business partners are involved in the SC process)
Road transportation is an important part of the logistics in the container transport chain, and several actors are involved such as Freight Forwarders, Haulier Companies, Terminals, or Ship Agents. In order to have a common understanding of the operations, there is a documentation flow parallel to the physical flow of goods. For road transportation it is needed a

transport order, a document which determines the obligations between carrier and shipper. This document is local and therefore is regulated by national law. The main information included in the document is the container type, dimensions, weight, temperature, seal, dangerous goods information, etc. Step 1. The process starts when the importer or its Freight Forwarder request a transport. Step 2. The Ship Agent provides the transport order documentation to the Freight Forwarder and the Terminal Operator. Step 3. The Haulier Company completes the document assigning a truck. Step 4. Finally, when the prerequisites are met, the Terminal Operator confirms the delivery. Although this process is done thought the Port Community System (PCS) in the container transport, the vehicles transport process is still on paper and email. During the road transport operation, the driver needs the documentation is case is required by the traffic police or other security forces.

Table 32 - Business partners involved in the "Transportation Order" process.

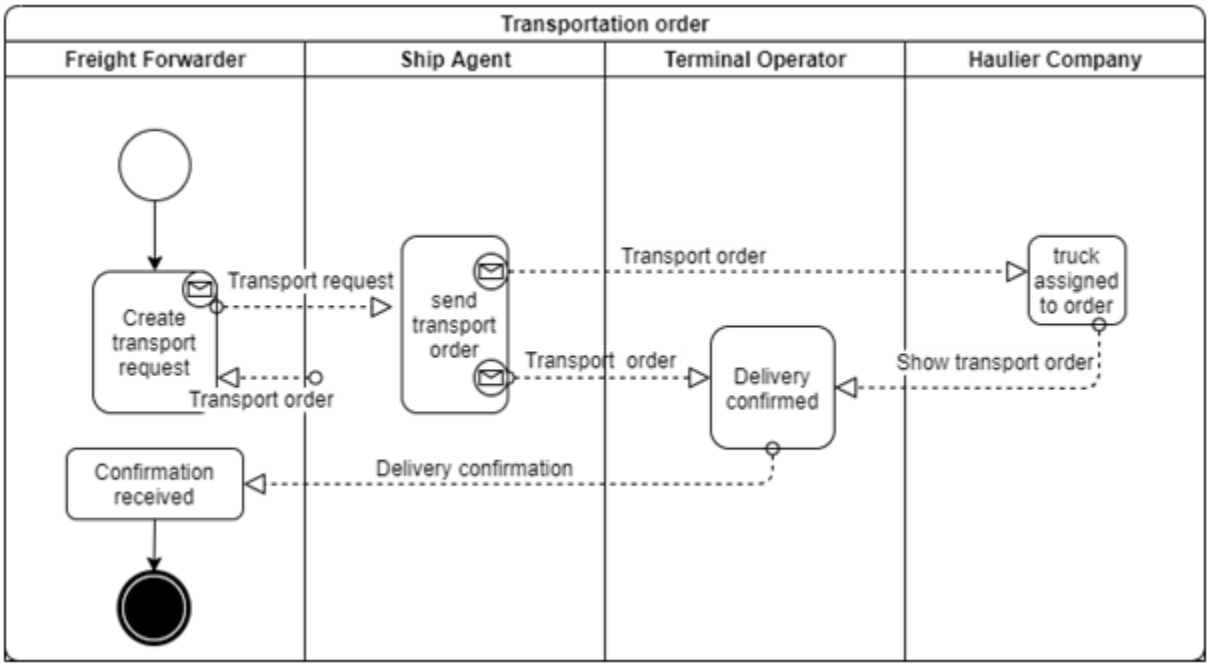


Figure 32 - Business process model for the "Transportation Order" process.

5.1.1.3 ToE's infrastructure description

Since ToE I adopts the business view, the assets and infrastructures do not belong to the current ToE's environment and they will not be subject to evaluation. The current section is N/A for ToE I (only the business processes together with their workflows are applied here).

5.1.2 ToE II: Technical view of the VTS-SCS

ToE II reflects the CYRENE technical SCS perspective. The underlined SCS is the Vehicle Transport Service (VTS) as defined in the introduction of section 5.1. “ToE II” sets the scope to evaluate SC processes of the VTS under a technical view that goes to a further analysis of the ICT infrastructure operating within these processes. The current section encompasses the business environment of ToE II: VTS processes, involved business partners and SC stakeholders and assets utilized for the completion of these processes. As mentioned previously in the beginning of section 5.1, in the current report under examination assets will be presented only with a high-level ICT infrastructure view, as it is referred at the beginning of section 5.1.

VTS-SCS processes derive from an aggregation of industry sectors, such as the automobile industry, maritime transport and logistics industry. The VTS-SCS, as presented in the previous section, are: Vehicles Purchase Phase; Shipment Phase; Pre-arrival Phase and Vessel Arrival, Vehicles Unloading and Delivery Phase. Each of the VTS-SCS phase encompasses major SCS processes for the VTS provision, which have been described in detail in ToE I (the business view of the VTS-SCS). Regarding the asset view description of the VTS-SCS, for the purpose of the current project to illustrate the CYRENE CA methodology, ToE II will reflect assets of the SCS processes concerning the Pre-Arrival phase and Vessel Arrival, Vehicles Unloading and Delivery phases, which mostly engage port-related processes and distribution chain processes (the port authority business partner of the current VTS use case will be the Valenciaport Foundation which is a pilot partner of the CYRENE project).

5.1.2.1 Identification and description of SCS business processes of ToE II

Within this section, the recorded VTS processes for each identified SCs phase are specified.

The VTS-ToE II SCS processes abovementioned, have already been described and analysed (section 5.1.1.1 Identification and description of SCS business processes of ToE I) and as they remain the same, no other actions required to be fulfilled in this section.

5.1.2.2 Identification and description of SCS business partners of ToE II

Process analysis and business partners identification of VTS-ToE II have already been described (section 5.1.1.2 Identification and description of SCS business partners of ToE I and corresponding SCS business process models) and as they remain the same, no other actions required to be fulfilled in this section.

5.1.2.3 ToE’s II infrastructure description

Since ToE II adopts a technical view, assets used for the VTS-SCS processes execution will be presented. The VTS-business partners (BPs) that participate in the SCS processes of the Pre-Arrival phase and Vessel Arrival, Vehicles Unloading and Delivery phases, were asked to report all assets used in the VTS processes. As mentioned previously, in the current document, only high-level infrastructure representations of the BPs that encompass these assets are displayed.
The under examination SCS processes according to which the infrastructure representations are depicted are enlisted below adopting the template structure that is stressed in the beginning of section 5.1:

C. Pre-arrival Phase

- C.1 Port Call Request process

VTS-SCS Assets involved in the "Port Call Request" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners (BPs) of the underlined SCS process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Port Authority	The Port Authority manages the PCS, an open and neutral electronic platform, that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. The is composed of the following elements of software and hardware: (a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has a recovery site with all the systems replicated, to ensure the availability. (b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system. (c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security. (d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019. (e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents. (f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019. (g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service. (h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.
Ship Agent	The Ship Agent is one of the main actors in the port call process. It needs access to the PCS to manage the operations. The systems used for that activity are the following hardware and software.; (a) To access the PCS, the Ship Agent has a laptop LENOVO Yoga C930 with the following characteristics: Intel® Core™ i5- 8250U processor, 8GB RAM DDR4, and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64.

	(c) The Ship Agent uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Microsoft Edge. (e) The shipping agent's laptop is protected with an AVG antivirus against viruses and malware software.
Terminal Operator	The systems needed by the Terminal Operator in order to access the PCS and manage the documental activity are the following hardware and software. (a) To access the PCS, the Terminal Operator has a laptop HP x360 1040 G6 with the following characteristics: Intel® Core™ i5-8265U processor, 8GB RAM DDR4, and 256 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Terminal Operator uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Google Chrome. (e) The Terminal Operator's laptop is protected with a Norton 360 antivirus against viruses and malware software.
Customs	Customs needs to receive the request to start the customs clearance of goods process. The systems used for that activity are the following hardware and software. (a) To receive the information from the PCS Customs has a server Dell PE R740. (b) The operating system on the server is a Microsoft Windows Server 2019. (c) Customs uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The server is protected with a Kaspersky Security Cloud antivirus against viruses and malware software.

Table 33 - Identified infrastructures of the "Port Call Request" process.

- C.2 Standard Cargo Manifest process

VTS-SCS Assets involved in the of the "Standard Cargo Manifest" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged BPs of the underlined SCS process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Port Authority	The Port Authority is managing the PCS, an open and neutral electronic platform that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. The is composed of the following elements of software and hardware:

	(a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has recovery site with all the systems replicated, to ensure the availability. (b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system. (c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security. (d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019. (e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents. (f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019. (g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service. (h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.
Ship Agent	The Ship Agent is one of the main actors in the Standard cargo manifest process. It needs access to the PCS to manage the operations. The systems used for that activity are the following hardware and software: (a) To access the PCS, the Ship Agent has a laptop LENOVO Yoga C930 with the following characteristics: Intel® Core™ i5- 8250U processor, 8GB RAM DDR4, and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Ship Agent uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Microsoft Edge. (e) The shipping agent's laptop is protected with an AVG antivirus against viruses and malware software.
Customs	Customs needs to receive the request to manage the customs clearance of goods process. The systems used for that activity are the following hardware and software: (a) To receive the information from the PCS Customs has a server Dell PE R740. (b) The operating system on the server is a Microsoft Windows Server 2019.

	(c) Customs uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The server is protected with a Kaspersky Security Cloud antivirus against viruses and malware software.

Table 34 - Identified infrastructures of the "Standard Cargo Manifest" process.

- C.3 Entry Summary Declaration (ENS) process

VTS-SCS Assets involved in the "Entry Summary Declaration (ENS)" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Port Authority	The Port Authority is managing the PCS, an open and neutral electronic platform that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. The is composed of the following elements of software and hardware. (a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has recovery site with all the systems replicated, to ensure the availability. (b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system. (c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security. (d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019. (e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents. (f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019. (g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service. (h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.

Ship Agent	The Ship Agent is one of the main actors in the Entry Summary Declaration process. It needs access to the PCS to manage the operations. The systems used for that activity are the following hardware and software. (a) To access the PCS, the Ship Agent has a laptop LENOVO Yoga C930 with the following characteristics: Intel® Core™ i5- 8250U processor, 8GB RAM DDR4, and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Ship Agent uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Microsoft Edge. (e) The shipping agent's laptop is protected with an AVG antivirus against viruses and malware software.
Customs	Customs needs to receive the request to manage the customs clearance of goods process. The systems used for that activity are the following hardware and software. (a) To receive the information from the PCS Customs has a server Dell PE R740. (b) The operating system on the server is a Microsoft Windows Server 2019. (c) Customs uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The server is protected with a Kaspersky Security Cloud antivirus against viruses and malware software.

Table 35 - Identified infrastructures of the "Entry Summary Declaration (ENS)" process.

- C.4 Loading and Discharge List process

VTS-SCS Assets involved in the "Loading and Discharge List" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Port Authority	The Port Authority is managing the PCS, an open and neutral electronic platform that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. The is composed of the following elements of software and hardware. (a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has recovery site with all the systems replicated, to ensure the availability.

	(b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system. (c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security. (d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019. (e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents. (f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019. (g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service. (h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.
Ship Agent	The Ship Agent is one of the main actors in the Loading and discharge list process. It needs access to the PCS to manage the operations. The systems used for that activity are the following hardware and software. (a) To access the PCS, the Ship Agent has a laptop LENOVO Yoga C930 with the following characteristics: Intel® Core™ i5- 8250U processor, 8GB RAM DDR4, and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Ship Agent uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Microsoft Edge. (e) The shipping agent's laptop is protected with an AVG antivirus against viruses and malware software.
Terminal Operator	The systems needed by the Terminal Operator in order to access the PCS and manage the documental activity are the following hardware and software. (a) To access the PCS, the Terminal Operator has a laptop HP x360 1040 G6 with the following characteristics: Intel® Core™ i5-8265U processor, 8GB RAM DDR4, and 256 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Terminal Operator uses Microsoft Office 365 and Adobe Reader to manage and create their documents.

	(d) The browser chosen to access the PCS web application is Google Chrome. (e) The Terminal Operator's laptop is protected with a Norton 360 antivirus against viruses and malware software.

Table 36 - Identified infrastructures of the "Loading and Discharge List" process.

D. Vessel Arrival, Vehicles Unloading and Delivery Phase

- D1. Discharge Vehicles process

VTS-SCS Assets involved in the "Discharge Vehicles" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Terminal Operator	The systems needed by the Terminal Operator in order to manage the Discharge vehicles process are the following hardware and software. (a) To manage the operations, the Terminal Operator has a laptop HP x360 1040 G6 with the following characteristics: Intel® Core™ i5-8265U processor, 8GB RAM DDR4, and 256 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Terminal Operator uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Google Chrome. (e) The Terminal Operator's laptop is protected with a Norton 360 antivirus against viruses and malware software. (f) Dckers exchange information with a MUNBYN PDA Android 8.1 Honeywell with barcode scanner. (g) TOS systems is hosted on a server Lenovo ThinkSystem SR665.

Table 37 - Identified infrastructures of the "Discharge Vehicles" process.

- D.2 Customs Declarations process

VTS-SCS Assets involved in the "Customs Declarations" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description

Port Authority	The Port Authority is managing the PCS, an open and neutral electronic platform that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. It receives Single Administrative Document request response from Customs. The is composed of the following elements of software and hardware: (a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has recovery site with all the systems replicated, to ensure the availability. (b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system. (c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security. (d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019. (e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents. (f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019. (g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service. (h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.
Customs	Customs systems are managing the Customs declarations requests. The systems used for that activity are the following hardware and software: (a) To receive the information from the PCS Customs has a server Dell PE R740. (b) The operating system on the server is a Microsoft Windows Server 2019. (c) Customs uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The server is protected with a Kaspersky Security Cloud antivirus against viruses and malware software.
Freight Forwarder	The systems needed by the Freigt Fowarder to exchange and manage the documental activity are the following hardware and software. (a) To send the information the Freight Fowarder has a laptop Asus ZenBook UX325EA-EG016T with the following characteristics: Intel® Core™ i5- 1135G7 processor, 8GB RAM and 512 GB SSD storage.

	(b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Freight Fowarder uses Microsoft Office 365 and and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Mozilla Firefox. (e) The Freight Fowarder's laptop is protected with a McAfee Total Protection antivirus against viruses and malware software.

Table 38 - Identified infrastructures of the "Customs Declarations" processs.

- D.3 Transportation Order process

VTS-SCS Assets involved in the "Transportation Order" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Ship Agent	The Ship Agent is one of the actors in the Transportation order process. It needs to exchange documents with other stakeholders involved to manage the road operations. The systems used for that activity are the following hardware and software. (a) To access the PCS, the Ship Agent has a laptop LENOVO Yoga C930 with the following characteristics: Intel® Core™ i5- 8250U processor, 8GB RAM DDR4, and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Ship Agent uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Microsoft Edge. (e) The shipping agent's laptop is protected with an AVG antivirus against viruses and malware software.
Terminal Operator	The systems needed by the Terminal Operator in order to manage the documental activity are the following hardware and software: (a) To access the PCS, the Terminal Operator has a laptop HP x360 1040 G6 with the following characteristics: Intel® Core™ i5-8265U processor, 8GB RAM DDR4, and 256 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Terminal Operator uses Microsoft Office 365 and Adobe Reader to manage and create their documents.

	(d) The browser chosen to access the PCS web application is Google Chrome. (e) The Terminal Operator's laptop is protected with a Norton 360 antivirus against viruses and malware software.
Freight Forwarder	The systems needed by the Freight Fowarder to exchange and manage the documental activity are the following hardware and software: (a) To send the information the Freight Forwarder has a laptop Asus ZenBook UX325EA-EG016T with the following characteristics: Intel® Core™ i5- 1135G7 processor, 8GB RAM and 512 GB SSD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Freight Fowarder uses Microsoft Office 365 and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Mozilla Firefox. (e) The Freight Fowarder's laptop is protected with a McAfee Total Protection antivirus against viruses and malware software.
Haulier Company	The Haulier Company is involved in the transport operations, so it needs access to the order of transportation document. Furthermore this document is the necessary justification to pick up the goods and enter the port premises. The systems used for that activity are the following hardware and software. (a) To access the PCS the haulier has a laptop Acer Aspire 3 A515-54-72TH with the following characteristics: Intel® Core™ i7- 10510U processor, 8GB RAM and 256GB HDD storage. (b) The laptop has the last Microsoft operating system, Windows 10 x64. (c) The Haulier uses Microsoft Office 2016 and and Adobe Reader to manage and create their documents. (d) The browser chosen to access the PCS web application is Google Chrome. (e) The haulier's laptop is protected with a Bitdefender GravityZone antivirus against viruses and malware software. (f) The haulier needs a printer because the driver of the truck has to have the order of transportation printed. It has a Brother HL- L2370DN.

Table 39 - Identified infrastructures of the "Transportation Order" process.

The business process models of the current VTS-ToE II SCS respective processes have been already developed in section 5.1.1.2 and as they remain the same no other actions required to be fulfilled in this section.

5.1.3 ToE III: Sectorial view of the VTS-SCS

"ToE III" reflects sector-specific processes of automotive manufacturer, and its SC assets that hosts and uses in order to participate in the VTS entire SCS. "ToE III" sets the scope to evaluate SC processes under a sectorial perspective that goes to a further analysis of the ICT infrastructure operating within these processes. As for the previous ToE, the current section encompasses the business environment of ToE III: processes, involved business partners and SC stakeholders and the ICT infrastructure they utilize for the completion of these processes. The processes under examination that will be analysed are enlisted below adopting the template structure that is stressed in the beginning of the section 5.1.

The SC processes described here are related to the Inbound Logistics phase of components shipment, from the assembly plant to the production plant, and they are listed below:

1. Supply of partial-assembled components
2. Supply of the finished components
3. Monitoring of components during transportation
4. Vehicle Assembly

ToE III reflects the CYRENE sectorial SC perspective. It is linked to the Vehicle Transport SC and to the related Vehicle Transport Service (VTS) defined in the introduction of section 5.1.

5.1.3.1 Identification and description of SCS business processes of ToE III

Within this section, the business processes for the Inbound Logistics phase are specified.

- 1 Supply of partial-assembled components

ToE "Supply of partial-assembled components" process (A general description of the business process and its business goal)
The process involves the steps for the supply and execution of the final assembly of partial-assembled parts provided by external suppliers. The current process consists in all the operations needed to supply the pre-assembled parts and perform the final assembly, check their quality and store them before shipping them to the car manufacturing plant. Not all parts need an intermediate assembly and in that case they are directly supplied from the components supplier plant to the vehicle production plant.

Table 40 - Supply of partial-assembled components process description.

- 2 Supply of finished components

ToE "Supply of finished components" process

(A general description of the business process and its business goal)
This process is related to the transportation of finished components from the warehouse where they have been stored after intermediate assembly to the car manufacturing plant, where they are assembled with the rest of vehicle parts. This process involves the following operations: transportation documents arrangement, loading of components on containers, truck formalities arrangement, loading of containers on the truck. The shipment is executed by an external supply service provider, while the management of the whole process is by FCA Supply Chain Management Area.

Table 41 - "Supply of finished components" process description.

- 3 Monitoring of components during transportation

ToE "Monitoring of components during transportation" process (A general description of the business process and its business goal)
During the Inbound Logistics, IoT are used to track, trace, and monitor the quality of components transported on containers from the supplier plant to the vehicle production plant. The main objective for the use of these devices is the monitoring of containers parameters during transportation from the assembly plant to the FCA production plant. The current process happens in parallel with the previous one.

Table 42 - "Monitoring of components" process description.

- 4 Vehicle Assembly

ToE "Vehicle Assembly" process (A general description of the business process and its business goal)
The components are received, assembled and the final quality is checked in the production plant. Main steps in this process regards the unloading of components, the registration in the plant internal systems and the vehicle manufacturing.

Table 43 - "Vehicle Assembly" process description.

5.1.3.2 Identification and description of SCS business partners of ToE III

In the current section, the SC processes identified in section 5.1.3.1 are further analyzed into consequent steps and the business partners involved in these processes for the provision of the Inbound Logistics are specified along with their business roles.

- 1 Supply of partial-assembled components

ToE "Supply of partial-assembled components" Business Partners

(Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)
Components Supplier, Intermediate assembly plant, Vehicle Plant SC Manager, Warehouse
Description (Process analysis describing how the business partners are involved in the SC process)
This process is executed in the Intermediate Assembly plant. Here, the Supply Chain Manager makes order of partial assembled components, according to the production plant demand. Then, the external supplier responds to the request, sending the material to the plant where the parts assembly is executed. Finally, after the components are finished, they are stored in a warehouse, before they are shipped to the manufacturing plant, where they are assembled with the other vehicle parts.

Table 44 - Business partners identification and analysis of the "Supply of partial-assembled components" process.

- 2 Supply of finished components

ToE "Supply of finished components" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)
Vehicle plant SC Manager, Warehouse, Supply service provider
Description (Process analysis describing how the business partners are involved in the SC process)
This process starts with the request of components supply by the SC manager. The request is received and then the seal needed for the transportation of the material is produced. The information on the warehouse stock is updated and then the Supply service provider proceed with the loading of containers on the trucks. After all documentation is ready and the truck has been loaded, the transportation towards the final assembly plant starts.

Table 45 - Business partners identification and analysis of the "Supply of finished components" process.

- 3 Monitoring of components during transportation

ToE "Monitoring of components during transportation" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)

Supply Chain Manager, Vehicle Assembly plant
Description (Process analysis describing how the business partners are involved in the SC process)
The FCA Supply Chain Manager is the only actor in the monitoring process. He needs to access a web application to monitor the behavior of containers' parameters and localization. By using this system, he/she can have knowledge about events that could endanger the quality of the transported material, i.e.: high vibrations or temperature shocks, and also he/she can be informed about the position of the truck, and then update the Estimated Time of Arrival (ETA). Thanks to the near-real time data about quality conditions and localization of the material during the shipment, the final assembly plant is able to schedule and/or reschedule, if needed, the production.

Table 46 - Business partners identification and analysis of the "Monitoring of components during transportation" process.

- 4 Vehicle Assembly

ToE "Vehicle Assembly" Business Partners (Process analysis, identifying and describing all the business partners participated in the current underlined SC process and their roles within the process (taking into account the cyber assets operating to support their interconnections)
Business Partners (BP_i) Participating in the process (Record business partners' entities)
Vehicle assembly plant, Vehicle plant SC Management
Description (Process analysis describing how the business partners are involved in the SC process)
As soon as the components arrive at the final assembly plant, the SC manager updates information about the stock available. The components are registered in the internal systems of the plant. Then their quality is checked and if the control is passed, they proceed to the production, where they will be assembled with the other parts of the vehicle.

Table 47 - Business partners identification and analysis of the "Vehicle Assembly" process.

5.1.3.3 ToE's infrastructure description

Through this section, high level ICT infrastructure representations that are used by business partners who are involved in the identified SC processes are provided.

- 1 Supply of partial-assembled components

ToE infrastructures of the "Supply of partial-assembled components" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description

Components Supplier	The asset utilized by the components supply in this process is the so called “eSupplierConnect”. It is a portal providing useful features to improve performance, collaboration and communication between FCA and supplier partners. It allows this BP to receive orders by the SC Manager requiring the material. (a) This system is hosted on a database. (b) Data about all the actors involved in the activity and data produced are stored in a relational database Microsoft SQL server. (c) It is reachable through a laptop. (d) To ensure the security and integrity of the entire system, FCA internal regulations in terms of ICT security are followed.
Intermediate assembly plant	In the Intermediate Assembly plant, the main assets utilized are the Manufacturing Execution System (MES) and the Material Requirements Planning (MRP). The first one is used to track and document all the steps of the transformation of raw materials to finished components, while the second one is used for process planning, scheduling and inventory control. The hardware required for these systems are servers with high computational capacity. In fact, they leverage on optimization algorithms that uses a lot of input parameters in order to organize, plan, schedule, reschedule, register all the assembly materials and operations, maximizing efficiency and improving the assembly output.
Vehicle Plant SC Manager	This BP is the actor who starts the whole process. He utilizes the eSupplierConnect portal, that has been already described above, to make the demand for material supply.
Warehouse	Here the main actors are operators who provide to organize and execute procedures and manual operations for the material handling. The system utilized for managing data about warehouse material is the Warehouse Management System. (a) This system is hosted on a server. (b) Data about all the actors involved in the activity and data produced are stored in a relational database Microsoft SQL server. (c) To ensure the security and integrity of the entire system, company internal regulations in terms of ICT security are followed.

Table 48 - Identified infrastructures of the “Supply of partial-assembled components” process.

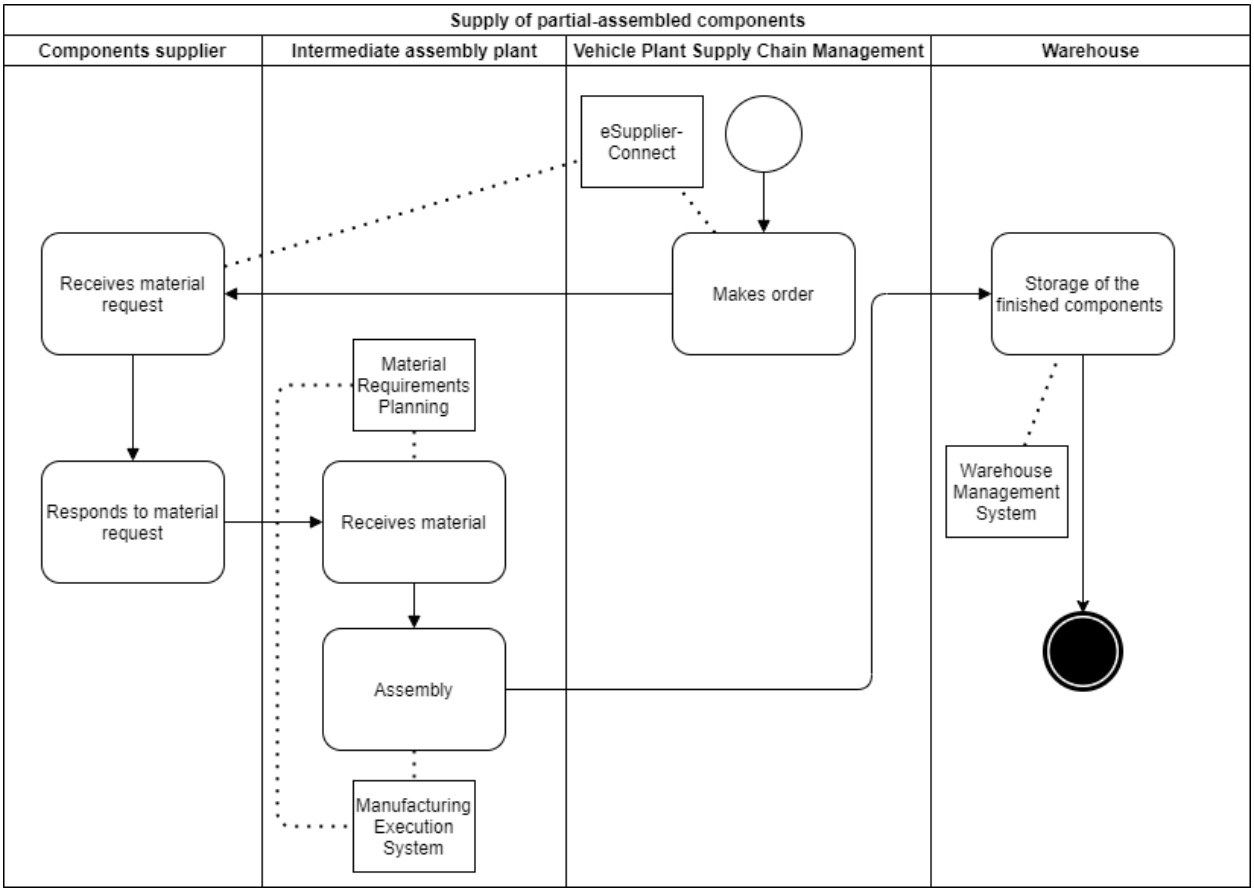


Figure 33 - Business process model for the"Supply of partial-assembled components" process.

- 2 Supply of finished components

ToE infrastructures of the "Supply of finished components" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Vehicle Plant SC Manager	This BP is the actor who starts this process. He utilizes the eSupplierConnect portal, that has been already described above, to notify to the SC service provider that the material is ready for pick-up.
Warehouse	The main tool utilized in the Warehouse in this process is the Transportation Management System (TMS), which is a FCA internal system. Here all the data related to the shipment operations are managed and collected and the transport documentation is issued. (a) This system is hosted on a server. (b) Data about all the actors involved in the activity and data produced are stored in a relational database Microsoft SQL server. (c) It is reachable through a laptop.

	(d) To ensure the security and integrity of the entire system, company internal regulations in terms of ICT security are followed. Moreover, the WMS is used also in this process, in order to update information on material available in the warehouse.
Supply Service provider	The main system used by this BP is the eSupplierConnect already described above. In fact, through it, he receives the demand for providing supply service and then, after he sends the information

Table 49 - Identified infrastructures of the "Supply of finished components" process.

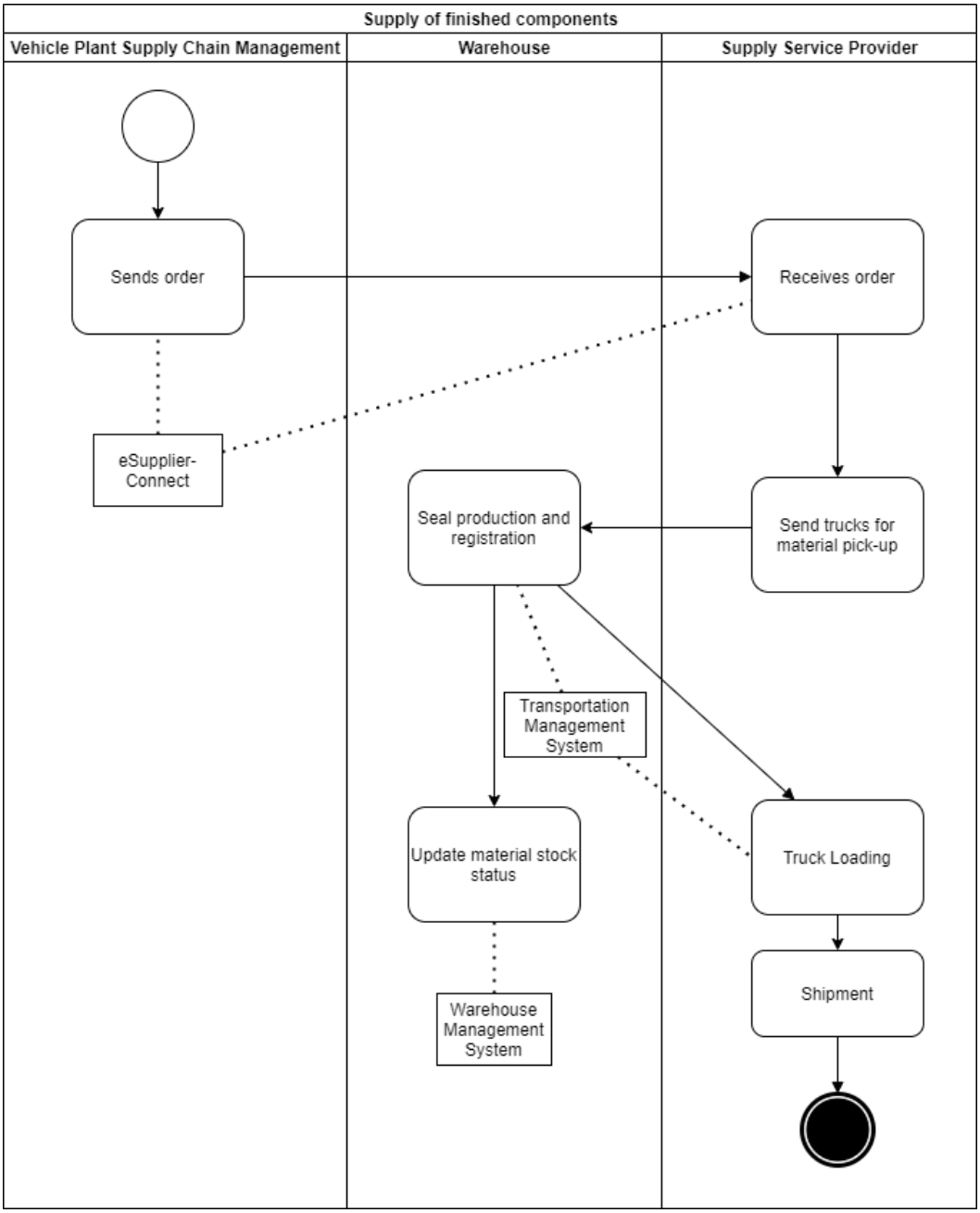


Figure 34 - Business process model for the "Supply of finished components" process.

- 3 Monitoring of components during transportation

ToE infrastructures of the "Monitoring of components" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Supply Chain Manager	The FCA Supply Chain Manager the main actor in monitoring process. He needs access to the i4.0 web application to monitor the behaviour of process parameters. The systems used for that activity are the following hardware and software. (a) He uses the Transport Management System, for the documents and all information related to the material supply (i.e. information on the orders, on the transportation documentation, on the trucks, and so on) (b) Data from the loggers are visualized on the web application (c) To access the web application he needs a laptop and credentials (d) Data can be visualized in real time or downloaded for analysis. Downloaded data can be visualized by using Microsoft Excel (e) Data are stored on an external SQL server Loggers with 3G/4G connection are installed on the containers. The wireless connection (3G/4G) has no protection measures (e.g. encryption) and the data are sent as clear text. There is only a basic authentication mechanism for local access, and the suppliers have permission to access/modify.
Vehicle Assembly Plant	The main tool utilized in this process are the Transportation Management System (TMS), the Warehouse Management System (WMS) and the Material Requirements Planning (MRP). The features of the hardware needed for using these systems are the same of the ones listed in the tables above.

Table 50 - Identified infrastructures of the "Monitoring of components" process.

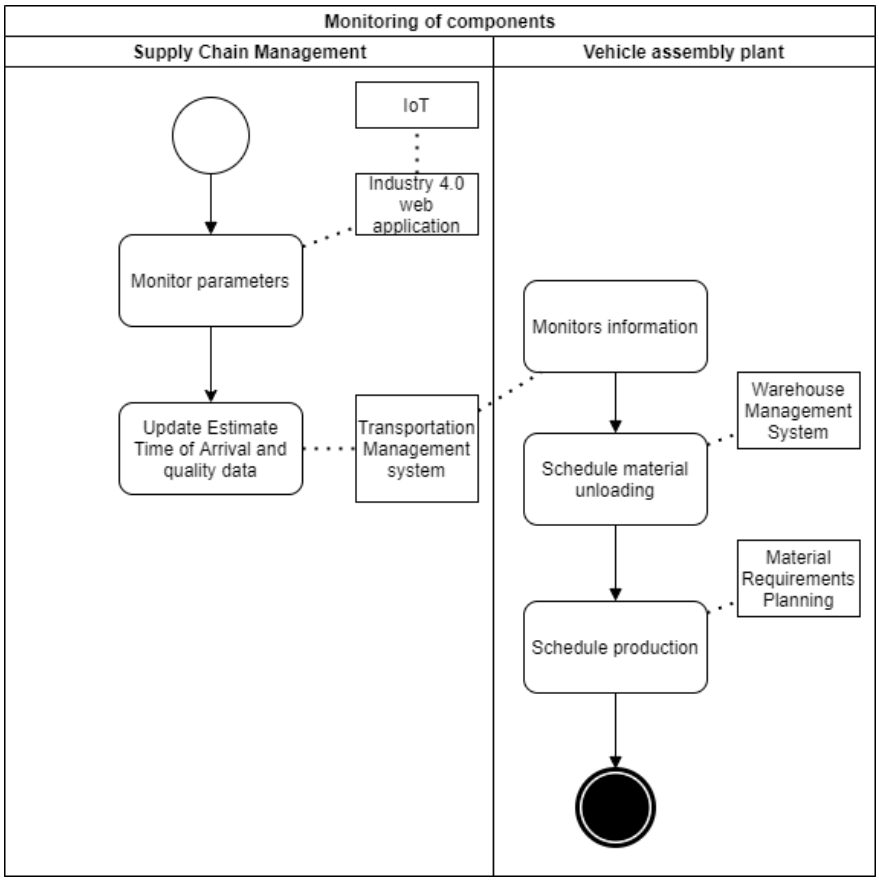


Figure 35 - Business process model for the "Monitoring of components" process.

- Vehicle Assembly

ToE infrastructures of the "Vehicle Assembly" Process (Infrastructure representations of the cyber assets and the overall technical equipment required to cover communications and transactions among the engaged business partners of the underlined SC process; data exchange services between heterogeneous systems and interoperable functionalities are also mentioned wherever exist)	
Business Partner (BP_i)	Description
Vehicle Plant SC Manager	The systems used here by the BP are the Material Requirements Planning (MRP) and the Transportation Management System (TMS)
Vehicle Assembly Plant	The tools used in this process are the Transportation Management System (TMS), the Warehouse Management System (WMS) and the Manufacturing Execution System (MES).

Table 51 - Identified infrastructures of the "Vehicle Assembly" process.

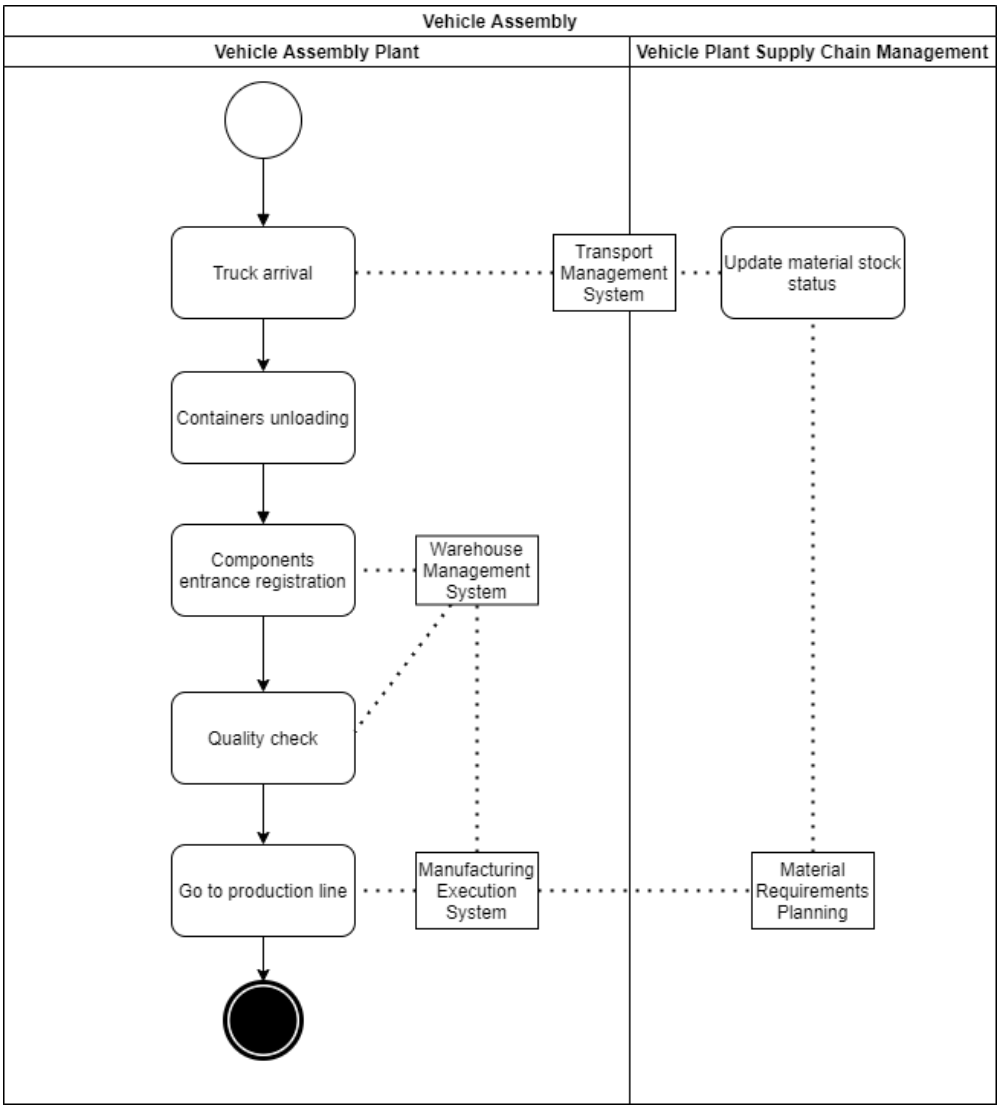


Figure 36 - Business process model for the "Vehicle Assembly" process.

5.2 Requirements for self-conformity assessing CYRENE ToEs

5.2.1 Requirements for CYRENE ToE I

ToE I requirements for self-conformity assessment corresponds to the assurance level "basic", which is EAL 1 level of assurance, as defined in the CC (CC-PART3, 2017). The assurance class for the evaluation will be the Class AVA: Vulnerability Assessment dealing with the first component of the class, which is AVA_VAN.1 (CC-PART3, 2017). The purpose of the vulnerability assessment activity is to identify the exploitability of flaws or weaknesses in the ToE's environment (CC-PART3, 2017). In this section, the ToE I requirements are presented according to the ToE I business environment description.

As defined in section 5.1, ToE I is the "Vehicle Transport Service" (VTS) and refers to the CYRENE business SC aspect. The Vehicle Transport Service is a complex SCS, including several

collaborating actors coming from different industries and it has been selected regarding its high impact to the EU economy (see section 5.1). According to the scenario described in section 5.1, ToE I business environment refers to the identified SC processes. These processes were decomposed to a thorough analysis identifying the business partners involved and the business roles they have in each process for the provision of the VTS. On this grounds, CYRENE ToE I concerns self-conformity assessment requirements, which are as follows:

Identifier	Description
ToE_I_CA_1	Set the boundaries of the ToE's environment (VTS as defined in section 5.1)
ToE_I_CA_2	Clarify what will be evaluated (i.e., the identified VTS processes, exploring the actors involved, their interactions, information exchange, business logic)
ToE_I_CA_3	Assign a Business Agreement between the involved SC parties with an embedded Security Declaration statement
ToE_I_CA_4	ToE I must be compliant with the content of the Business Agreement and the embedded Security Declaration statement
ToE_I_CA_5	Identify accepted certifications of the business partners involved in the ToE, related to the SC processes they execute for the provision of the VTS
ToE_I_CA_6	In case the business partners SCS processes are certified, it must be examined if the flow and the execution of these processes are compliant with the corresponding certification requirements
ToE_I_CA_7	The SCS processes must address what has been declared in ToE I business environment
ToE_I_CA_8	Clear identification and concrete analysis of the SCS processes content
ToE_I_CA_9	Business partners of the VTS participate in the identified SCS processes as defined in ToE I business environment
ToE_I_CA_10	Business roles of the participants in each VTS process must be in line with what has been described in ToE I business environment
ToE_I_CA_11	Information exchanges in the identified VTS processes must be carried out as it has been described in ToE I business environment
ToE_I_CA_12	Business partners interactions undertaken in each process must be in line with what has been described in ToE I business environment
ToE_I_CA_13	Each VTS process shall be fulfilled according to the business goal identified for this process in ToE I business environment
ToE_I_CA_14	If the organizational business policies (i.e., invoice policy), security policies, security plans and security measures are enforced, the business partners should adopt these processes (declared in the Security Declaration statement) and take care to be implemented properly

ToE_I_CA_15	ToE I environment identification must be compliant with the Common Criteria Evaluation
ToE_I_CA_16	Paperwork of the identified SC processes are in line with the description of ToE I business environment
ToE_I_CA_17	The business flow of the SC processes meets the description of ToE I business environment
ToE_I_CA_18	If privacy considerations and additional conventions described in ToE I business environment are fulfilled
ToE_I_CA_19	Identification of the security issues of each SC process of the VTS
ToE_I_CA_20	Identification of possible threat scenarios that address the defined security issue
ToE_I_CA_21	Identification of the protection profile according to the ToE I environment

Table 52 - Requirements for CYRENE ToE I.

5.2.2 Requirements for CYRENE ToE II

TOE II requirements include the technical requirements related to the ICT systems and assets involved in the VTS and are as follows:

Identifier	Description
ToE_II_CA_1	Identification of the compromised assets among all the VTS systems
ToE_II_CA_2	All the related activity in the VTS should be auditable
ToE_II_CA_3	Ensure data privacy in all the communication with external systems following the European and National legislation
ToE_II_CA_4	Ensure confidentiality of the communications through the different channels
ToE_II_CA_5	Ensure integrity of the data, so that anybody can not change anything from the message
ToE_II_CA_6	Ensure the authenticity of the involved actors avoiding identity fraud
ToE_II_CA_7	Set the boundaries of the ToE's environment (VTS as defined in section 5.1)
ToE_II_CA_8	Clarify what will be evaluated (i.e. the identified VTS processes, exploring the actors involved, their interactions, the infrastructure they utilize and the assets they operate for the provision of the VTS)
ToE_II_CA_9	Assign a Business Agreement between the involved SC parties with an embedded Security Declaration statement

ToE_II_CA_10	ToE II must be compliant with the content of the Business Agreement and the embedded Security Declaration statement
ToE_II_CA_11	Identify accepted certifications of the business partners involved in VTS-ToE II, related to the SC processes they execute for the provision of the VTS
ToE_II_CA_12	Identify accepted certifications of the business partners involved in VTS-ToE II, related to the SC assets they operate for the provision of the VTS
ToE_II_CA_13	Identify implemented security controls of the SCS assets of the business partners they operate for the provision of the VTS and they are included in the current ToE (and to the signed Security Declaration statement as a consequence)
ToE_II_CA_14	Identify accepted certifications of the business partners involved in VTS-ToE II, related to the security controls of the SCS assets they operate for the provision of the VTS
ToE_II_CA_15	Ensure that after performing the risk assessment in order to implement an optimal mitigation strategy, all business partners involved will undertake appropriate security controls (whether and wherever required) in order to reach the VTS desired security level which they have agreed upon through the Security Declaration signed commitment
ToE_II_CA_16	In case business partners VTS processes are certified, it must be examined if the flow and the execution of these processes are compliant with the relevant certification requirements
ToE_II_CA_17	The VTS processes must address what has been declared in VTS-ToE II environment
ToE_II_CA_18	Clear identification and concrete analysis of the VTS processes content
ToE_II_CA_19	Business partners of the VTS participate in the identified SCS processes as defined in ToE II business environment
ToE_II_CA_20	Business roles of the participants in each VTS process must be in line with what has been described in VTS-ToE II business environment
ToE_II_CA_21	Information exchanges in the identified VTS processes must be carried out as it has been described in VTS-ToE II business environment
ToE_II_CA_22	Business partners interactions undertaken in each process must be in line with what has been described in VTS-ToE II business environment
ToE_II_CA_23	Identify the existing asset interdependencies for the provision of the VTS (within a participated organization and between VTS interacted business partners) and check whether they are illustrated in the corresponding VTS processes according to the description of VTS-ToE II environment
ToE_II_CA_24	ICT infrastructure (or parts of the infrastructure) that operate for the provision of the VTS must be in consensus with VTS-ToE II description

ToE_II_CA_25	Each VTS process shall be fulfilled according to the business goal identified for this process in ToE II business environment
ToE_II_CA_26	If the organizational business policies (i.e., invoice policy), security policies, security plans and security measures are enforced, the business partners should adopt these processes (declared in the Security Declaration statement) and take care to be implemented properly
ToE_II_CA_27	VTS-ToE II environment identification must be compliant with the Common Criteria Evaluation
ToE_II_CA_28	Check whether the security assumptions (intended use of the implementation of the ToE) of VTS-ToE II that will be thoroughly analyzed in D2.2 are fulfilled
ToE_II_CA_29	VTS-ToE II must be assessed taking into account the key concepts of protection profiles (PP), packages of security requirements, the specified topic of conformance and the consequences of evaluation according to the CC
ToE_II_CA_30	VTS-ToE II must address the identified security issue and the described Security Target (ST) and through the implementation of the CA process examine if the described security objectives are satisfied
ToE_II_CA_31	VTS-ToE II meets the privacy considerations determined in the Security Declaration statement
ToE_II_CA_32	CYRENE CA process for the VTS-ToE II is in line with the content of Class AVA: Vulnerability Assessment dealing with the description of the first component of the class, which is AVA_VAN.1 (CC-PART3, 2017)

Table 53 - Requirements for CYRENE ToE II.

5.2.3 Requirements for CYRENE ToE III

TOE III requirements include the sectorial requirements related to the ICT systems and assets involved in the Automotive SC and are as follows:

Identifier	Description
ToE_III_CA_1	Identification of the compromised assets among all the Automotive SC systems
ToE_III_CA_2	All the related activities in the Automotive SC should be auditable
ToE_III_CA_3	Ensure the identification of the vulnerable assets
ToE_III_CA_4	Perform impact assessment on top of verified risks
ToE_III_CA_5	Ensure data privacy in all the communication with external systems following the European and National legislation
ToE_III_CA_6	Ensure confidentiality of the communications through the different channels

ToE_III_CA_7	Ensure integrity of the data, so that anybody can not change anything from the message
ToE_III_CA_8	Ensure the authenticity of the involved actors avoiding identity fraud
ToE_III_CA_9	All occurred risks should be reported
ToE_III_CA_10	Perform forecasting of possible threats/attacks
ToE_III_CA_11	Dashboards should be available to final users (i.e. for visual inspection and management)
ToE_III_CA_12	Mitigation actions should be proposed by the system
ToE_III_CA_13	Support to the end-user should be provided in the decision-making process
ToE_III_CA_14	Set the boundaries of the ToE's environment (VTS as defined in section 5.1)
ToE_III_CA_15	Clarify what will be evaluated (i.e. the identified Automotive SC processes, exploring the actors involved, their interactions, the infrastructure they utilize and the assets they operate)
ToE_III_CA_16	Assign a Business Agreement between the involved SC parties with an embedded Security Declaration statement
ToE_III_CA_17	ToE III must be compliant with the content of the Business Agreement and the embedded Security Declaration statement
ToE_III_CA_18	Identify accepted certifications of the business partners involved in ToE III, related to the SC processes they execute
ToE_III_CA_19	Identify accepted certifications of the business partners involved in ToE III, related to the SC assets they operate
ToE_III_CA_20	Identify implemented security controls of the SCS assets of the business partners they operate for the provision of the Automotive SCS and they are included in the current ToE III (and to the signed Security Declaration as a consequence)
ToE_III_CA_21	Identify accepted certifications of the business partners involved in ToE III, related to the security controls of the SCS assets they operate for the provision of the Automotive SC
ToE_III_CA_22	Ensure that after performing the risk assessment in order to implement an optimal mitigation strategy, all business partners involved will undertake appropriate security controls (whether and wherever required) in order to reach the desired security level which they have agreed upon through the Security Declaration signed commitment
ToE_III_CA_23	In case business partners Automotive SC processes are certified, it must be examined if the flow and the execution of these processes are compliant with the corresponding certification requirements

ToE_III_CA_24	The Automotive SC processes must address what has been declared in ToE III environment
ToE_III_CA_25	Clear identification and concrete analysis of the Automotive SC processes content should be performed
ToE_III_CA_26	Business partners of the Automotive SC participate in the identified SCS processes as defined in ToE III business environment
ToE_III_CA_27	Business roles of the participants in each Automotive SC process must be in line with what has been described in ToE III business environment
ToE_III_CA_28	Information exchanges in the identified Automotive SC processes must be carried out as it has been described in ToE III business environment
ToE_III_CA_29	Business partners interactions undertaken in each process must be in line with what has been described in ToE III business environment
ToE_III_CA_30	Identify the existing asset interdependencies for the provision of the Automotive SC and check whether they are illustrated in the corresponding processes according to the description of ToE III environment
ToE_III_CA_31	ICT infrastructure (or parts of the infrastructure) that operate for the provision of the Automotive SC must be in consensus with ToE III description
ToE_III_CA_32	Each Automotive SC process shall be fulfilled according to the business goal identified for this process in ToE III business environment
ToE_III_CA_33	ToE III environment identification must be compliant with the Common Criteria Evaluation

Table 54 - Requirements for CYRENE ToE III.

6. Conclusion

The CYRENE Phase 1 main results are the output of the activities of four tasks (T1, T2, T3, T4), and have been presented in this document.

This report, reporting the analysis of Supply Chain and requirements, establishes the basis in setting up the Conformity Assessment Process along with the accompanying Certification Schemes. The specifications presented in this document, will guide the design and development activities for realizing the CYRENE Conformity Assessment process.

7. References

[1] ENISA report, ICT security certification opportunities in the healthcare sector, ENISA, 2018

[2] Mentzer, John T. Supply chain management. Sage, 2001

[3] N.Kailash, R. Saha, S. Goyal (2017), “Systematic literature review of classification and categorisation of benchamarking in supply chain management”, International Journal of Process Management and Benchmarking, Vol.7, No.2, pp.183-205

[4] Ageron, B.,Lavastre, O., Spalanzani, A., (2013),"Innovative supply chain practices: the state of French companies", Supply Chain Management: An International Journal, Vol. 18 Iss 3 pp. 265 –276

[5] Jabbour, A. B., Omodei Jr.,J. C , Jabbour, C. J. , (2014),"Extending lean manufacturing in supply chains: a successful case in Brazil", Benchmarking: An International Journal, Vol. 21 Iss 6 pp. 1070 -1083

[6] Mentzer, J. T. (2001). Managing Supply Chain Collaboration. Supply Chain Management. pp. 83-84

[7] Seliger, G., B. Viehweger, and B. Wieneke. "Decision support in design and optimization of flexible automated manufacturing and assembly." *Robotics and computer-integrated manufacturing* 3.2 (1987): 221-227

[8] Mattsson, Stig-Arne. *Embracing change: management strategies in the e-economy era*. Intentia Publ., 2000

[9] Barratt, Mark, and Ruth Barratt. "Exploring internal and external supply chain linkages: Evidence from the field." *Journal of Operations Management* 29.5 (2011): 514-528

[10] N. Polemi, P. Kotzanikolaou, S. Papastergiou (2016) “Design and Validation of the ME-DUSA Supply Chain Risk Assessment Methodology and System”, Elsevier International Journal of Critical Infrastructure Protection (IJIP), 14(1), 1-39

[11] E. M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, “A novel risk assessment methodology for SCADA maritime logistics environments,” Appl. Sci., vol. 8, no. 9, 2018, doi: 10.3390/app8091477

[12] Taleb, N. N. (2018). Skin in the Game. Random House

[13] Blos, M. F., Quaddus, M., Wee, H.M., Watanabe, K. (2009). “Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil”. Supply Chain Manag. An Int. J. 14 (4), 247e252

[14] Shahbaz, M. S., RM, R. Z., Bin, M. F., & Rehman, F. (2017). “What is supply chain risk management? A review”. Advanced Science Letters, 23(9), 9233-9238

[15] Musa, S. N. (2012). “Supply chain risk management: identification, evaluation and mitigation techniques” (Doctoral dissertation, Linköping University Electronic Press)

[16] Wieland, A., & Wallenburg, C. M. (2012). “Dealing with supply chain risks”. International Journal of Physical Distribution & Logistics Management

[17] Prakash, S., Soni, G., & Rathore, A. P. S. (2017). “A critical analysis of supply chain risk management content: a structured literature review”. Journal of Advances in Management Research

[18] Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). “Supply chain risk management: a literature review”. International Journal of Production Research, 53(16), 5031-5069

[19] ENISA "Cybersecurity Certification. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS", v1.0, 1-07-2020. Online available: https://scholar.google.com/scholar?hl=el&as_sdt=0%2C5&q=ENISA+cybersecurity+certification+2019&btnG= last accessed 4-03-2021

[20] Wieland, A., & Wallenburg, C. M. (2012). “Dealing with supply chain risks”. International Journal of Physical Distribution & Logistics Management

[21] Yaakub, S., & Mustafa, H. K. (2015). “Supply chain risk management for the SME’s”. Academic Journal of Interdisciplinary Studies, 4(1–S2), 151

[22] Kalogeraki, E.-M., Apostolou, D., Polemi N., Papastergiou S. (2018). "Knowledge Management Methodology for Identifying Threats in Maritime/Logistics Supply Chains" in S. Durtst, P. Evangelista (Eds) (SI) “Logistics knowledge management: state of the art and future perspectives”, Knowledge Management Research and Practice Journal, Taylor and Francis, ISSN: 1477-8238 (Print) 1477-8246, DOI: 10.1080/14778238.2018.1486789, 16(4): 508-524

[23] Schechter, S.E. (2004). “Computer security strength & risk: A quantitative approach”. Harvard University Cambridge, Massachusetts; 2004

[24] Ralston, P.; Graham, J.; Hieb, J. (2007). "Cyber security risk assessment for SCADA and DCS networks". ISA Trans.,46, pp. 583–594

[25] Wyss, D.; Durán, F. (2001) “OBEST: The Object-Based Event Scenario Tree Methodology”; Sandia National Laboratories: Livermore, CA, USA, 2001

[26] R. R. Henning: “Security service level agreements: quantifiable security for the enterprise?”, in proceedings of the 1999 workshop on new security paradigms, ACM, pp. 54-60 (1999)

[27] Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science, 149, pp. 65-70

[28] Alberts, C.J.; Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE Approach; Addison-WesleyLongman Publishing Co., Inc.: Boston, MA, USA, 2002

[29] Clusif Methods Commission, “MEHARI V3 Risk Analysis Guide”, 2004

[30] Zambon, E., Etalle, S., Wieringa, R. J., & Hartel, P. (2011). “Model-based qualitative risk assessment for availability of IT infrastructures”. Software & Systems Modeling, 10(4), pp. 553-580

[31] Djordjevic, I.; Gan, C.; Scharf, E.; Mondragon, R.; Gran, B.A.; Kristiansen, M.; Dimitrakos, T.; Stølen, K.; “Opperud, T.A. Model Based Risk Management of Security Critical Systems”; WIT Transactions on Modelling and Simulation, Vol.31; WIT Press: Southampton, UK, 2002

[32] (CRAMM, 2005) Insight Consulting, CRAMM User Guide, Issue 5.1, United Kingdom, 2005

[33] Ntouskas, T. and Polemi, N. (2012) "STORM-RM: a collaborative and multicriteria risk management methodology", International Journalof Multicriteria Decision Making, Vol. 2, No. 2, pp.159–177

[34] Papastergiou S., Polemi D. and Karantjias A. (2015) “CYSM: An innovative physical/cyber security management system for ports”. Special Session on “Innovative Risk Management Methodologies and Tools for Critical Information Infrastructures (CII)” within the 6th International Conference on Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management (HCI International 2015), August, 2015, Los Angeles, CA, USA

[35] De Oliveira, U. R., Espindola, L. S., & Marins, F. A. S. (2018). “Analysis of supply chain risk management researches”. Gestao e Producao, 25(4), pp. 671-695

[36] Myerson Roger B., Game Theory - Analysis of Conflict, Harvard University Press, 1991

[37] T. Alpcan and T. Başar: “Network Security: A Decision and Game Theoretic Approach”, Cambridge University Press, (2010)

[38] Somasundaram Kiran K., Baras John S., "Pareto Nash Replies for Multi-Objective Games", Institute for Systems Research, University of Maryland, ISR Technical Report, 2008

[39] S. Rass: “On Game-Theoretic Network Security Provisioning”. Springer Journal of Network andSystems Management, 21, 1 (2013), 47-64

[40] Cox Louis Anthony Jr, "Game Theory and Risk Analysis", Risk Analysis, vol. 29, no. 8, pp. 1062–1068, August 2009

[41] Rajbhandari Lisa, SnekkenesEinar Arthur, "Mapping between Classical Risk Management and Game Theoretical Approaches", Communications and Multimedia Security, vol. 7025, pp. 147-154, 2011

[42] Ceryno, P. S., Scavarda, L. F., Klingebiel, K., & Yüzgülec, G. (2013). “Supply chain risk management: a content analysis approach”. International Journal of Industrial Engineering and Management, 4(3), pp. 141-150

[43] Ouyang M. (2014). “Review on modeling and simulation of interdependent critical Infrastructure systems”, Reliability Engineering and System Safety, 121, pp.43–60

[44] Kjølle, G.H., Utne, I.B., Gjerde, O., "Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies", Reliability Engineering & System Safety, vol. 105, pp. 80-89, September 2012

[45] Lee, E. E., Mitchell, J. E. and Wallace, W. A. (2007). “Restoration of services in interdependent infrastructure systems: A network flows approach,” IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 37, no. 6, pp. 1303–1317, 2007

[46] Svendsen N. K. and Wolthusen, S. D. (2007) “Connectivity models of interdependency in mixed-type critical infrastructure networks,” Information Security Technical Report, vol. 12, no. 1, pp. 44–55, 2007

[47] Kotzanikolaou, P., Theoharidou, M., Gritzalis, D., "Assessing n-order dependencies between critical infrastructures", International Journal of Critical Infrastructures, Inderscience Publishers, vol.9, no.1-2, pp.93-110, 24, Jan 2013

[48] Shin, D. H., Qian, D., & Zhang, J. (2014). Cascading effects in interdependent networks. IEEE Network, 28(4), 82-87

[49] Tang, L., Jing, K., He, J., & Stanley, H. E. (2016). Complex interdependent supply chain networks: Cascading failure and robustness. Physica A: Statistical Mechanics and its Applications, 443, 58-69

[50] Papastergiou, Spyridon, Nineta Polemi, and Panayiotis Kotzanikolaou. “Design and validation of the Medusa supply chain risk assessment methodology and system.” International Journal of Critical Infrastructures 14, no. 1 (2018): 1-39

[51] Papastergiou, S. and Polemi, D. (2017). “Securing Maritime Logistics and Supply Chain: The Medusa and MITIGATE approaches”. Marit. Interdiction Oper. J. 2017, 14, pp. 42–48

[52] ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[53] ISO/IEC DIS 15408-2, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

[54] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[55] ISO/IEC 18045:2008, Information technology — Security techniques — Methodology for IT security evaluation

[56] ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services

[57] https://www.nap.edu/read/4921/chapter/5

[58] https://ec.europa.eu/docsroom/documents/6280/attachments/1/translations/en/renditions/pdf

[59] https://www.iec.ch/conformity-assessment/types-conformity-assessment

[60] https://www.standardsportal.org/usa_en/conformity_assessment/conformity_assessment_approaches.aspx

[61] https://ieeexplore.ieee.org/abstract/document/7784925

[62] https://www.enisa.europa.eu/publications/healthcare-certification/at_download/fullReport

[63] CSA (Cybersecurity Act) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

[64] (ENISA 2020A) ENISA (2020). “ENISA Threat Landscape – 2020”, Online available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (last access in November 2020)

[65] cyberwatching.eu. (n.d.). *BUILDING STRONG CYBERSECURITY IN THE EUROPEAN UNION*. Retrieved March 01, 2021, from https://cyberwatching.eu/

[66] Densmore, R. (Ed.). (2019). *Privacy Program Management; Tools for Managing Privacy Within Organization* (Second ed.). IAPP Publication

[67] *The Directive on security of network and information systems (NIS Directive)*. (2020, December 16). An official website of the European Union. Retrieved December 18, 2020, from https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

[68] European Commission. (2020, December 16). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. An official website of the European Union. Retrieved March 01, 2021, from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[69] The European Parliament and The Council of The European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Luxembourg: Office for Official Publications of the European Communities

[70] The European Parliament and The Council of The European Union. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526*. Luxembourg: Office for Official Publications of the European Communities

[71] The European Parliament & Office for Official Publications of the European Communities. (2000). *Charter of fundamental rights of the European Union*. Luxembourg: Office for Official Publications of the European Communities

[72] Hijmans, H., & Raab, C. (2018). Ethical Dimensions of the GDPR. In *Commentary on the General Data Protection Regulation*. Edward Elgar. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3222677

[73] International Organization for Standardization. (n.d.). *ABOUT US*. Retrieved March 01, 2021, from https://www.iso.org/about-us.html

[74] International Organization for Standardization. (2009). *ISO/IEC 27000* (First edition ed.). ISO copyright office

[75] International Organization for Standardization. (2012). *ISO/IEC 17065:2012*. Retrieved March 01, 2021, from https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en

[76] International Organization for Standardization. (2019). ISO in brief. Retrieved March 01, 2021, from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf

[77] Sloot, B. (2017). Legal fundamentalism: is data protection really a fundamental right? In Data Protection and Privacy: (In)visibilities and Infrastructures (pp. 1-24). Springer. https://www.springer.com/gp/book/9783319507958

[78] Specification for security management systems for the supply chain. Online available: https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-1:v1:en

Appendix A – Glossary and Examples

The glossary is available and continuously updated in the project website[59]. It is an aggregation of terms and definitions based on different sources, such as Common Criteria and other ISO standards, NIS Directive, EU Cybersecurity Act and other Regulations, ENISA reports, EU Horizon2020 projects, NIST, CVSS, etc. It also contains examples, where necessary, to help the reader obtain a better understanding of these terms and the thin lines that may exist among them.

Another objective of the glossary is to integrate all the definitions possible and state their differences, if any, when they refer to the same term. For this purpose, there is a Notes/Remarks column, which the reader can also use for additional reading.

This glossary is divided into three main parts: the Security and Certification Concepts, the Supply Chain and Business Concepts and the Maritime Transport Concepts.

Table 55, *Table 56*, and *Table 57*, are extracts from the three different parts are presented as an example of the glossary contents included in the project website[59].

Term	Abbreviation	Definition(s)	Reference(s)	Example(s)	Notes/ Remarks
Security Concepts					
Information	**-**	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.	[CNSSI No. 4009]		
Information system		set of applications, services, information technology assets, or other information-handling components	[ISO/IEC 27000:2018]	An Enterprise Resource Planning (ERP) system	
Information Security Management System	ISMS	Set of interrelated or interacting elements of an organization to establish policies and	[ISO/IEC 27000:2018]	ISO 27001	

[59] https://www.cyrene.eu/glossary/

		objectives and processes to achieve those objectives			
Confidentiality	**-**	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes	[ISO/IEC 27000:2018]		
Integrity	**-**	Property of accuracy and completeness	[ISO/IEC 27000:2018]		
Availability	**-**	Property of being accessible and usable on demand by an authorized entity.	[ISO/IEC 27000:2018]		
Accountability	**-**	The state of being answerable (in response) for assigned actions and decisions.	[ISO/IEC 27000:2018]		
Authenticity	**-**	Property that an entity is what it claims to be.	[ISO/IEC 27000:2018]		
Reliability	**-**	Property of consistent intended behaviour and results	[ISO/IEC 27000:2018]		
Non-repudiation	**-**	Ability to prove the occurrence of a claimed event or action and its originating entities	[ISO/IEC 27000:2018]		

Table 55 - Extract from Security and Certification concept glossary.

Term	Abbreviation	Definition(s)	Reference(s)	Example(s)	Notes/ Remarks
Supply Chain and Business Concepts					
Application	**-**	IT solution, including application software,	ISO/IEC 27032:2012		

		application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function			
Application service	**-**	Software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications.	ISO/IEC 27032:2012	Online storage, Customs online service	Application service provider: operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models [ISO/IEC 27032:2012].
Application software	**-**	Software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself	ISO/IEC 26514:2008		
Asset	**-**	Something (item, thing or entity) that has value (potential or actual value) to the organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation. [ISO/IEC 27001: 2013; ISO/IEC 20000-	ISO/IEC 27001: 2013; ISO/IEC 20000-1: 2018	An asset can be for example an application server, a presence sensor, a mobile or a municipal building.	The only difference of the two terms is that the second makes provision for individuals and the separation of governments from organizations.

		1: 2018] Information asset: Anything that has value to an individual, an organization or a government. [ISO/IEC 27032: 2012]			
Business objective	-	result to be achieved. An objective can be strategic, tactical, or operational. Objectives can relate to different disciplines (e.g. financial, health and safety, and environmental goals) and can apply at different levels (e.g. strategic, organization-wide, project, product and process. An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).	ISO/IEC 27000: 2018		
Cosignee / Shipper / Cosignor	-	A person or company that consigns or receives goods for transportation.	EU H2020-DS-2014-01 project "MITIGATE"		
Critical Infrastructure	CI	An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or	Council Directive 2008/114/EC	SCADA, port, Port Community System (PCS)	European critical infrastructure (ECI) is a critical infrastructure located in Member States the disruption or destruction of

		social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions			which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure [Council Directive 2008/114/EC].
Critical Information Infrastructure	CII	ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)	Council Directive 2008/114/EC	Human Machine Interface (HMI)	
Critical services	**-**	A critical service is a service that is essential for the maintenance of critical societal or economic activities.	NIS Directive, 2016		
Customer		Person or organization that could or does receive a product or a service that is intended for or required by this person or organization	ISO 9000:2015	Consumer, client, end-user, retailer, receiver of product or service from an internal process, beneficiary	

				and purchaser.	

Table 56 - Extract from Supply Chain and Business concept glossary.

Term	Abbreviation	Definition(s)	Reference(s)	Example(s)	Notes/Remarks
Maritime Transport Concepts					
Baltic and International Maritime Council	BIMCO	BIMCO is one of the greatest international shipping associations representing ship owners. It undertakes the control of around 65 percent of the world's tonnage and it has a strong membership, engaging more than 120 countries, involving managers, brokers and agents. BIMCO's main objective is to protect its global membership via the provision of information and consulting that forwards fair business practices and invests on the harmonisation and standardization of commercial shipping practices and contracts.	Baltic and International Maritime Council, Den Store Danske Encyklopædi. Denstoredanske.dk. Online available: https://denstoredanske.lex.dk/Baltic_and_International_Maritime_Council?utm_source=denstoredanske.dk&utm_medium=redirect&utm_campaign=DSDredirect		https://www.bimco.org/
Barge operator	-	A company that provides barge capacity and barge transport.	EU H2020-DS-2014-01 project "MITIGATE"		
Berth Management Systems	-	Those systems are used by Port Authorities to manage and ensure safety in	"Port Cybersecurity - Good practices for		

		mooring processes: warnings and alerts, meteorological data, video cameras streams, berth allocation management, etc.	cybersecurity in the maritime sector", ENISA, 2019		
Border Control	-	The border control authorities are responsible of taking measures to monitor the state borders and to regulate the movement of people, animals and goods. In the EU, with Schengen agreement, the crews and passengers are controlled only once when they come from a non-EU country.	"Port Cybersecurity - Good practices for cybersecurity in the maritime sector", ENISA, 2019		
Bunkering	-	The provision of solid, liquid or gaseous fuel or of any other energy source used for the propulsion of the waterborne vessel as well as for general and specific energy provision on board of the waterborne vessel whilst at berth.	Regulation (EU) 2017/352, Article 2		
Cargo	-	Items that are placed on the ship to be transported to another port, such as boxes, pallets, cargo transport units, and bulk liquid and non-liquid matter.	ISO 20858:2007		
Cargo Community System	CCS	Usually owned and managed by port stakeholders that are	"Port Cybersecurity - Good		

		usually private companies in charge of the terminal port operations. This system is used to share information on port operations related to the cargo and containers between all involved stakeholders (content of the cargo, localisation of a container, hour of its transfer, customs declarations, etc.)	practices for cybersecurity in the maritime sector", ENISA, 2019		
Cargo handling	-	The organisation and handling of cargo between the carrying waterborne vessel and the shore, whether it be for import, export or transit of the cargo, including the processing, lashing, unlashing, stowing, transporting and temporary storage of the cargo on the relevant cargo-handling terminal and directly related to the transporting of the cargo, but excluding, unless the Member State determines otherwise, warehousing, stripping, repackaging or any other value added services related to the cargo.	Regulation (EU) 2017/352, Article 2		
Carrier	-	Freight transporting company	EU H2020-DS-2014-01		

			project "MITIGATE"		
Centre for International Maritime Security	CIMSEC	A 501(c)3 non-partisan think tank incorporated as a non-profit in the state of Maryland. CIMSEC was formed in 2012 and as of 2020 has 20 international chapters and over 2,000 members and subscribers in 60 countries. CIMSEC does not take organizational positions and encourages a diversity of views in the belief that a broad range of perspectives strengthens our understanding of the challenges and opportunities in the maritime domain.	http://cimsec.org/about		

Table 57 - Extract from Maritime Transport concept glossary.

Appendix B – Validation of CYRENE ToEs

This Appendix presents the three CYRENE Advisory Boards that have been formed in the first six months of the project's lifetime. It also presents the organization of the first project workshop, in which members of the Advisory Boards participated, and the feedback received by them.

B.1 CYRENE Advisory Boards

CYRENE has defined three Advisory Boards, which are expected to provide their expert advice on key topics the project addresses, related to the certification of security aspects of supply chains. The role and expectations of the three boards are as follows:

User Advisory Board (UAB): it will support the project with its requirements collection and evaluation tasks, including

(i) providing sound and concrete advice on requirements related to security aspects of modern supply chains, as well as the design of tools, scenarios and user stories that will be developed in the context of the project,
(ii) participating in the evaluation phases of the developed tools and prototypes, and
(iii) acting as channels and multipliers for the exploitation and market uptake of the project's results.

External Advisory Board (EAB): it will support the project with its requirements and dissemination objectives, including:

(i) Ensuring that the project's outcomes address not only the requirements of the specific domains via the project's pilots, namely the domain of automotive industry and the one of vehicle transportation, but from other industrial sectors as well.
(ii) Bringing in touch the project with potential users (citizens, local authorities, ministries) of the solutions to be developed, other similar projects and research initiatives, as well as policy makers and standardization bodies.
(iii) Advising on the compliance of project's results with legal, ethics, standardization and certification regulations and relevant legislation.

Ethical Advisory Board (EthAB): it will support the project for implementing its ethical management strategy including:

(i) adherence to privacy laws and regulations,
(ii) handling of anonymization processes,
(iii) handling of informed consent processes for participants of the pilot operations,
(iv) processes associated with secure storage of incident handling datasets.

The three Advisory Boards were formed in the first six months of the project's lifetime.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952690.

B.2 First Project Workshop

CYRENE organized its first (web) workshop on March 31, 2021. The objective of the workshop was the elicitation of feedback from the three Advisory Boards on requirements relating to the certification of security aspects of supply chains that had been collected by the project in the first six months. The workshop agenda is shown in *Table 58*.

Time (CET)	Topic	Speaker
10:00-10:05	Welcome	PN
10:05-10:20	CYRENE Overview	MAG UBI
10:20-10:30	Security Aspects of Supply Chains	SU
10:30-10:50	Supply Chains (SC) as Targets of Evaluation (ToE), CYRENE ToEs	FP MAG
10:50-11:10	End user requirements	UNSPMF
11:10-11:40	CYRENE Questionnaire Feedback, discussion, Q/A by AB members (collection of end user requirements)	UNSPMF
11:40-11:45	Conclusions and closing remarks	PN

Table 58 - Workshop agenda.

The workshop agenda, a copy of the presentations, and a tailored version of D2.1 were communicated to the Advisory Board members before the workshop. During the workshop the presentations that were given by the project focused on:

1. The objectives of the project and its technical approach.
2. The State of the Art on security aspects of supply chains and related risks.
3. The European cybersecurity certification initiatives and approaches to certification of supply chains.
4. The compiled by the project Supply Chain requirements, expressed as Targets of Evaluation.
5. Details of business process, assets and infrastructure, and sector specific requirements.

Following the project presentations, a Q&A session took place for facilitating interactions with the Advisory Boards and receiving their feedback and comments on the presented Supply Chain security certification requirements. The Q&A session started by summarizing the outcome of the project, which is a methodology and a set of tools for the Conformity Assessment of security aspects of Supply Chains.

The main issues raised by Advisory Board members, are summarized in *Table 59*, along with the approach the project takes to address them.

Suggestion	CYRENE approach
IoT devices be included as SC assets	CYRENE plans to address IoT as assets of supply chains
Cyber-physical systems be addressed by the project	CYRENE plans to address cybersecurity aspects of CPS
Security aspects of cloud-based services supporting supply chains to be considered	CYRENE will consider developments in the security of cloud-based services. The supply chain certification scheme to be designed and proposed by CYRENE is based on a similar scheme on cloud services certification proposed by ENISA
Enlarge the base of supply chains addressed and include Hydrogen-LNG SC	CYRENE takes a general approach to security certification of SCs but it will focus it pilots on the two supply chain scenarios that have been prescribed.
Consider certification of software products	CYRENE addresses SCs and infrastructures that support them, but not certification of software products per se, which falls into the realm of other certification initiatives

Table 59 - Suggestions from the Advisory Boards.

Further input was sought by Advisory Board members who were asked to provide offline their feedback to a questionnaire that had been prepared and setup by the project at https://ec.europa.eu/eusurvey/runner/cyrene-questionnaire. The replies to the questionnaire received were analyzed, and the results are presented in Chapter 4.

The workshop completed with a slight delay with respect to its original schedule.