



Horizon 2020 Program

ICT-02-2020

Building blocks for resilience in evolving ICT systems



Certifying the Security and Resilience of Supply Chain Services

D3.1: Conformity Evaluation Process & Multi Level Evidence Driven Supply Chain Risk Assessment

CYRENE Report 3

Abstract: In this report the CYRENE dual-use methodology is presented and can be used: by the SCS provider & business partners to estimate their risks, undertake controls, develop the SCS-ISMS and the SCS- protection profile (PP); and as a conformity evaluation process that can be used by an accessor to assess the claims of the SCS-PP using the guidelines of the proposed CYRENE SCS-scheme. The methodology will implement the principles of ISO/IEC27001, ISO/IEC27005, ISO28000 and ISO/IEC15408.

Table of Contents

List of Tables	5
List of Figures	7
List of Acronyms	9
Executive Summary	12
1 Introduction	13
1.1 Scope	13
1.2 Relation with other work packages and tasks	14
1.3 Document Structure	15
2 CYRENE enhanced Risk and Conformity Assessment (RCA) Methodology: Overview	16
2.1 Scope & Objectives	16
2.2 Relationship with international Standards & other Methodologies	18
2.2.1 Relation to ISO/IEC 27000-series	18
2.2.2 Relation to ISO 28000-series	19
2.2.3 Relation to ISO/IEC 15408	19
2.2.4 Relation to ISO/IEC 18045	20
2.2.5 Relation to ETSI-TVRA	20
2.2.6 Relation to MITIGATE	20
2.2.7 Relation to vulnerability severity of CVSS	21
2.3 Extended Security Model	31
2.4 Assurance of SCS	34
2.4.1 Identification of Attack Potential in CYRENE	34
2.4.1.1 Attack Potential according to ISO/IEC 15408 and ETSI-TVRA	34
2.4.1.2 Attacker's Potential in relation to adversary's characteristics	35
2.4.2 CYRENE SCS vulnerability evaluation scale in relation to the Attack Potential	38
2.4.3 CYRENE Levels of Attacker's Profile	40
2.4.4 CYRENE SCS assurance scale	41
3 CYRENE RCA Methodology Design Criteria	42
3.1 Notifications and Assumptions	43
3.1.1 Enhanced Risk and Conformity assessment ontology requirements	44
3.1.2 Requirements for Adopted Security Standards	45
3.1.3 Building Blocks of the CYRENE RCA Methodology	46

3.2	CYRENE ontology for enhanced Risk and Conformity Assessment	47
3.2.1	Related works	47
3.2.2	OntoCyrene	48
3.2.2.1	Architecture of OntoCyrene	49
3.2.2.2	OntoCyrene Class Hierarchy	49
3.2.2.3	OntoCyrene Object and Data Properties (Relationships)	53
3.2.3	Ontology Population and Validation	56
3.2.3.1	Description of “Port Call Request” Process	57
3.2.3.2	Ontology Population: Sector Perspective	57
3.2.3.3	Ontology Population: Business perspective	59
3.2.3.4	Ontology Population: Asset perspective	62
3.2.3.5	Ontology Population: Connecting three perspectives.	63
3.2.3.6	Validating the OntoCyrene	64
3.3	Use of the Methodology	66
3.3.1	SCS Business Partners	66
3.3.2	ICT / Security Experts	67
3.3.3	Sector Specific Parties	67
3.3.4	SCS Assessors	67
4	Supply Chain Service (SCS) as Target of Evaluation (TOE)	68
4.1	SCS at a glance	68
4.2	SCS Scheme Elements	69
4.3	SCS Security Declaration and Application Statement (SDA)	70
5	CYRENE RCA Methodology	71
5.1	Overview Model of the CYRENE RCA Methodology	71
5.2	CYRENE enhancements	73
5.3	Step Analysis of the CYRENE CA Methodology	74
	Step 0: Scope of the SCS RCA	74
	Step 1: Analysis of the SCS	76
	Step 1.1: Scope, objectives, and requirements of the SCS	76
	Step 1.2: SCS Business Partners	80
	Step 1.3: SCS Modelling	80
	Step 1.3.1: Identification and description of SCS business processes.	81

Step 1.3.2: Identification and description of SCS business partners	81
Step 1.3.3 SCS-TOE's infrastructure description (if applicable)	81
Step 1.3.4 Business process model generation	81
Step 1.3.5 Identification of SCS components criticality and asset model generation	81
Step 2: SCS Threat Analysis	93
Step 2.1: Identification of Threat Scenarios/Threats	93
Step 2.2: SCS Threat Assessment	94
Step 3: Vulnerability and Impact Analysis	97
Step 3.1 Estimation of Attack Potential	98
Step 3.2: Vulnerability Severity Estimation	98
Step 3.3. Evidence-Based Vulnerability Analysis (VA)	99
Step 3.4: Identification of Confirmed & Zero-Day Vulnerabilities	100
Step 3.5: Building all Vulnerability Chains within the SCS	101
Step 3.6 Identification of Attack Methods & Attack Graphs	103
Step 3.7 Attack Impact	104
Step 3.8 Systematic Documentation of Vulnerabilities	105
Step 3.9 Occurrence Likelihood & Impact Assessment	105
Step 4: Risk Assessment- Establishment of Risk	107
Step 5: Risk Compliance to Security Assurance Certification Scheme	109
Step 6: Risk Mitigation: Security Countermeasure Identification	112
Step 6.1: Countermeasures in the SCS	112
6 Conclusions	117
7 References	118
8 Glossary & Examples	121
8.1 Supply chain and business concepts	122
8.2 Security and certification concepts	127
9 Appendices	140
Appendix A: Security Declaration & statement of Application (SDA) –template	140
Appendix B: Protection Profile for an SCS-template	146
Appendix C: SCS inventory -template	151
Appendix D: SCS Criticality -templates for SCS Business Partners	152
I. SCS process criticality – template	152

II. SCS Business Partners importance to the SCS process – template	153
Appendix E: An introduction to BPMN and ontology	154
Main standards and frameworks	154
I. Business Process Model and Notation (BPMN)	154
II. Ontology	156
Appendix F: Vulnerability Documentation- template	158
Appendix G: Scoring and Measurements	160
I. Assurance Components – Attack Potential Scale	160
II. Individual IA, Scale	161
III. Conformity Assessment Quantitative and Qualitative Scales	161
IV. SCS Criticality Scales	162
V. Assurance Levels	163
Appendix H: Cybersecurity Mitigation Strategies	165

List of Tables

Table 1 – CYRENE CA methodology considerations for the vulnerability severity measurement on SCS environments towards the Environmental Metric Group of CVSS 3.1.....	25
Table 2 – Description of the attacker’s capability.....	35
Table 3 – Attacker’s multi-dimensional profile [9].	36
Table 4 – Proposed quantification of attacker’s profile [10].	37
Table 5 – CYRENE vulnerability analysis evaluation scale in relation to the Attack Potential (AP).	39
Table 6 –Relation between Assurance elements.....	41
Table 7 – Identification of the CYRENE SCS assurance scale.....	42
Table 8 – List of OWL axioms from natural language specifications.....	52
Table 9 – Object properties defined and modelled for asset driven perspective.	54
Table 10 - Object properties defined and modeled for the business-driven perspective.	54
Table 11 – Object properties defined and modeled for the sector-driven perspective.....	55
Table 12 –Object properties defined and modelled for security related concepts.	55
Table 13 – Object properties used to implement departments of the SCS-P.	58
Table 14 – Object properties used to implement partners of the SCS-P.....	58
Table 15 – Object properties used to implement activity instance.	61
Table 16 – Object properties used to implement connecting objects.....	62
Table 17 – List of asset-driven instances and relationships implemented for P1n the example.	63
Table 18 – Implementing connecting points for three perspectives in the example.	64
Table 19 – The CYRENE RCA methodology.	72

Table 20 – Step analysis structure of the CYRENE RCA methodology.	74
Table 21 – Step 0 example.	75
Table 22 – Step 1.1 example.	79
Table 23 – Step 1.2 example.	80
Table 24 – SCS asset cyber dependencies identification.	84
Table 25 – Example for identification of SCS process criticality.	86
Table 26 – Example of identification of SCS business partners' importance to the "Entry Summary Declaration" process.	87
Table 27 – Example of asset criticality 'Rule 3' for 'SCS asset 8'.	90
Table 28 - Example of asset criticality 'Rule 5' for SCS asset model complexity.	92
Table 29 – Step 2.1 example	94
Table 30 – MITIGATE Threat scale.....	96
Table 31 – Step 2.2 Example.....	96
Table 32 – Step 3.1 example.	98
Table 33 - Example of vulnerability chaining.....	101
Table 34 – SCS Asset interdependencies example.....	102
Table 35 – CYRENE Security Assurance Certification Scheme measures.....	111
Table 36 – CYRENE Supply Chain countermeasures.	116
Table 37 – Extracted from Supply Chain and Business Concepts CYRENE online glossary...	126
Table 38 – Certification and Security Concepts of the updated CYRENE online glossary.	139
Table 39 – SCS assets inventory (ISMS) template.....	151
Table 40 –SCS process criticality template.	152
Table 41 –SCS Business Partners (SCS-BPs) assessment to the execution of the SCS process (template).....	153
Table 42 – Quantitative and qualitative values of AP according to ISO/IEC 15408.....	160
Table 43 – Estimation of the overall Resulting impact.	161
Table 44 – CYRENE probability scale.....	161
Table 45 – Mapping SCS-P to the industry sectors of essential and important services of NIS 2 Directive [13].	162
Table 46 – SCS criticality qualitative scale of the CYRENE enhanced Risk and Conformity Assessment (RCA) methodology.	163

List of Figures

Figure 1 – CYRENE Dynamic Conformity Assessment Process: A layered-based presentation.	14
Figure 2 – CYRENE’s Circles of Consideration.	15
Figure 3 – CVSS 3.1 base, temporal, and environmental metric groups.....	21
Figure 4 – Extended Information Security Model that connects Risk and Conformity Assessment.	32
Figure 5 – The Protection Profile (PP) as presented in the Common Criteria (CC), 2017 [7].	33
Figure 6 – ENISA AHWG on Risk Assessment, 2020 (Coordinator: Cord Bartels) [8].	33
Figure 7 –Requirements for developing the CYRENE ontology model.	45
Figure 8 – Main sub ontologies in OntoCyrene.....	49
Figure 9 – OntoCyrene superclasses in class hierarchy.....	49
Figure 10 – Subclasses designed for modeling Business-driven perspective.....	50
Figure 11 –Roles modeled in OntoCyrene	52
Figure 12 – Sector-driven perspective modeled in the Ontology.	52
Figure 13 – Security aspects of OntoCyrene in terms of super/sub classes.	53
Figure 14 – OntoCyrene data properties.	55
Figure 15 – Connecting points of the three perspectives.....	56
Figure 16 – Instances for partners of the SCSP in the example.	58
Figure 17 – Sector view instantiation.....	59
Figure 18 – BPMN diagram of “Port Call Request” process.....	59
Figure 19 – Encoded BPMN diagram of “Port Call Request” process.....	60
Figure 20 – All relationships for A6 in the ontology.....	64
Figure 21 – All relationships for Ship_Owner in the ontology.....	65
Figure 22 – All relationships for HP_DL850 in the ontology.....	65
Figure 23 – Example of SCS assets operating within an SCS process among different SCS business partners.....	83
Figure 24 – Example of SCS assets operating within different SCS process among different SCS business partners.....	83
Figure 25 – Example of asset interdependencies of SCS assets operations within a specific SCS Business partner of an SCS process, between different SCS Business partners of an SCS process, and between different SCS Business partners participating in different SCS processes.	83
Figure 26 – SCS assets inherit SCS process criticality to which they belong (Rule 1).	88
Figure 27 – SCS asset 8 that operates in SCS process A and SCS process B inherits the worst- case scenario of SCS criticality, which “Medium” level of criticality of SCS Process A.	89
Figure 28 – SCS asset criticality depends on the frequency of its appearance in the overall number of the SCS processes.	90
Figure 29 –Asset vulnerabilities combinations graph.....	102
Figure 30 – CYRENE Protection Profile according to Common Criteria.	146
Figure 31 – BPMN 2.0 main elements.....	155
Figure 32 – Proposed stack for Semantic Web by W3C.....	156

Figure 33 – CVRF 1.1 Attributes.158
Figure 34 – CISCO XML vulnerabilities indicative report.159

List of Acronyms

Acronym	Description
AL	Assurance Level
AP	Attack Potential
ACSC	Australian Cyber Security Centre
BP	Business Partner
BPMN	Business Process Model and Notation
CA	Conformity Assessment
CAB	Conformity Assessment Body
CC	Common Criteria
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
CII	Critical Information Infrastructure
CVL	Cumulative Vulnerability Level
EDR	Endpoint Detection and Response
EAL	Evaluation Assurance Level
EUCSA	European Cyber Security Act
EUCC	European Cybersecurity Certification scheme
EUSCS	European Cybersecurity Certification Scheme for Supply Chain Services
NIS Directive	Network and Information Security Directive
GDPR	General Data Protection Regulation
ICVL	Individual Chain Vulnerability Level
IPVL	Individual Propagated Vulnerability Level
ICT	Information and Communications Technology

ISMS	Information Security Management System
EUSCS	European Union Supply Chain Service Certification Scheme
MRA	Mutual Recognition Agreement
NCA	National Certification Authority-
OES	Operator of Essential Service
OS	Operating System
OIS	Operator of Important Service
PCA	Principal Component Analysis
PDCA	Plan-Do-Check-Act
PAM	Privileged Access Management
PVL	Propagated Vulnerability Level
PP	Protection Profile
RA	Risk Assessment
RCA	enhanced Risk and Conformity Assessment
SAR	Security Assurance Requirements
SDA	Security Declaration and Application Statement
SFR	Security Functional Requirements
ST	Security Target
SLA	Service Level Agreement
SIEM	Security Information and Event Management
SCSMS	Supply Chain Security Management System
SCS	Supply Chain Service
SCS-BP	Supply Chain Service Business Partner
SCS-PP	Supply Chain Service Protection Profile
SCS-P	Supply Chain Service Provider
SCS-RA	Supply Chain Service Risk Assessment

SCS-TOE	Supply Chain Service as Target of Evaluation
TVRA	Threat Vulnerability Risk Analysis
TOE	Target of Evaluation
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
VA	Vulnerability Analysis
VTS	Vehicle Transport Service
VSL	Vulnerability Severity Level

Executive Summary

This report presents the proposal of an enhanced Risk and Conformity Assessment (RCA) methodology that combines all the relative standards, policy and legal requirements mentioned in CYRENE Report 2. This RCA methodology is an enhanced method of dual use, as it should be able to be used by:

SCS Providers and Business Partners to help them get prepared for a certification, and assessors in order to demonstrate the validity of the claims, for example, in a Protection Profile.

In this document every step of the CYRENE RCA methodology is analysed in a form of scope, input and expected outcome, followed by an example for better comprehension of the reader. In addition, eight appendices are included in the current document.

1 Introduction

1.1 Scope

The main objectives of this report were to:

- i. design and develop the strategy of realizing CYRENE's conformity assessment process, and
- ii. specify the CYRENE multi-level evidence-driven Supply Chain risk assessment process as well as delineate its implementation activities to be undertaken within the project.

During its first task, the activities were focused on the production of models for representing SCS assets, along with the dependencies among them. Furthermore, the models were connected to collections/hierarchies of events.

CYRENE has produced and specified algorithms for the qualitative as well as the quantitative analysis of the cascading effects of security threats, risks, and propagated vulnerabilities. Several tools and techniques were utilized, such as:

- production of scoring models that will consider the utility/value of the various SCs assets in order to quantify and assess the potential damages that are associated with the various risks;
- multi-layer graph modeling,
- spectral graph theoretic methods for quantification of vulnerabilities, and
- dynamic network modeling, in order to account for the dynamic nature of the system, due to, e.g., the mobile assets.

Moreover, this report focuses on the identification of measures that could alleviate/reduce the cascading effects of security events in SCS. These measures will be connected to the outcomes of the multi-layer algorithms for detecting multi-layer dependencies and the impact of relevant risks. In particular, the measures will be activated in response to the detection of the dependencies of the SCS in the scope of specific risks and security events. As part of this task, the project also integrated algorithms, quantitative as well as qualitative analysis techniques, and measures in an integrated risk management/conformity assessment. The output is directed to the relevant assessment authorities and services, including self-assessment, third-party assessment, and self-attestation.

Finally, the fourth task's activities, which were also running in parallel with the previous three tasks of this report, provided detailed specifications of the CYRENE Conformity Evaluation Process and the collaborative evidence-based SCS risk assessment approach. These took into consideration the stakeholders involved in the collaborative process, the role and authorizations of each Business Partner, as well as the collaboration workflows associated with the assessment and simulation processes. A detailed analysis was carried out to device evidence and metrics which were classified with respect to the three CYRENE relevant aspects of the supply chain:

- business,
- infrastructure, and
- individual IoT device level.

1.2 Relation with other work packages and tasks

This report is aligned with all the literature reviewed in CYRENE Report 1 so that the CYRENE RCA Methodology is compliant with all the relevant standards, policy, and legal requirements. In addition, it follows and compliments the proposed CYRENE Cybersecurity Certification Scheme for Supply Chain Services (EUSCS), developed in CYRENE Report 2, which was based upon the European Cybersecurity Certification Scheme (EUCC) as well as the EU cybersecurity certification scheme for Cloud Services (EUCS).

More specifically, the produced models were used to design, test, and simulate the various multi-layer algorithms. This work reported in this document took as input results on modeling, classification, and contextual definition of the SCS. The modeling carried out was used for the actual construction of the horizontal layers 1-3 (see Figure 1), which were described in CYRENE Report 1.

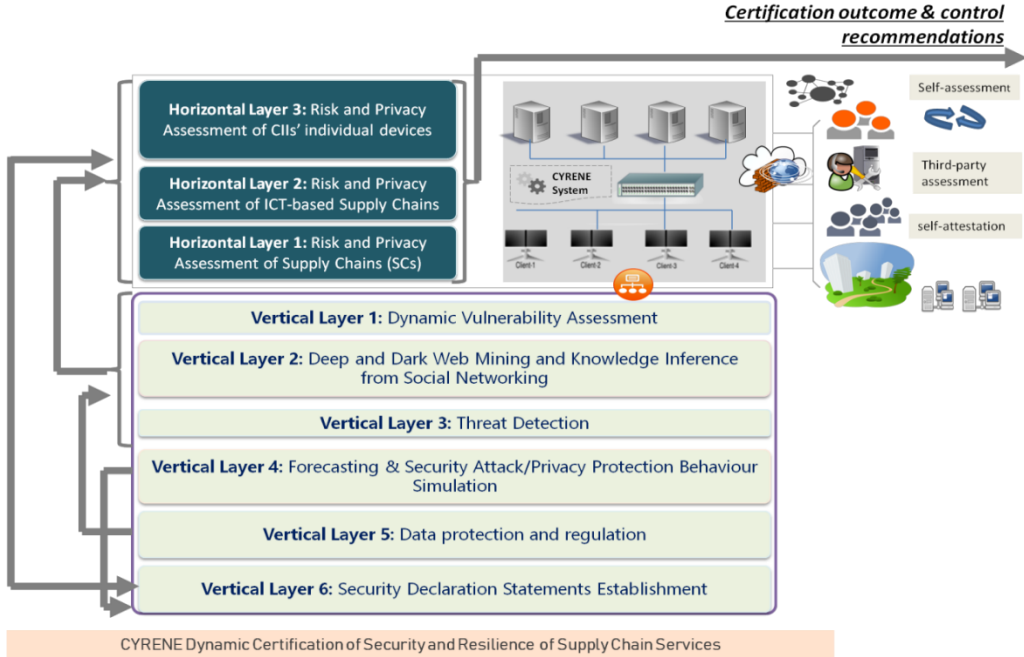


Figure 1 – CYRENE Dynamic Conformity Assessment Process: A layered-based presentation.

In addition, the multi-layer modeling reported in this document was mapped to the CYRENE's four circles of consideration (see Figure 2).

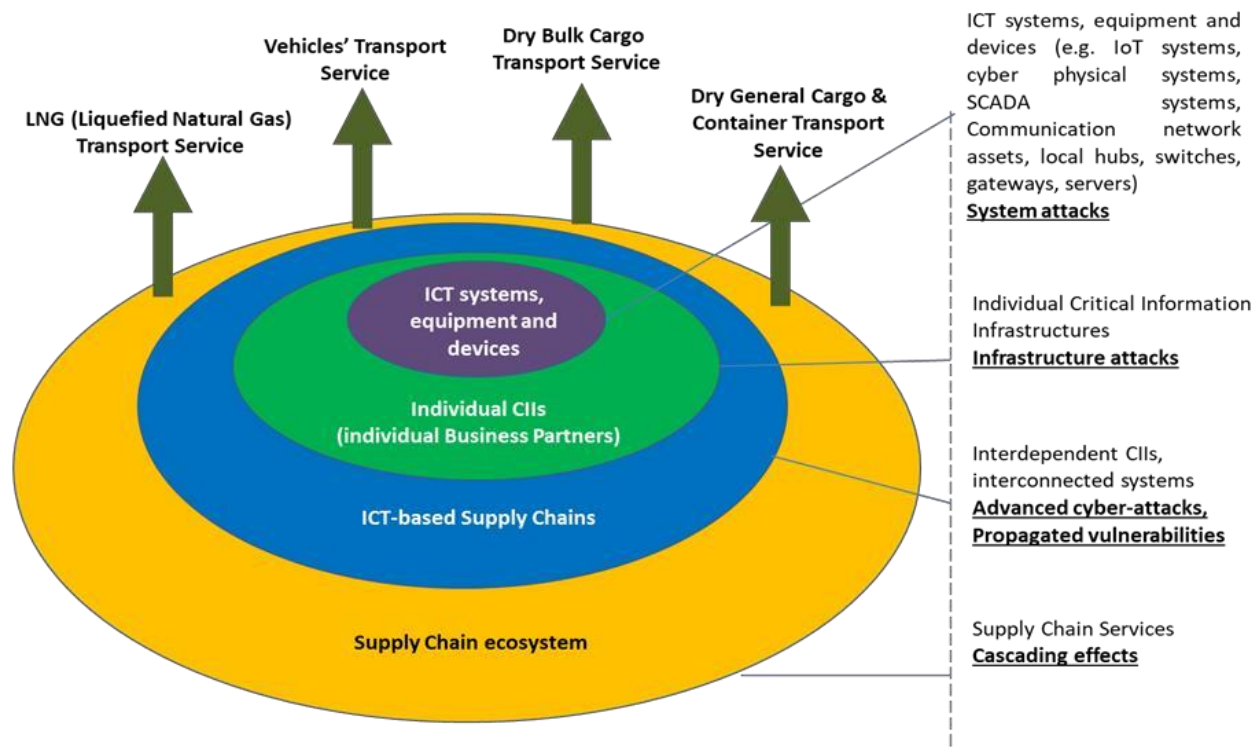


Figure 2 – CYRENE's Circles of Consideration.

1.3 Document Structure

The rest of this document is structured as follows:

- Chapter 2 provides an overview of the CYRENE Enhanced Risk and Conformity Assessment (RCA) Methodology;
- Chapter 3 presents the Design Criteria of the CYRENE RCA Methodology;
- Chapter 4 explains how the SCS can be viewed as a TOE, be subject to the CYRENE RCA methodology, and decomposed into its generic elements;
- Chapter 5 analyzes step by step the CYRENE RCA Methodology, in a form of scope, input, and outcome, followed by an example for better comprehension of the reader;
- Chapter 6 depicts the conclusions of the work that has previously been analyzed;
- Chapter 7 mentions the references used for all this content;
- Chapter 8 aggregates the additional glossary used in CYRENE Reports 1 and 2, which enriched the online ongoing work¹;
- Chapter 9 includes eight appendices to back up the report, help the reader better understand its content as well as provide them with useful ready-to-use templates.

¹ <https://www.cyrene.eu/glossary/>

2 CYRENE enhanced Risk and Conformity Assessment (RCA) Methodology: Overview

The current section introduces the CYRENE enhanced Risk and Conformity Assessment (RCA) methodology. It poses the main scope and the objectives of the methodology and describes its relationship with international standards and other corresponding methodologies. In addition, it addresses the interrelations between the risk assessment and conformity assessment and delineates an extended security model to demonstrate the dual use of the CYRENE RCA methodology. Eventually, it analyses the main concepts of SCS assurance that establish the CYRENE RCA methodology.

2.1 Scope & Objectives

According to EC 765/2008 regulation [1], Conformity Assessment (CA) is the process that demonstrates whether specified requirements relating to a product, process, service, system, person, or body have been fulfilled².

The CYRENE enhanced Risk and Conformity Assessment (RCA) methodology is an enhanced risk assessment methodology that aims to be used by the SCS-providers/partners to assess and manage their cyber risks, implement effective controls (considering attackers' profile, assurance level of the SCS, use of the various SCS-assets in the SCS-processes) and develop the Protection Profile (PP) of the SCS. The CYRENE RCA methodology can be used to develop a collaborative Information Security Management System (ISMS), appropriate for the SCS (SCS-ISMS), managed by the SCS Provider (SCS-P), where all SCS Business Partners (SCS-BPs) can collaborate.

CYRENE RCA facilitates the preparation of the SCS to be certified, i.e., prepare the PP to be submitted for conformity assessment and issuance of an SCS certificate.

On the other hand, the CYRENE RCA methodology can be used by the assessor to assess the claims of the SCS-PP; in particular, it can be used by a self-assessor (in case the SCS assurance level is "Basic" and self-assessment is feasible), or a Conformity Assessment Body (CAB) (in case the assurance level is "substantial" or "high"). The assessors will also use the guidelines as provided in the proposed European Cybersecurity Certification Scheme for Supply Chain Services (EUSCS), presented in CYRENE Report 2 [2] to prepare their audit report and issue an SCS cybersecurity certificate in case they are an authorized body e.g. CAB authorized by a National Certification Authority (NCA). Thus, it is the evaluation methodology that supplements the proposed EUSCS to check whether the PP claims are valid and if the SCS can be subject to security certification.

² <https://www.cyrene.eu/glossary/>

It is considered an integral part of the EUSCS to demonstrate its security objectives in line with Article 51 of the EU Cybersecurity Act (EUCSA) [3]. Thereby, the CYRENE RCA methodology paves the way to guarantee the business and technical competence of the SCS.

Assessing the risks of SCS can expand the business partners' security awareness on the under examination SCS and give them insights into what measures should be undertaken and where in order to improve its level of security. In this regard, managing the SCS risks, preparing the PP, and having an assessor conduct conformity assessment and issue a certificate of SCS aims to enhance the security, privacy, resilience, accountability, and trustworthiness of SCS and thus to increase their level of competence in the internal market and as a consequence to strengthen the EU economy.

The main objectives of the CYRENE RCA methodology are the following:

- cover the main activities from context definition, over risk identification and analysis up to mitigation actions (i.e. identification and measurement of all relevant cyber threats, prediction of potential attacks/threats paths and patterns, estimation of the existence of zero-day exploitable vulnerabilities, evaluation of the SCS-vulnerabilities considering their propagation, assessment of the potential impacts and estimation and prioritization of the corresponding SCS-risks) to produce a risk assessment report and risk treatment plan;
- the developed risk assessment report and risk treatment plan will guide the SCS-P to manage their cybersecurity risks and implement effective countermeasures under an SCS Security Declaration and Application statement (SCS SDA) in collaboration with the Business Partners (SCS-BP) involved in the SCS. The SCS-BP will also prepare documentation for all assets they host and all controls implemented covering info like tests, outcomes conducted;
- the outcomes of the above activities will be stored, and updated in the SCS-ISMS by the SCS-P in collaboration with the SCS-BPs;
- guide the assessor to evaluate the conformity of SCS towards a given security certification schema which applies to ICT SCS (i.e., the CYRENE EUSCS) in case an SCS-P provider seeks assessment under an SCS MRA;
- provide an evaluation mechanism that SCS partners can use to define the protection profile (PP) of the SCS, and assessors can use to examine whether the security requirements of a security certification schema related to SCS (i.e. CYRENE EUSCS) are met and if the specificities that have been followed to describe the SCS as Target of Evaluation (SCS-TOE), i.e security-relevant sites explicitly required by a PP, apply to the adopted security certification schema;
- develop cybersecurity and privacy evaluation process that can support different types of evaluations, including (i) Self-assessment (when assurance level “basic” can be adopted according to the EUCSA) allowing the SCS-P and SCS-BPs to self-assess the security of the SCS, according to the relevant certification scheme, (ii) third-party assessment (when assurance level “substantial” or “high” is feasible according to the EUCSA), where an independent party (CAB) performs the assessment;
- apply to different SCS perspectives: overall business view, holistic-technical view, sector-specific technical view;
- evaluate the security and resilience of SCS, the interconnected processes, ICT infrastructures composing these services, and the individual devices and assets that support the provision of the SCS;

- facilitate the SCS-provider/partners (in particular their security officers and SCS-operators) to recognize, model, dynamically analyze and estimate risks and their cascading effects, taking into account the associated weaknesses, threats, and threat agents along with the potential and likelihood of attack and the optimal mitigation actions and countermeasures to establish a rigorous security profile for SCS in a collaborative manner;
- enable the creation of collaborative ISMS in terms of developing an SCS inventory engaging all main generic SCS components (i.e. processes, business partners, assets) along with its security information (i.e. security controls, vulnerabilities, threats, etc.), hosting all risk management services;
- bring together practices from different research fields, such as conformity assessment and certification schemas for the SCS certification and audit, forecasting, attack simulation, and risk propagation for the estimation of the SCS security and maintenance;
- comply with standards relevant to SCS security and IT evaluation (i.e., ISO 28000, ISO/IEC 27001, ISO/IEC 15048, and ISO/IEC 18045 standards);
- contribute to the implementation of EU regulations, e.g., the EU Network and Information Security Directive (NIS Directive and NIS 2 Directive), the EU Cybersecurity Act (EUCSA), the General Data Protection Regulation (GDPR).

2.2 Relationship with international Standards & other Methodologies

Within this section, international standards and other methodologies relevant to the CYRENE RCA methodology are presented indicating the extent the CYRENE RCA methodology adopts them.

2.2.1 *Relation to ISO/IEC 27000-series*

ISO/IEC 27000- series³, also known as Information Security Management System (ISMS) Family of Standards, is a set of International Standards that are used to help organizations develop and implement a framework to manage information security risks and controls of their information assets as well as to prepare themselves to assess it. These standards can cover all types of organizations and all sizes, from micro to medium and large size businesses, that are involved in an SCS.

With the guidance of this family of standards' security techniques, the CYRENE RCA methodology uses the requirements for creating an ISMS set by ISO/IEC 27001:2013, and incorporates continuous improvement processes, such as the Plan-Do-Check-Act (PDCA) cycle, by committing the provider of the SCS as well as engaging the business partners involved in the whole procedure.

³ <https://www.iso.org/news/ref2266.html>

CYRENE also consults ISO/IEC 27002:2013, a compliance standard, which reports a list of controls for good security practices and the requisites that an existing method should have to be standard-compliant and includes specific risk handling aspects such as the identification of risk and the creation of an initial risk treatment plan.

By fixing a minimal framework, ISO/IEC 27005:2018 sets the requirements for the information security risk management process itself, for the identification of the threats and vulnerabilities allowing to estimate the risks, their level and then to be in a position to define an effective treatment plan. It also proposes the use of both quantitative and qualitative methods for the calculation of the risk level, which CYRENE takes into account; however, it does not support any specific technique for this purpose or any computational method to analyze and combine the assessment information.

2.2.2 Relation to ISO 28000-series

ISO 28000-series of standards is a set of requirements that organizations need to address to establish a management system to assure the quality or security of the aspects involved in the supply chain industry.

The standards of this series that CYRENE consults are ISO 28000:2007⁴, also known as Supply Chain Security Management System (SCSMS), which introduces the specifications, and ISO 28001:2007⁵, which provides best practices for SCS security implementation, assessments, and plans, as well as the requirements and guidance.

2.2.3 Relation to ISO/IEC 15408

ISO/IEC 15408⁶ (CC) establishes the concepts, principles, and techniques for IT security evaluation. The standard consists of three parts: the ISO/IEC 15408-1:2009 that introduces the general concepts and model, the ISO/IEC 15408-2:2008 that includes the security functional components, and the ISO/IEC 15408-3:2008 that describes the security assurance components.

More specifically, CYRENE uses the CC's concepts of Protection Profile (PP) and Target of Evaluation (TOE), as well as the Vulnerability Analysis (VA) assurance family, AVA_VAN. It also consults the Security Functional Requirements (SFRs) that are defined in CC as a translation of the security objectives for the Target of Evaluation (TOE) into a standardized language, the

⁴ <https://www.iso.org/standard/44641.html>

⁵ <https://www.iso.org/standard/45654.html>

⁶ ISO/IEC 15408-1/2/3:2008-09, <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408>

implementation of which addresses the threats of counterfeited or tainted products and components.

2.2.4 Relation to ISO/IEC 18045

CYRENE consults ISO/IEC 18045:2008⁷ as a companion standard of ISO/IEC 15408 that provides a methodology to help an IT security evaluator to conduct a CC evaluation by defining the minimum actions to be performed.

2.2.5 Relation to ETSI-TVRA

The ETSI-TVRA methodology⁸ orients security objectives, both to assets and their environments. CYRENE consults indicative examples that are presented in this methodology to better apprehend the distinction between the similar terms of security objectives and security requirements, which according to CC are of great importance. In addition, the CYRENE CA methodology takes into account the ETSI-TVRA methodology in terms of acknowledging the inherent factors on which the attack potential is dependent. The ETSI-TVRA factors considered to estimate the attack potential are based on the CC "Common Methodology for Information Technology Security Evaluation: "Evaluation methodology", 2009, v3.1 Rev.3⁹.

2.2.6 Relation to MITIGATE

The MITIGATE risk assessment methodology [4],[5],[6] provides a holistic view of the ICT infrastructure required for the provision of the supported SCS spanning across business partners and organization boundaries, in order to identify and evaluate all SC cyber threats and risks within the SC. MITIGATE promotes collaboration among BPs and takes into account the involvement and importance of the BPs in the provision of the SCS under consideration.

CYRENE methodology takes into account MITIGATE and enhances it with all the three metric groups of the latest version of CVSS, the v3.1, using a fuzzier logic, instead of a deterministic one, when applied in lower SCS assurance levels. In higher SCS assurance levels, the MITIGATE deterministic approach is used for the calculation of attack paths by CYRENE.

⁷ <https://www.iso.org/standard/46412.html>

⁸ https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

⁹ <https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf>

2.2.7 Relation to vulnerability severity of CVSS

The open framework of CVSS v3.1¹⁰ stands for Common Vulnerability Scoring System and is made for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups:

- the Base group, which represents the intrinsic qualities of a vulnerability that are constant over time and across user environments,
- the Temporal group, which reflects the characteristics of a vulnerability that change over time, and
- the Environmental group, which represents the characteristics of a vulnerability that are unique to a user's environment.

The Base metrics produce a score ranging from 0 to 10. Scoring also the Temporal and Environmental metrics, can then modify the Base score. A CVSS score is accompanied by a vector string, which in reality is a compressed textual representation of the values used to derive the score.

Using the CVSS 3.1 of FIRST¹¹, basic, temporal, and environmental metrics will be during the RCA process execution taking into account the implemented security controls on the identified SCS assets to estimate the Vulnerability Severity Level (VSL) presented in step 3.2 of section 5.3 of the current document.

Figure 3 depicts the metric groups of CVSS 3.1 to estimate the vulnerability severity:

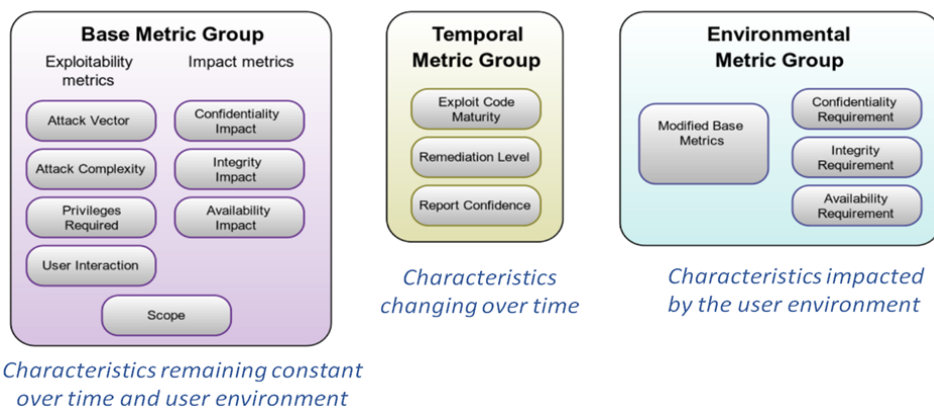


Figure 3– CVSS 3.1 base, temporal, and environmental metric groups.

CYRENE uses version 3.1 of CVSS from an SCS point of view and enhances the Environmental group metrics by helping the analyst define which options should be chosen for the under examination SCS according to specific considerations. In Table 1, the mapping between the Environmental Metrics of CVSS 3.1 vulnerability severity score and these CYRENE

¹⁰ <https://www.first.org/cvss/v3-1/>

¹¹ FIRST “Common Vulnerability Scoring System (CVSS) v3.1 Specification Document, Rev.1 (2019). Online available: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

methodology's considerations is analyzed. The following assumptions and notions have been adopted by CYRENE:

CYRENE assumes that the SCS-P with the collaboration of the SCS-BPs has an online inventory (an essential component of the **online SCS-ISMS**), managed by the SCS-Provider, where information about the **SCS-environment** (e.g., SCS-processes, SCS-asset models, individual SCS-assets with their controls and their documentations) has been uploaded and it is updated. Note that the documentation of the controls (implemented by each SCS-BP) will contain info regarding implementation/maintenance procedures, proofs of effectiveness (outcomes of penetration tests), and level of effectiveness.

CYRENE introduces the notion of the **criticality of an SCS-asset** based on the: number of SCS-processes that are being used, the importance of the SCS-process(es) it supports, and position of the asset in the SCS-asset model (how many steps before it can be reached).

CVSS v3.1 Environmental Metrics		CYRENE Customisations		Remarks	
Security Requirements	Confidentiality Requirement (CR)	CVSS score customization depending on the importance of the Confidentiality of the affected IT asset to a user's organization, relative to other impacts.	SCS Security Requirements	CVSS score customization depending on the importance of the Confidentiality of the affected SCS asset to the SCS, relative to other impacts.	The identification of the Security Requirements in CVSS v3.1 depends on the specific business environment of the organization and the value the asset has to the organization, while in CYRENE CA methodology depends on the SCS environment and SCS asset criticality to the provision of the SCS.
	Integrity Requirement (IR)	CVSS score customization depending on the importance of the Integrity of the affected IT asset to a user's organization, relative to other impacts.		CVSS score customization depending on the importance of the Integrity of the affected SCS asset to the SCS, relative to other impacts.	

	Availability Requirement (AR)	CVSS score customization depending on the importance of the Availability of the affected IT asset to a user's organization, relative to other impacts.		CVSS score customization depending on the importance of the Availability of the affected SCS asset to the SCS, relative to other impacts.	
Modified Base Metrics	Modified Attack Vector (MAV)	Assumption: the number of potential attackers for a vulnerability that could be exploited from across a network is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device.	SCS Modified Base Metrics	Assumption: that the number of potential attackers for a vulnerability that could be exploited from across a SC-chain is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device. CYRENE's Attack Vector could only be modified to "Network".	Both: Reflection of the context by which vulnerability exploitation is possible. In CYRENE: for MAV estimation the analyst needs to advice: - the SCS-ISMS inventory; - the asset model complexity (asset length, entry points).
	Modified Attack Complexity (MAC)	Description of the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.		Description of the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.	Both: Any requirements for user interaction in order to exploit the vulnerability is excluded. In CYRENE: for MAC estimation the analyst needs to advice: - the SCS-ISMS inventory; - the asset model complexity (asset length, entry points).
	Modified Privileges	This metric describes the level of privileges an attacker must		This metric describes the level of privileges an attacker must	In CYRENE: for MPR estimation the analyst needs to advice:

	Required (MPR)	possess before successfully exploiting the vulnerability.		possess before successfully exploiting the SCS asset's vulnerability.	<ul style="list-style-type: none"> - the SCS-ISMS inventory; - the asset model complexity (asset length, entry points).
	Modified User Interaction (MUI)	Caption of whether the vulnerability of a component can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.		Caption of whether the vulnerability of a SCS component can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.	<p>In CYRENE: for MUI estimation the analyst needs to advice:</p> <ul style="list-style-type: none"> - the SCS-ISMS inventory; - the asset model complexity (asset length, entry points).
	Modified Scope (MS)	Caption of whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope.		Caption of whether a vulnerability in one vulnerable SCS component impacts resources in other SCS components beyond its security scope.	<p>In CYRENE: for MS estimation the analyst needs to advice:</p> <ul style="list-style-type: none"> - the SCS-ISMS inventory; - the asset model complexity (asset length, entry points).
	Modified Confidentiality (MC)	Measurement of the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.		Measurement of the impact of the SCS asset's confidentiality to the provision of the SCS due to a successfully exploited vulnerability.	<p>In CVSS v3.1: estimation by the analyst based on specific characteristics of a user's environment within the organization.</p> <p>In CYRENE: For estimation the analyst needs to consider the SCS asset's configurations within the SCS environment:</p> <ul style="list-style-type: none"> - the SCS-ISMS inventory;
	Modified Integrity (MI)	Measurement of the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.		Measurement of the impact of the SCS asset's integrity to the provision of the SCS due to a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.	<ul style="list-style-type: none"> - the asset's criticality; - the asset model complexity i.e., check the SCS-asset location within the asset model and the complexity for

	Modified Availability (MA)	Measurement of the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.		Measurement of the impact of the SCS asset's availability to the provision of the SCS due to a successfully exploited vulnerability.	its reach (entry points, paths, length of paths).
--	-----------------------------------	--	--	--	---

Table 1 – CYRENE CA methodology considerations for the vulnerability severity measurement on SCS environments towards the Environmental Metric Group of CVSS 3.1.

More analytically, Table 1 consists of three main columns:

1. The **CVSS v3.1 Environmental Metrics**, which enables the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user’s organization, measured in terms of complementary/alternative security controls in place, Confidentiality, Integrity, and Availability. The metrics are the modified equivalent of Base metrics and are assigned values based on the component placement within the organizational infrastructure.
 - a. **Security Requirements:** These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user’s organization, measured in terms of Confidentiality, Integrity, and Availability. That is, if an IT asset supports a business function for which Availability is most important, the analyst can assign a greater value to Availability relative to Confidentiality and Integrity. Each Security Requirement has three possible values: Low, Medium, or High.
 - i. **Confidentiality Requirement (CR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Confidentiality of the affected IT asset to a user’s organization, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Confidentiality impact metric versus the other modified impacts.
 - ii. **Integrity Requirement (IR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Integrity of the affected IT asset to a user’s organization, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Integrity impact metric versus the other modified impacts.
 - iii. **Availability Requirement (AR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Availability of the affected IT asset to a user’s organization, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Availability impact metric versus the other modified impacts.
 - b. **Modified Base Metrics:** These metrics enable the analyst to override individual Base metrics based on specific characteristics of a user’s environment. Characteristics that affect Exploitability, Scope, or Impact can be reflected via an appropriately modified Environmental Score. The full effect on the Environmental score is determined by the corresponding

Base metrics. That is, these metrics modify the Environmental Score by overriding Base metric values, prior to applying the Environmental Security Requirements. For example, the default configuration for a vulnerable component may be to run a listening service with administrator privileges, for which a compromise might grant an attacker Confidentiality, Integrity, and Availability impacts that are all High. Yet, in the analyst's environment, that same Internet service might be running with reduced privileges; in that case, the Modified Confidentiality, Modified Integrity, and Modified Availability might each be set to Low. This metric intends to define the mitigations in place for a given environment. It is acceptable to use the modified metrics to represent situations that increase the Base Score. For example, the default configuration of a component may require high privileges to access a particular function, but in the analyst's environment, there may be no privileges required. The analyst can set Privileges Required to High and Modified Privileges Required to None to reflect this more serious condition in their particular environment.

- i. **Modified Attack Vector (MAV):** This metric reflects the context by which vulnerability exploitation is possible. This metric value (and consequently the Environmental Score) will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component. The assumption is that the number of potential attackers to a vulnerability that could be exploited from across a network is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device, and therefore warrants a greater Environmental Score.
- ii. **Modified Attack Complexity (MAC):** This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Such conditions may require the collection of more information about the target, or computational exceptions. The assessment of this metric excludes any requirements for user interaction in order to exploit the vulnerability (such conditions are captured in the User Interaction metric). If a specific configuration is required for an attack to succeed, the Base metrics should be scored assuming the vulnerable component is in that configuration.
- iii. **Modified Privileges Required (MPR):** This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability. The Environmental Score is greatest if no privileges are required.
- iv. **Modified User Interaction (MUI):** This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component. This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner. The Environmental Score is greatest when no user interaction is required.
- v. **Modified Scope (MS):** The Scope metric captures whether a vulnerability in one vulnerable component has impact on resources and components beyond its security scope. Formally, a security authority is a mechanism (e.g., an application, an operating system, firmware, a sandbox environment) that defines and enforces access control in terms of how certain subjects/actors (e.g., human users, processes) can access certain restricted objects/resources

(e.g., files, CPU, memory) in a controlled manner. All the subjects and objects under the jurisdiction of a single security authority are considered to be under one security scope. If a vulnerability in a vulnerable component can affect a component which is in a different security scope than the vulnerable component, a Scope change occurs. Intuitively, whenever the impact of a vulnerability breaches a security/trust boundary and impacts components outside the security scope in which vulnerable component resides, a Scope change occurs. The security scope of a component encompasses other components that provide functionality solely to that component, even if these other components have their own security authority. For example, a database used solely by one application is considered part of that application's security scope even if the database has its own security authority, e.g., a mechanism controlling access to database records based on database users and associated database privileges. The Environmental Score is greatest when a scope change occurs.

- vi. **Modified Confidentiality (MC):** This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The Environmental Score is greatest when the loss to the impacted component is highest.
 - vii. **Modified Integrity (MI):** This metric measures the impact on the integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information. The Environmental Score is greatest when the consequence to the impacted component is highest.
 - viii. **Modified Availability (MA):** This metric measures the impact on the availability of the impacted component resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component. The Environmental Score is greatest when the consequence to the impacted component is highest.
2. The **CYRENE Customisations** of the CVSS v3.1 Environmental Metrics, which enable the analyst to customize the CVSS score depending on the importance of the affected SCS-asset in the SCS environment, measured in terms of complementary/alternative security controls (documented in the SCS-ISMS) Confidentiality, Integrity, and Availability. The metrics are the modified equivalent of Base metrics based on the position of the SCS-asset in the SCS-asset model.
- a. **SCS Security Requirements:** These metrics enable the analyst to customize the CVSS score depending on the importance of the affected SCS asset, measured in terms of Confidentiality, Integrity, and Availability. That is, if an SCS asset supports an SCS business process for which Availability is most important, the analyst can assign a greater value to Availability relative to Confidentiality and Integrity. To identify the SCS asset value to the provision of the SCS, the analyst shall check:

- the SCS asset's criticality to the SCS
- the effectiveness of the security controls that each SCS partner has implemented for each SCS asset, which can be found in the SCS-ISMS inventory
- the asset model complexity.

Each Security Requirement has three possible values: Low, Medium, or High.

- i. **Confidentiality Requirement (CR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Confidentiality of the affected SCS asset to the SCS, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Confidentiality impact metric versus the other modified impacts.
 - ii. **Integrity Requirement (IR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Integrity of the affected SCS asset to the SCS, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Confidentiality impact metric versus the other modified impacts.
 - iii. **Availability Requirement (AR):** This metric enables the analyst to customize the CVSS score depending on the importance of the Availability of the affected SCS asset to the SCS, relative to other impacts. This metric modifies the Environmental score by reweighting the Modified Confidentiality impact metric versus the other modified impacts.
- b. **SCS Modified Base Metrics:** These metrics enable the analyst to override individual Base metrics based on specific characteristics of the SCS environment. Characteristics that affect Exploitability, Scope, or Impact can be reflected via an appropriately modified Environmental Score. The full effect on the Environmental score is determined by the corresponding Base metrics. That is, these metrics modify the Environmental Score by overriding Base metric values, before applying the Environmental SCS Security Requirements. To modify the Base Metrics value to the SCS asset's vulnerability, the analyst shall check the SCS asset's criticality to the SCS and the effectiveness of the security controls that are implemented on this asset. This metric intends to define the mitigations in place for a given SCS environment. It is acceptable to use the modified metrics to represent situations that increase the Base Score.
- i. **Modified Attack Vector (MAV):** This metric reflects the context by which vulnerability exploitation is possible. This metric value (and consequently the Environmental Score) will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component. The assumption is that the number of potential attackers for a vulnerability that could be exploited from across an SC-chain is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device, and therefore warrants a greater Environmental Score. As the Scope of CYRENE is limited to assets that are connected directly with other assets of the same SCS, the Attack Vector could only be modified to "Network". The further the distance, the greater number of potential attackers may be to exploit the vulnerability.
 - ii. **Modified Attack Complexity (MAC):** This metric describes the conditions beyond the attacker's control that must exist in order to exploit the

vulnerability. Such conditions may require the collection of more information about the target, or computational exceptions. The assessment of this metric excludes any requirements for user interaction in order to exploit the vulnerability (such conditions are captured in the User Interaction metric). If a specific configuration is required for an attack to succeed, the Base metrics should be scored assuming the vulnerable component is in that configuration.

- iii. **Modified Privileges Required (MPR):** This metric describes the level of privileges an attacker must possess before successfully exploiting the SCS asset's vulnerability. The Environmental Score is greatest if no privileges are required.
- iv. **Modified User Interaction (MUI):** This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable SCS component. This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner. The Environmental Score is greatest when no user interaction is required.
- v. **Modified Scope (MS):** The Scope metric captures whether a vulnerability in one vulnerable SCS component impacts resources in other SCS components beyond its security scope. Formally, a security authority is a mechanism (e.g., an application, an operating system, firmware, a sandbox environment) that defines and enforces access control in terms of how certain subjects/actors (e.g., human users, processes) can access certain restricted objects/resources (e.g., files, CPU, memory) in a controlled manner. All the subjects and objects under the jurisdiction of a single security authority are considered to be under one security scope. If a vulnerability in a vulnerable SCS component can affect another SCS component that is in a different security scope than the vulnerable component, but still belongs to the SCS asset modeling, a Scope change occurs. Intuitively, whenever the impact of a vulnerability breaches a security/trust boundary and impacts SCS components outside the security scope in which vulnerable SCS component resides, a Scope change occurs. The security scope of an SCS component encompasses other SCS components that provide functionality solely to that component, even if these other components have their own security authority. For example, a database used solely by one application is considered part of that application's security scope even if the database has its own security authority, e.g., a mechanism controlling access to database records based on database users and associated database privileges. The Environmental Score is greatest when a scope change occurs.
- vi. **Modified Confidentiality (MC):** This metric measures the impact of the SCS asset's confidentiality on the provision of the SCS due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The Environmental Score is greatest when the loss to the impacted SCS component is highest.

- vii. **Modified Integrity (MI):** This metric measures the impact of the SCS asset's integrity on the provision of the SCS due to a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
The Environmental Score is greatest when the consequence to the impacted SCS component is highest.
 - viii. **Modified Availability (MA):** This metric measures the impact of the SCS asset's availability to the provision of the SCS due to a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted SCS component, this metric refers to the loss of availability of the impacted SCS component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component.
3. The **Remarks**, which point out the differences between the previous two and provides additional information.
- a. **SCS Security Requirements:** The identification of the Security Requirements in CVSS v3.1 depends on the specific business environment of the organization and the value the asset has to the organization. The identification of the Security Requirements in CYRENE RCA methodology depends on the SCS environment and SCS asset criticality to the provision of the SCS.
 - i. The identification of the Security Requirements in CVSS v3.1 depends on the specific business environment of the organization and the value the asset has to the organization.
 - ii. The identification of the Security Requirements in CYRENE RCA methodology depends on the SCS environment and SCS asset criticality to the provision of the SCS,
 - b. **SCS Modified Base Metrics:**
 - i. **Modified Attack Vector (MAV):** In CYRENE RCA methodology in order to estimate the MAV score the analyst needs
 - 1. to explore the developed SCS-ISMS inventory to identify the strength of the implemented security controls to the SCS assets
 - 2. the asset model complexity: the distance that exists between a possible asset entry point and the targeted asset (asset length), and from how many assets entry points an attacker can access it (asset entry points).
 - ii. **Modified Attack Complexity (MAC):** In CYRENE RCA methodology in order to select the MAC value, in addition to the CVSS specification for this metric, the analyst shall check:
 - 1. the SCS location within the SCS network
 - 2. the asset model complexity (asset length, entry points).
 - iii. **Modified Privileges Required (MPR):** To select the MPR value, in addition to the CVSS specification for this metric, the analyst should check the SCS- check the SCS- asset location within the asset model and the complexity for its reach (entry points, paths, length of paths).
 - iv. **Modified User Interaction (MUI):** In CYRENE CA methodology to select the MUI value, in addition to the CVSS specification for this metric, the

analyst should check the SCS- asset location within the asset model and the complexity for its reach (, entry points, paths, length of paths).

- v. **Modified Scope (MS):** To select the MPR value, in addition to the CVSS specification for this metric, the analyst should check the SCS-asset location within the asset model and the complexity for its reach (, entry points, paths, length of paths).
- vi. **Modified Confidentiality (MC), Modified Integrity (MI), Modified Availability (MA):** In CVSS v3.1 these metrics are estimated by the analyst based on specific characteristics of a user's environment within the organization.

In CYRENE CA methodology these metrics are estimated by the analyst considering the SCS asset's configurations within the SCS environment:

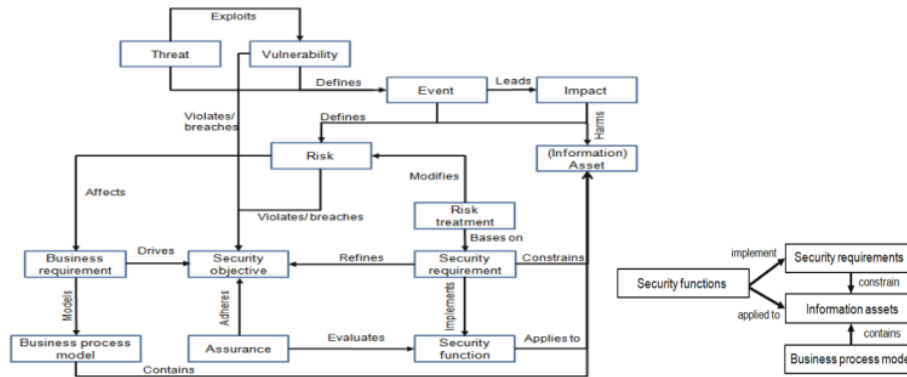
- the developed SCS-ISMS inventory to identify the strength of the implemented security controls to the SCS assets
- the asset's criticality,
- the asset model complexity i.e., check the SCS-asset location within the asset model and the complexity for its reach (, entry points, paths, length of paths).

2.3 Extended Security Model

The extended security model, described in this section, demonstrates the interconnections among the terms of risk assessment and conformity assessment. **This relation reveals the double use of the CYRENE RCA methodology**, i.e., it can be used by the SCS- providers and partners to manage their cyber risks and generate the SCS Protection Profile (SCS-PP); and also by the assessors to assess the SCS-PP claims, generate the audit report and issue an SCS certificate.

On the upper part of Figure 4, the concepts related to risk management (according to ISO/IEC 2700x family of standards) are being presented whereas on the lower part, we see how these concepts are used for conformity assessment (according to ISO/IEC15408 and ISO/IEC18045). In particular, in the upper part, we see how the threats exploit vulnerabilities that may lead to a (security) event that impacts the (information) assets. The threat, vulnerability, and impact levels are the three factors used to estimate the cyber risk level of the asset to the particular threat. Controls and mitigation actions will reduce the risks (Risk treatment Plan).

Extended Information Security Model



(Source: Taubenberger, Stefan (2014) "Vulnerability Identification Errors in Security Risk Assessments". PhD thesis The Open University).



!#\$%&'()*+,-./:;<=>?@A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\] ^ _ ` { | } ~ ¡ ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬ ® ¯ ° ± ² ³ ´ µ ¶ · ¸ ¹ º » ¼ ½ ¾ ¿

Figure 4 – Extended Information Security Model that connects Risk and Conformity Assessment¹².

On the lower part of the above picture, we see the concepts related to conformity assessment (according to ISO15408 and ISO 18045). In particular, we see that the risks affect the business requirements which can be expressed in terms of process models. The business requirements drive the security objectives (which are defined according to the assurance, refined by the security requirements and) selected controls and mitigation actions are selected according to the security requirements of the assets. Also, the security requirements are used to implement security functions.

The use of the CYRENE-CA will enable the SCS-providers with the business partners to manage the risks of the SCS and also develop the SCS-PP. The SCS-PP is required by the assessor to be provided for the SCS to be assessed (SCS- Target of Evaluation (TOE) following the guidelines of the SCS scheme (see CYRENE Report 2 [2]) against the claims found in SCS-PP (Figure 5).

¹² <http://oro.open.ac.uk/39626/>

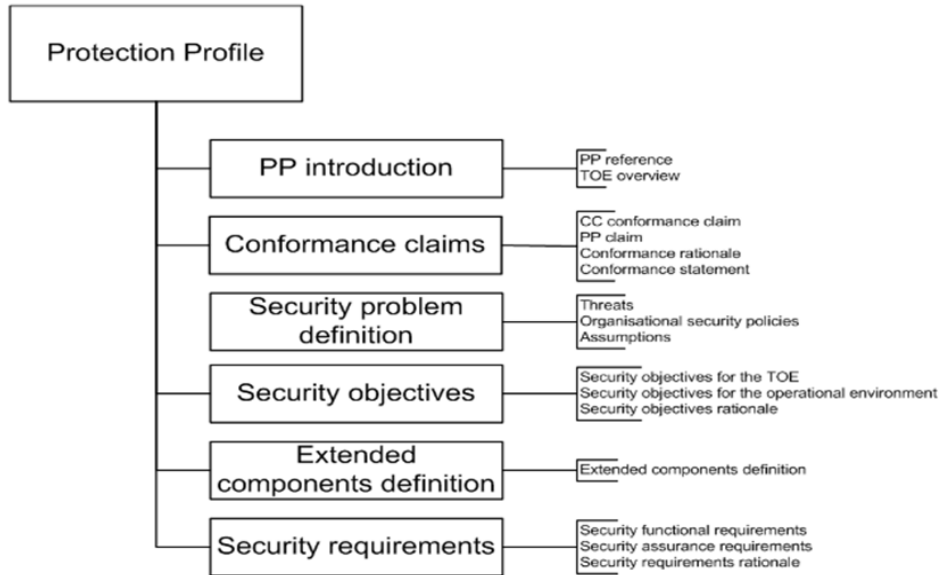


Figure 5 – The Protection Profile (PP) as presented in the Common Criteria (CC), 2017 [7].

Another similar model that reveals the connections of the risk assessment (ISO/IEC 2700x) and conformity assessment (ISO/IEC 15408) was provided by ENISA AHWG on Risk Assessment [8].

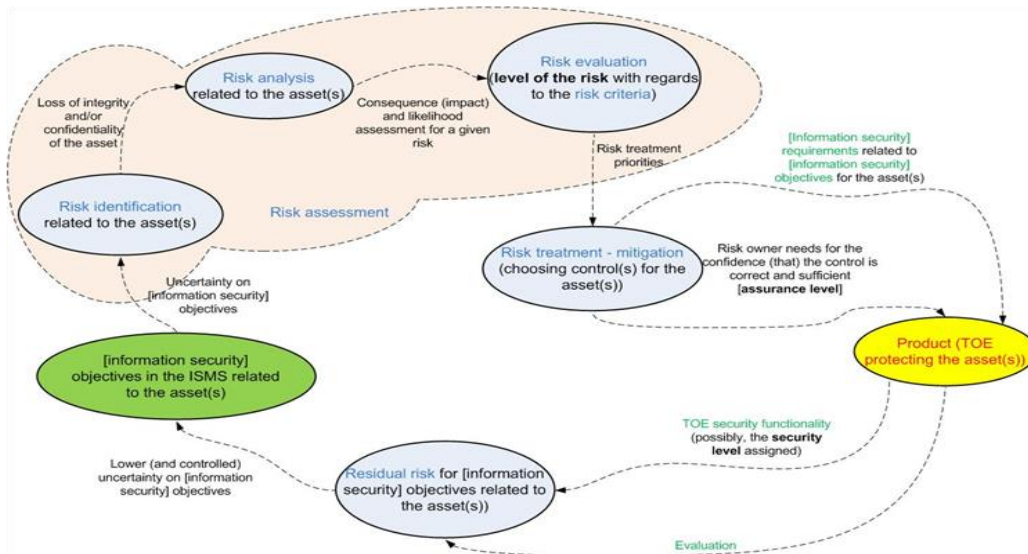


Figure 6 – ENISA AHWG on Risk Assessment, 2020 (Coordinator: Cord Bartels) [8].

The above diagram shows that the security objectives of the asset and the information related to the asset and found in the ISMS are inputs to the risk assessment phases (risk identification/analysis/evaluation), that feed the risk management phase (risk treatment-migration phase). The output of the risk treatment is used to generate the Protection Profile (PP) of the product that is the TOE. Once the PP is submitted for evaluation, the residual risk (risk remaining after risk treatment) is reported.

2.4 Assurance of SCS

Assurance grounds for confidence that an asset meets the Security Functional Requirements (SFRs). Assurance level is the basis for confidence that an asset meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an asset has been evaluated but as such **does not measure the security** of the asset concerned (cf. EUCSA, article 2.22 [3]). Assurance corresponds to the proofs and evidence that the implemented controls address the SFRs provided in the risk treatment Plan.

The **Evaluation Assurance Level (EAL)** corresponds to guidance directed at security control implementers; EAL specifies the nature and extent of control implementation/applicability by providing evidence (supporting documentation e.g. test cases/ test outcomes) in the Risk Treatment Plan.

The EAL does not measure the level of security/vulnerability or risk level but rather **measures the level of confidence that the controls are adequate to address the SFRs**. Therefore, a higher EAL does not necessarily indicate a more secure (a low vulnerability level) asset.

ISO/IEC 15408 (CC) establishes the concepts, principles, and techniques for IT security evaluation. The standard consists of three parts: the ISO/IEC 15408-1:2009 that introduces the general concepts and model, the ISO/IEC 15408-2:2008 that includes the security functional components, and the ISO/IEC 15408-3:2008 that describes the security assurance components.

The EU Cybersecurity Act (EUCSA) presents an assignment of the assurance levels as they shall be based on the use of the assurance components for vulnerability assessment defined in ISO/IEC 15408-3:2008.

2.4.1 Identification of Attack Potential in CYRENE

In this section, the Attack Potential (AP) metric (see Section 8) is identified in the context of the CYRENE RCA methodology. At first, it is described with regards to the ISO/IEC 15408 and ETSI-TVRA methodology, and then with regards to the attacker's profile characteristics according to NIST and some other latest research approaches. Eventually, the AP metric and attacker's profile are presented in the scope of the CYRENE SCS assurance scales.

2.4.1.1 Attack Potential according to ISO/IEC 15408 and ETSI-TVRA

The ISO/IEC 15408-1:2009¹³ international standard and the ETSI-TVRA methodology¹⁴ consider the *Attack Potential (AP)* metric as a measurement of the "effort needed to exploit a vulnerability (-ies) in a TOE".

¹³ <https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en>

¹⁴ https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

The “effort” is expressed as a function of properties related to the attacker (e.g. motivation, capabilities, means, objectives) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure). AP is used to conduct the vulnerability analysis and determine the selection of controls.

Concerning the above considerations, the ISO/IEC 15408 and ETSI-TVRA methodology take into account a set of factors enlisted below, to estimate the overall attack potential required to exploit a vulnerability. These factors are:

- **TOE Knowledge:** Knowledge of the TOE refers to specific expertise in relation to it. Type of knowledge can be: Public information/ Restricted information/ sensitive/critical
- **Time:** The total amount of time (elapsed time) taken by an attacker to identify that a particular, potential, weakness may exist, develop an attack method and sustain the effort required to mount the attack. Adopt the worst-case scenario. Duration: minutes/ hours/ days/ weeks/ months
- **Expertise:** The level of general knowledge of the underlying principles, product type, or attack methods. Level of Expertise: Laymen/ Efficient/ Experts
- **Opportunity/Access to the ToE:** Related to the Elapsed Time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to an asset that may increase the likelihood of detection. (i.e. effort off-line, continuous access, access over a number of sessions)
- **Window of opportunity:** (Access to an asset) (i.e. effort off-line, continuous access, access over a number of sessions)
- **Equipment:** Addresses the IT hardware/software or other equipment required to identify or exploit a vulnerability. Equipment: Standard/ Specialized/ Bespoke/ Multiple bespoke.

2.4.1.2 Attacker’s Potential in relation to adversary’s characteristics

In [9], to develop quantifiable psychological attacker’s personality profiles, the Fogg Behaviour Model along with the facets of the big five personality traits of agreeableness, extraversion, conscientiousness, neuroticism, and openness to experiences. These personality traits can be affected by genetic, environmental, and genes’ factors combined with alternative ways of thinking. In addition, such considerations are explored towards the characteristics of the attacker’s potential as defined in NIST [10], shown in Table 2.

Characteristics of the attacker’s potential by NIST			
Qualitative Values	Semi-Quantitative Values		Description of the Attacker
Very High	96-100	10	A very sophisticated level of expertise
High	80-95	8	A sophisticated level of expertise
Moderate	21-79	5	Moderate resources
Low	5-20	2	Limited resources
Very Low	0-4	0	Very limited resources

Table 2 – Description of the attacker’s capability.

Within this framework, an attacker’s multi-dimensional profile is proposed in [9], shown in Table 3.

Facets	
Personality Traits	Extraversion
	Conscientiousness
	Openness to experiences
Social Traits	Selected social exposure
	Not conventional relationships
	Not talkative
	Manipulative
Technical skills & Resources	Networking skills
	IT skills
	Soft skills
	Forensics skills
	Available resources
	Relationship with the organization (insider, outsider, supplier/SCS partner)
Motivations	e.g. economic, political, commercial or governmental espionage, etc.
Triggers	e.g. Zero-day vulnerability warnings for attacks, price published in the Dark Web for those that will successfully exploit the vulnerability, hackers' groups, etc.

Table 3 – Attacker’s multi-dimensional profile [9].

More analytically, each personality trait contains the following characteristics:

- Extraversion: gregariousness, assertiveness/outspokenness, activity/energy level, positive emotions/mood;
- Conscientiousness: orderliness/neatness, achieving-striving/perseverance, self-discipline, dutifulness/carefulness), self-efficacy;
- Openness to experiences: intellect/creativity, imaginative, scientifically interested/originality, adventurousness.

Respectively, each social trait consists of the characteristics below:

- Selected social exposure: difficult to adapt to conventional social norms, easy to build strong e-bonds with co-hackers in communities in the Deep Web - these communities are open by invitation only;
- Not conventional relationships: finds social situations difficult, easy to build professional virtual relationships, hackers enter virtual communities building strong relations and discover security vulnerabilities through social engineering, which helps them to execute sophisticated attacks;
- Not talkative: difficult to initiate social talks, difficult to express him/herself in a social setting;
- Manipulative: leads people into providing confidential information to compromise information systems.

Moreover, each technical skill or resource is explained as follows:

- Networking skills: functional and operational aspects of e.g. routers and switches, DNS, HCP;
- IT skills: Operating Systems, Languages, Software and emerging technologies;
- Soft skills: problem solver, team worker;
- Forensics skills: use security scripts, forensics tools;
- Available resources: owns or has access to high computer processing power (e.g. powerful machines, multiple Virtual Machines, HPCs) and security communities (e.g. hacking/penetration testing/cryptanalytic).

In addition, the relationship with the organization includes an insider (works in the organization), a supplier/Supply Chain partner (provides services or part of the organizations' value chain), or an Outsider.

The motivations could be either economic, political, commercial, or governmental espionage, boredom, fun, revenge, evangelists of governmental openness and transparency ("us against them" view), or whistle blower (warns the society of any digital wrongdoings).

Finally, what could trigger someone to such an attack is zero-day vulnerability warnings for attacks, the price published in the Dark Web for those that will exploit the vulnerability, hackers' groups, announced that work on the exploitation of this new vulnerability, etc.

After the analysis of the abovementioned, the research work of [9] continues by proposing a quantification of the attacker's profile, depicted in Table 4.

Qualitative Values	Semi-Quantitative Values		Description of the Attacker
Very High (expert attacker)	96-100	10	Has 100% of the traits described in Table 3 in all categories
High (experienced attacker)	80-95	8	Has more than 80% of the traits described in Table 3
Moderate (junior attacker)	21-79	5	Has more than 20% of the traits described in Table 3
Low (mature attacker)	5-20	2	Has more than 5% of the traits described in Table 3
Very Low (not skilled attacker)	1-4	1	Has less than 4% of the traits described in Table 3

Table 4 – Proposed quantification of attacker's profile [10].

As a result, capturing the attacker's characteristics and identifying the level of his capability, a set of traits (i.e. personality, technical skills and resources, relationship with the organization, motivation, triggers) should be taken into consideration to structure his/her profile. The analysis of the attacker's profile is directly connected with the effort (s)he is expected to provide to exploit a vulnerability. The higher score of the adversary, the most likely the attack will be successful, thus the attack potential (AP) will be increased as the score of the attacker's profile increases, and hence the vulnerability will be exploited resulting in a higher vulnerability level. The connections of the notions will be further exploited in the next section.

2.4.2 CYRENE SCS vulnerability evaluation scale in relation to the Attack Potential

ISO/IEC 18045:2008-3 identifies five different levels for the assurance class AVA, and the “Levelling is based on an increasing rigor of vulnerability analysis by the assessor and increased levels of AP required by an attacker to identify and exploit the potential vulnerabilities” [11].

Considering this vulnerability analysis evaluation scale (AVA_VAN assurance class) of ISO/IEC 18045:2008 (CC), Table 5 demonstrates the related actions that should be undertaken to identify potential vulnerabilities and estimate the SCS- TOE resistance to the AP on an adopted assurance level in both cases of the dual use of the CYRENE RCA methodology which are addressed in section 2.3 (enhanced SCS-RA, utilized by the SCS-P and SCS-BPs to handle their cyber risks and develop the SCS-PP and CAP, utilized by the SCS-assessors to assess the SCS-PP claims, create the audit report and issue an SCS certificate). Moreover, based on the ISO/IEC 18045 (CC), the following table maps the corresponding rigor and depth of the vulnerability analysis evaluation (assurance class AVA) required to ensure that the SCS- TOE is resistant to attacks committed by an attacker with a specified level of Attack Potential (AP). Last but not least, following the ISO/IEC 18045:2008 (CC) the minimum AP needed to commit an attack in a given vulnerability analysis evaluation is explored as well.

	SCS-provider Action elements	Assessor’s actions to identify potential vulnerabilities	Assessor’s actions to identify the strength of the implemented controls in relation to AP	Attacker Profile/ Attack Potential (AP)	EAL
AVA_VAN 1	Provides the SCS, suitable for testing	Confirms that the information provided (all components in SCS-environment) is sufficient to identify the perimeter of the assessment	Penetration testing - Basic AP	Enhanced Basic	1
		Searches public domain sources to identify potential vulnerabilities in the SCS-assets			
AVA_VAN 2	Provides the SCS, suitable for assessment	Considers specific SCS environment dependencies for the vulnerability analysis	Penetration testing - Basic AP	Enhanced Basic	2,3

		Identifies potential SCS vulnerabilities			
AVA_VAN 3	Provides the SCS, suitable for testing	Conducts a focused vulnerability analysis including the previous actions	Penetration testing - Enhanced-Basic AP	Moderate	4
AVA_VAN 4	Provides the SCS- TOE, suitable for testing	Conducts an independent, methodical vulnerability analysis including all the previous actions	Penetration testing - Moderate AP	High	5
AVA_VAN 5	Provides the SCS-ToE, suitable for testing	Conducts an independent, methodical vulnerability analysis including all the previous actions	Penetration testing - High AP	Beyond High	6,7

Table 5 – CYRENE vulnerability analysis evaluation scale in relation to the Attack Potential (AP).

More analytically, for each AVA_VAN level, the following series of actions should be made in terms of conducting CYRENE vulnerability analysis evaluation:

AVA_VAN 1:

- The SCS-provider should provide the SCS, suitable for testing;
- The evaluator should confirm that the information provided (all components in SCS-environment) is sufficient to identify the perimeter of the assessment and proceed with the assessment and then search public domain sources to identify potential vulnerabilities in the SCS-assets;
- Penetration testing should be conducted by the evaluator based on the identified potential vulnerabilities (unless outcomes of such tests are in the documentation of the SCS-ISMS inventory) to determine the resistance of SCS to attacks performed by an attacker possessing **Basic AP**.

AVA_VAN 2:

- The SCS-provider should provide the SCS suitable for assessment;
- The following dependencies of the SCS environment are considered for the vulnerability analysis by the assessor:
 - ADV_ARC.1 Security architecture description,
 - ADV_FSP.4 Complete functional specification,
 - ADV_TDS.3 Basic modular design,
 - ADV_IMP.1 Implementation representation of the TSF,
 - AGD_OPE.1 Operational user guidance,
 - AGD_PRE.1 Preparative procedures,
 - ATE_DPT.1 Testing: basic design;
- An independent vulnerability analysis should be conducted by the evaluator, including the previous actions and using guidance documentation, functional specification, SCS design, and security architecture description and representation derived from SCS-BPs assets

and corresponding assets' and security controls' documentation in the SCS-ISMS and MRA to identify potential vulnerabilities in the SCS;

- Penetration testing should be conducted by the evaluator, based on the identified potential vulnerabilities (unless the outcomes of such tests are in the documentation of the SCS-ISMS inventory) to determine the resistance of SCS to attacks performed by an attacker possessing **Basic AP**.

AVA VAN 3:

- The SCS-provider shall provide the SCS, suitable for testing;
- A **focused** vulnerability analysis should be conducted by the evaluator, including the previous actions, i.e. guidance documentation, functional specification, SCS design, security architecture description derived from SCS-BPs assets and corresponding security controls documentation embedded in the SCS-MRA and the developed CYRENE SCS-ISMS inventory enhanced by an **implementation representation** to identify potential vulnerabilities in the SCS;
- Penetration testing should be conducted by the evaluator, based on the identified potential vulnerabilities (even if outcomes of such tests are found in the controls' documentation in the SCS-ISMS inventory), to determine the resistance of SCS to attacks performed by an attacker possessing **Enhanced-Basic AP**.

AVA VAN 4:

- The SCS-provider should provide the SCS- TOE, suitable for testing;
- An **independent, methodical** vulnerability analysis including all the previous actions shall be conducted by the evaluator;
- Penetration testing should be conducted by the evaluator, based on the identified potential vulnerabilities (even if outcomes of such tests are found in the controls' documentation in the SCS-ISMS inventory) to determine the resistance of SCS to attacks performed by an attacker possessing **Moderate AP**.

AVA VAN 5:

- The SCS-provider should provide the SCS- TOE, suitable for testing;
- An independent, methodical vulnerability analysis including all the previous actions should be conducted by the evaluator;
- Penetration testing should be conducted by the evaluator, based on the identified potential vulnerabilities (even if outcomes of such tests are found in the controls' documentation in the SCS-ISMS inventory) to determine the SCS is resistant to attacks performed by an attacker possessing **High AP**.

2.4.3 CYRENE Levels of Attacker's Profile

According to the previous sections, the Attack Potential (AP) depends on the attacker's profile (composed by various characteristics) and according to ISO/IEC 15408-1:2009 and NIST [10], it is considered as the effort needed for an asset to be attacked, in terms of an attacker's expertise, resources, and motivation. The AP in CYRENE depends on the attacker's profile. In the following Table 6, the CYRENE attacker's profile is developed on five distinct levels taking into account the 5 levels of AP presented by ENISA in its September 2021 report "Methodology for Sectoral

Cybersecurity Assessments - EU Cybersecurity Certification Network¹⁵ and concerning the attacker's characteristics (cf. section 2.4.1.2). The AP is required to employ a successful attack with regards to an adopted level of vulnerability analysis evaluation (how deep and rigorous the vulnerability analysis should be) of assurance class AVA (CC) (cf. section 2.4.2).

	Attacker Profile 1	Attacker Profile 2	Attacker Profile 3	Attacker Profile 4	Attacker Profile 5
Attacker's characteristics	An unskilled agent with very limited resources and opportunity	A skilled agent with limited resources and opportunity	A skilled agent with moderate resources and the opportunity	Agent of a sophisticated level of expertise with significant resources and opportunity	Agent of a very sophisticated level of expertise with significant resources and opportunity
Equivalent ISO/IEC 18045 Attack Potential (AP)	Basic	Enhanced-Basic	Moderate	High	Beyond High
Related AVA_VAN assurance component	AVA_VAN.1,2	AVA_VAN.3	AVA_VAN.4	AVA_VAN.45	N/A

Table 6 –Relation between Assurance elements.

2.4.4 CYRENE SCS assurance scale

As presented in the previous section 2.4.2, the AVA_VAN assurance family is the basis for the vulnerability analysis in ISO/IEC 15408-3.

The use of AVA_VAN as a key parameter allows flexibility for comparing assurance level implementations and this is why it is used in CYRENE methodology. This assignment is shown in the following table:

Vulnerability Analysis Level (AVA Class) (ISO/IEC 15408-CC)	Assurance Level (AL) (EUSCS)	CYRENE Assurance of SCS	EAL (ISO/IEC 15408-CC)

¹⁵ <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

AVA_VAN.1 Vulnerability survey	Basic	SCS is neither an essential nor important service according to NIS 2 directive [13]. The SCS-Provider is not a provider of essential services (according to NIS).	1
AVA_VAN.2 Vulnerability analysis	Substantial	SCS is an important service according to NIS 2 Directive. The SCS-Provider is a provider of important services (according to NIS).	2,3
AVA_VAN.3 Focused vulnerability analysis	Substantial	SCS is an essential service according to NIS and European (the SCS business partners involved are only EU) The SCS-Provider is a provider of essential services (according to NIS).	4
AVA_VAN.4 Methodical vulnerability analysis	High	SCS is an international essential NIS service (including non-EU SCS business partners) and the SCS-Provider is a provider of essential (international) services.	5
AVA_VAN.5 Advanced Methodical/ Advanced Technical/vulnerability analysis	High	SCS is a military/defense service. The SCS provider is a provider of essential service (national security, law enforcement).	6,7

Table 7 – Identification of the CYRENE SCS assurance scale.

As depicted in Table 7, the SCS criticality is evaluated on the following criteria: (i) whether the SCS resides in the Military / Defence sector, (ii) whether the SCS-P is considered an Operator of Essential Services (OES) or an Operator of Important Services (OIS), according to NIS 2 Directive [13] (described in CYRENE Report 2 and depicted in Appendix F-IV), (iii) whether the SCS is an international service or a European service. The terms “essential service”, “important service” and “international SCS” are further explained in Glossary (section 8). In addition, CYRENE SCS criticality is presented in a five-tier qualitative scale from “Very Low” to “Very High”, shown in Appendix F-IV of the current document.

3 CYRENE RCA Methodology Design Criteria

As described in section 2.1, the CYRENE RCA methodology provides a dual purpose of use; either to identify SCS risks, investigate the risk treatment and produce an SCS-PP (for SCS-P and SCS-BPs) or to check whether the claims of PP are valid and the SCS can be subject to

security certification according to the proposed EUSCS (see CYRENE Report 2 [2]) (for assessors). The methodology is structured following a sequential step-by-step approach, with distinct scope, inputs, and outcomes for each step. It is designed to be applicable to all sectors of SCS following evidence-based cybersecurity and privacy-aware conformity process that can adopt different assurance levels. It is compliant with EU and international regulations and standards. The CYRENE RCA methodology is considered collaborative as it requires the cooperation of SCS operators and other parties to be undertaken. In addition, the CYRENE RCA methodology is developed to cover different SCS perspectives mentioned in section 2.1.

The current section aims to enlist all notifications and assumptions needed, enclosing ontology requirements and requirements for security standards, to build the blocks of the CYRENE RCA methodology. Through this section, an overview of the methodology (i.e. basic steps, elements, and interrelations) will be presented in an ontology model. Eventually, the use of the current methodology is presented towards its dual-use and SCS different perspectives capability.

3.1 Notifications and Assumptions

In CYRENE Report 1 [12] and the CYRENE site¹⁶, the reader may find a glossary and interrelation of terms. In this report, we use only the terms necessary for the methodology (see Glossary in section 8).

The CYRENE CA methodology takes as a basis the following notifications and/or assumptions:

- The perimeter of the CYRENE SCS Risk Assessment (SCS-RA) includes only the SCS-assets in the provision of the SCS;
- The SCS-assets hosted by the different SCS Business Partners (SCS-BPs) are isolated from their organization network. Thus, only the SCS asset interdependencies are considered;
- Each SCS-BP has submitted their security policies in the SCS-ISMS along with the SCS-assets that they host and implemented controls documentation (implementation report, patches, exploits available, penetration testing results, certificates from vendors)
- The SCS Provider (SCS-P) and the SCS-BPs have signed an SCS Security Declaration and Application statement (SDA) that considers all above obligations;
- To use the CYRENE RCA methodology as a CAP and assess the claims of the PP, the SCS Provider, the SCS-BPs and the assessor (either self-assessor or CAB) should have signed an SCS Mutual Recognition Agreement (MRA) (see CYRENE Report 2) that considers all auditing and reviewing procedures and sets the mutual conditions for the recognition of certificate;
- Assurance level and thus attacker's maturity level / AP for the SCS are inputs for the methodology (Table 7);
- Only technical threats are considered for the overall technical view and sectorial view of the SCS, whereas for the business view of the SCS only business threats are considered;
- The SCS-P with the collaboration of the SCS-BPs has an online inventory that will be embedded in the SCS-ISMS managed by the SCS-P, where information about the SCS-

¹⁶ <https://www.cyrene.eu/glossary/>

environment (e.g. SCS-processes, SCS-asset models, individual SCS-assets with their controls and their documentations) has been uploaded and it is updated;

- The documentation of the controls (implemented by each SCS-BP) will contain info regarding implementation/maintenance procedures, proofs of effectiveness (outcomes of penetration tests), level of effectiveness;
- Five distinct levels of attacker's profile have been identified for the CYRENE RCA methodology with respect to Table 6;
- The assurance level of the SCS has been pre-defined according to Table 7;
- The level of the vulnerability analysis that has to be undertaken during the evaluation process of the CYRENE RCA methodology is identified according to the predefined SCS assurance level (Table 7);
- To identify interdependencies among entities (e.g. asset interdependencies, business partners' interactions) and recognize other types of relations (e.g. threats/vulnerabilities associated with SCS-TOE assets) within the SCS-TOE, an ontology is built to represent all knowledge that can be extracted from the SCS-TOE and define relevant semantics. The generated semantics from the developed methodology will be utilized with additional reasoning mechanisms' implementations to detect anomalies for serving threat monitoring and vulnerability management purposes.

3.1.1 Enhanced Risk and Conformity assessment ontology requirements

The conceptual models defined by CYRENE are considered as the basis for modeling an asset and its dependencies (Figure 7). Four circles of consideration were defined in order to analyze the SCS from different aspects. These areas of consideration were mapped into three different perspectives including i) business; ii) asset and iii) sector-specific views. Therefore, an important requirement for the Cyrene ontology is to apply these perspectives in order to model assets and their dependencies. At the business view level, the ontology should support the representation of elements related to the business view, including business processes, organizational processes, business partners, and business logic. At the asset level, the ontology should support the representation of assets related to the SCS and provide the ability to clearly differentiate the types of assets (for example, ICT, network-connected, software, human). At the Sector view level, the ontology should allow the representation of sector-specific elements.

It is also an important requirement for the ontology to ensure that it can be used in consequent project tasks to support risk and privacy assessment of SCS through the three defined horizontal layers: HL1, HL2, and HL3.

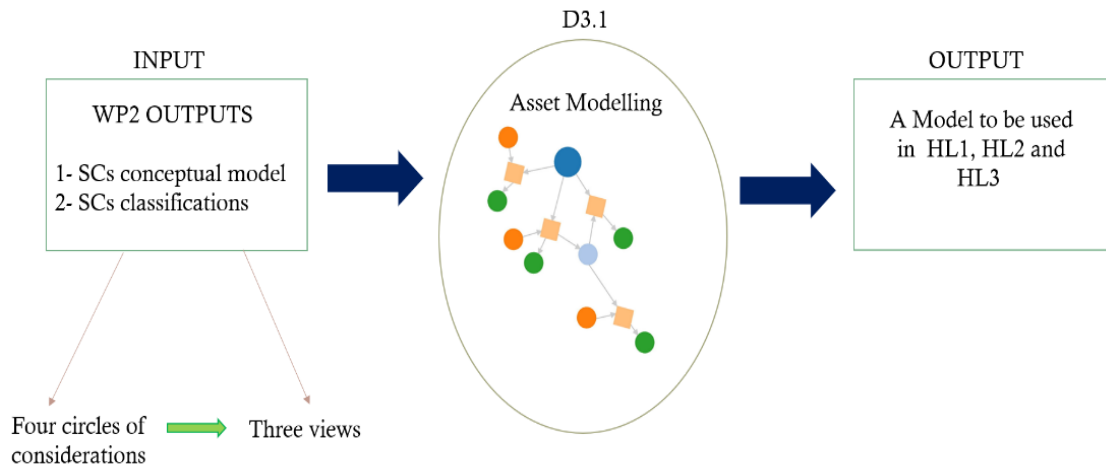


Figure 7 – Requirements for developing the CYRENE ontology model.

3.1.2 Requirements for Adopted Security Standards

General security requirements for the SCSs are defined by the ISO families 27000¹⁷ and 28000¹⁸, as already described in CYRENE Report 1 [12].

ISO 28000 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. (For further details, see CYRENE Report 1).

In particular, ISO 28003¹⁹ encompasses the requirements from ISO/IEC 17021²⁰, Conformity assessment — Requirements for bodies providing audit and certification of management systems. When assessing security supply chain security management systems, a number of requirements need to be met which go beyond what is required for the assessment and certification of supply chain security management systems covering other operational aspects of organizations. To formulate these additional requirements, ISO/IEC 17021 has been amended or modified where needed. This International Standard:

¹⁷ <https://www.iso.org/standard/73906.htm>

¹⁸ <https://www.iso.org/standard/44641.htm> |

¹⁹ <https://www.iso.org/standard/45416.html>

²⁰ <https://www.iso.org/obp/ui/#iso:std:iso-iec:17021:-1:ed-1:v1:en>

- provides harmonized guidance for the accreditation of certification bodies applying for ISO 28000 (or other specified supply chain security management system requirements) certification/registration;
- defines the rules applicable for the audit and certification of a supply chain security management system complying with the supply chain security management system standard's requirements (or other sets of specified supply chain security management system requirements);
- provides the customers with the necessary information and confidence about the way certification of their suppliers has been granted.

ISO 27000, also known as the ISMS family of standards, allows organizations to develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

The ISMS family of standards includes standards that:

- define requirements for an ISMS and for those certifying such systems;
- provide direct support, detailed guidance, and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS;
- address sector-specific guidelines for ISMS; and
- address conformity assessment for ISMS.

In particular, ISO 27006 "Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems" ²¹ outlines requirements and provides guidance for bodies providing audit and certification of an ISMS, in addition to the requirements set by ISO 17021-1 "Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements"²² and ISO 27001 "Information technology - Security Techniques - Information security management systems — Requirements"²³.

It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides an additional interpretation of these requirements for any body providing ISMS certification.

3.1.3 *Building Blocks of the CYRENE RCA Methodology*

The CYRENE RCA Methodology is built following the lines of the Cybersecurity Certification Scheme that have been proposed for SCS (EUSCS) in CYRENE Report 2 [2]. The EUSCS is based on the EUCC scheme [11], the common criteria-based European candidate cybersecurity

²¹ <https://www.iso.org/standard/62313.html>

²² <https://www.iso.org/standard/61651.html>

²³ <https://www.iso.org/isoiec-27001-information-security.html>

certification scheme, which has been created as a successor to the existing SOG-IS, and is also mainly based on the EUCS proposed cybersecurity certification scheme for cloud services.

In addition, for the creation of the CYRENE Methodology, other existing methods and approaches have been also used, such as the ETSI-TVRA methodology, which orients security objectives, both to assets and their environment, and the Common Vulnerability Scoring System (CVSS), which helps to assess the severity of computer system security vulnerabilities. In addition, CYRENE RCA methodology is enhancing the MITIGATE (Multidimensional, integrated, risk assessment framework and dynamic, collaborative Risk Management tools for critical information infrastructure) methodology [4],[5],[6].

MITIGATE provided an SCS risk assessment methodology that was based on ISO2700x and ISO28000, wherein CYRENE is also compliant with ISO15408.

CYRENE methodology has dual use: it can be used by the SCS-provider (with collaboration and consent of the SCS-BPs) to conduct a risk assessment, develop the SCS-ISMS and the SCS-protection profile (SCS-PP); it can also be used by the assessor to assess the claims in the SCS-PP.

3.2 CYRENE ontology for enhanced Risk and Conformity Assessment

The word ontology is derived from two Greek words: Onto -which means being - and Logia - which means discourse in the form of written or spoken. This section provides information about designing and implementing an ontology called “OntoCyrene” for the CYRENE project.

3.2.1 *Related works*

This section does not aim to provide a detailed discussion of all the literature related to ontologies but rather to outline some works that are very close to the CYRENE ontology.

Annane et al **Error! Reference source not found.** introduced an ontology named BBO based on pre-existing ontologies and the BPMN 2.0 meta-model. The ontology was implemented using protege software in the context of industry v4.0. The building blocks of the ontology were chosen and implemented based on the BPMN 2.0 elements including flow elements, activities, gateways events, etc. all these concepts were designed in the form of classes and subclasses in the ontology. The proposed ontology was populated using a real-world example and the results indicated that this ontology is able to represent the dynamic aspects of the example and returns correct results based on the designed queries. In order to evaluate the ontology, the authors used competency questions as an evaluation method. As a result, SPARQL queries derived from competency questions were designed to check the quality of answers. The results showed that the ontology has enough richness and quality.

In another contribution, Annane et al., **Error! Reference source not found.** compared the nine most cited business process ontologies in the literature. The motivation behind this work is to

compare BPMN-based ontologies with non-BPMN-based ontologies in representing business process specification and execution. Studied ontologies were divided into two categories: Ontologies developed from scratch and ontologies implemented based on BPMN 2.0. The benchmark for this comparative study were process specification and process execution attributes. The result of the study indicates that BPMN-based ontology have better representation capabilities in comparison with the non-BPMN-based ontologies.

Diego et al. **Error! Reference source not found.** designed a quadrable multistage semantic representation of BPMN models in order to enhance the mechanization of business process management. The proposed method saved the response time of the queries against the ontology. The building blocks of the proposed model have three levels: metamodel, business process model, and finally an assertional layer. The proposed representation model was evaluated using real-world case studies and the results indicated the ontology is able to return the result of the queries in an acceptable time frame.

Sanfilipo et al. **Error! Reference source not found.** conducted ontology-based analysis on two of BPMN main elements including event and activity. The results showed that activities are neither homeomeric nor cumulative, neither atomic nor anti-atomic but events (throw and catch events) are atomic and anti-cumulative.

Adamo et al. **Error! Reference source not found.** presented an ontology-based analysis of business processes modeling notations among four modeling languages/standards including BPMN, UML-AD, EPC, and CMMN. The evaluation criteria are classified into 3 categories namely behavioral, data, and organization. The findings of this study show that if BPMN is able to support this property that if two processes have had different participants, they must be separate processes. Likewise, if two or more activities had some shared participants, they may belong to the same process under some circumstances.

Doynikova et al. **Error! Reference source not found.** proposed an ontology to represent a number of metrics for cyber security management. This ontology aggregates primary security metrics with security information. The ontology formed a set of hierarchically interconnected security metrics for assessment and decision-making in the field of cyber security threats. The results showed that the proposed ontology has advantages over other methods in terms of representing the granularity of details, applying an inference engine to check inconsistency in the domain.

3.2.2 *OntoCyrene*

In this section, the OntoCyrene ontology is presented. The rest of this sub-section is organized as follows: in section 3.2.2.1 the architecture of the ontology will be presented. Subsection 3.2.2.2 introduces the designed ontology in terms of a class hierarchy. In section 3.2.2.3 all relationships including object properties and data properties designed for OntoCyrene will be presented.

3.2.2.1 Architecture of OntoCyrene

OntoCyrene is composed of four main sub ontologies namely; Asset, Business, Sector, and Certification. All these components were implemented as superclass/subclass using an object-oriented concept.

The asset component deals with the asset/technical perspective of the ontology. The business part of the ontology deals with a business-driven perspective and contains the concept of the process. Sector sub ontology handles the sector view for asset modeling and the certification component deals with the certification and conformity assessment in the Cyrene project. Figure 8 demonstrates these components.

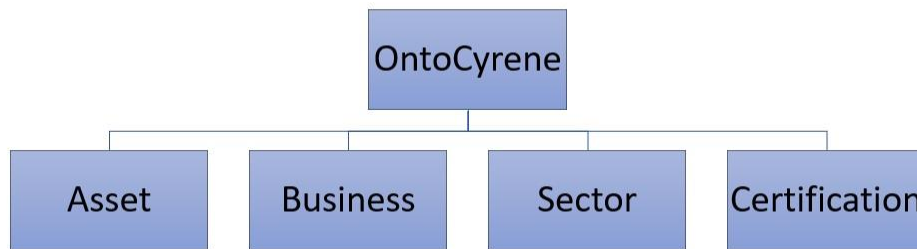


Figure 8 – Main sub ontologies in OntoCyrene.

3.2.2.2 OntoCyrene Class Hierarchy

In order to implement the architecture depicted in Figure 9, several superclasses and subclasses need to be designed. Figure 9 shows all superclasses which were designed in OntoCyrene.



Figure 9 – OntoCyrene superclasses in class hierarchy.

For each of three defined perspectives, there is a superclass designed in the ontology with corresponding names (Asset, Business, and Sector). The hierarchy also includes the “Certification” superclass for the conformity assessment part of the Cyrene project. Moreover, all security-related concepts like weakness, vulnerability, and attack were classified under the “Security” superclass. “Agent” superclass was designed for all active participants in the ontology

including humans and software. “Role” superclass includes all subclasses related to various roles that can be taken by humans, machines, and software.

Part of these superclasses contains subclasses. Figure 10 shows all sub-classes designed for the Business perspective.

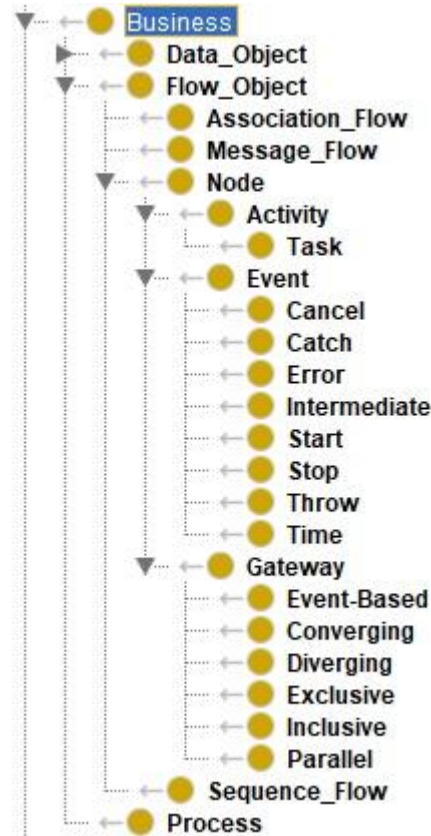


Figure 10 – Subclasses designed for modeling Business-driven perspective.

As depicted in Figure 10, main BPMN elements are modeled in ontology in the form of class/subclass. This includes data object, flow object, connecting object, and the process itself. All these elements are discussed in 3.2.2.1. In order to design these BPMN elements the following rules/restrictions were defined and implemented in OntoCyrene ontology:

N°	The specification in natural language	Formalized Specification
1	A Gateway MUST have either multiple <i>incoming</i> Sequence Flows or multiple <i>outgoing</i> Sequence Flows (i.e., it MUST merge or split the flow).	Gateway SubClassOf (has_incoming min 2 SequenceFlow) or (has_outgoing min 2 SequenceFlow)
2	A Gateway with a gatewayDirection of converging	ConvergingGateway equivalentTo Gateway and (has_incoming min 2 SequenceFlow)

	MUST have multiple <i>incoming Sequence Flows</i> , but MUST NOT have multiple <i>outgoing Sequence Flows</i> .	and (has_outgoing exactly 1 SequenceFlow)
3	A Gateway with a gatewayDirection of diverging MUST have multiple <i>outgoing Sequence Flows</i> , but MUST NOT have multiple <i>incoming Sequence Flows</i> .	DivergingGateway equivalentTo Gateway and (has_outgoing min 2 SequenceFlow) and (has_incoming exactly 1 SequenceFlow)
4	An Event Gateway MUST have two or more <i>outgoing Sequence Flows</i> .	EventBasedGateway SubClassOf (has_outgoing min 2 SequenceFlow)
5	The <i>outgoing Sequence Flows</i> of the Event Gateway MUST NOT have a conditionExpression.	EventBasedGateway SubClassOf not (has_outgoing some ConditionalSequenceFlow)
6	The Start Event starts the flow of the Process , and thus, will not have any <i>incoming Sequence Flows</i>	StartEvent SubClassOf not (has_incoming some SequenceFlow)
7	The Start Event should have at least one <i>outgoing Sequence Flow</i>	StartEvent SubClassOf (has_outgoing some SequenceFlow)
8	An Event Sub-Process MUST have one and only one Start Event .	EventBasedSubProcess SubClassOf (has_flowElements exactly 1 StartEventForEventBasedSubProcess)
9	An Event Sub-Process MUST NOT have any <i>incoming</i> or <i>outgoing Sequence Flows</i> .	EventBasedSubProcess SubClassOf not ((has_incoming some SequenceFlow) or (has_outgoing some SequenceFlow))
10	the End Event ends the flow of the Process , and thus, will not have any <i>outgoing Sequence Flows</i> .	EndEvent SubClassOf not (has_outgoing some SequenceFlow)
11	An End Event MUST be a target for a Sequence Flow . An End Event may have multiple <i>incoming Sequence Flows</i> .	EndEvent SubClassOf (has_incoming some SequenceFlow)
12	A source Gateway MUST NOT be of type Parallel or Event	SequenceFlow SubClassOf not ((has_conditionExpression some Expression) and (has_sourceRef some (ParallelGateway or EventBasedGateway)))
13	A Timer Event is an Event that has exactly one TimerEventDefinition .	TimerEvent EquivalentTo (Event and (has_eventDefinition exactly 1 TimerEventDefinition))
14	An Intermediate Event MUST be a	<ul style="list-style-type: none"> IntermediateEvent EquivalentTo

	source for a Sequence Flow .	(IntermediateCatchEvent IntermediateThrowEvent) or • IntermediateEvent SubClassOf (has_outgoing some SequenceFlow)
--	-------------------------------------	--

Table 8 – List of OWL axioms from natural language specifications.

The asset perspective has a number of subclasses including Hardware, Human (subclasses: individual and group), and Software. Asset in terms of hardware is considered as any machine which is assigned by an IP address and a role. As an example, a network-connected machine may be assigned a “client” role. Human and software may also accept a role (or a number of roles) in different supply chain scenarios. Thus, ontology has a superclass called “Role”. Figure 11 shows the class hierarchy for superclass “Role”. Defined roles in this ontology are just examples and need to be extended based on the SCS scenario.

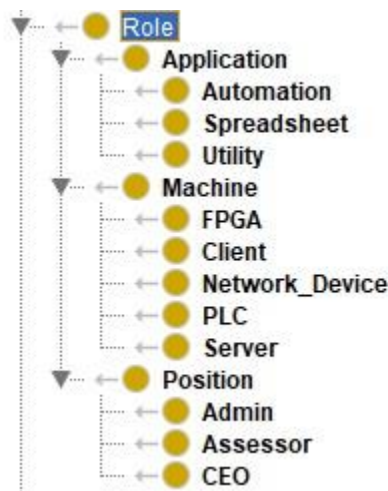


Figure 11 –Roles modeled in OntoCyrene

Another main sub ontology is related to Sector driven perspective (Figure 12). According to the definition of this perspective mentioned in 1.3, in this view, a Supply Chain Service Provider (SCSP) is analyzed/modeled from different aspects including its partners, its internal and external linkage, and also by its sub-sectors. Thus, for each of these aspects, a corresponding class and properties were designed and modeled in OntoCyrene.



Figure 12 – Sector-driven perspective modeled in the Ontology.

The last component discussed here is “Security”. In OntoCyrene, assets are assigned by a number of security-related values like CVSS score, Criticality Score, CVE_ID, CWE_ID, etc. These metrics are related to a threat, vulnerability, weakness, attack, and risk in the context of cyber security. Therefore, the Security superclass and all its object and data properties (discussed in 4.3) reflect corresponding blocks of these metrics. Figure 13 depicts the Security sub ontology.



Figure 13 – Security aspects of OntoCyrene in terms of super/sub classes.

3.2.2.3 OntoCyrene Object and Data Properties (Relationships)

In this subsection, all defined relationships (properties) will be discussed. In order to increase the readability of these documents, all properties are grouped based on the defined perspectives (Asset, Business, and Sector).

Asset Driven Properties.

Table 9 summarizes all asset-driven object relationships in the ontology.

	Domain (Class)	Object Property (Relationship)	Range (Class)
1	Individual	belongs	Group
2	Group	groups	Individual
3	Group	has_leader	Individual
4	Individual	is_leaderOf	Group
5	Asset	has_role	Role
6	Hardware	has_role	Machine
7	Software	has_role	App
8	Individual	has_role	Position
9	Asset	has_vulnerability	Vulnerability
10	Asset	has_weakness	Weakness
11	Software	is_accessing	Software Hardware
12	Human	is_relatedTo	Process
13	Hardware	is_assignedTo	Process
14	Hardware	is_connectingTo	Hardware Software
15	Hardware Software	is_controlling	Hardware Software
16	Software	is_hostedBy	Hardware

17	Software	is_installedOn	Hardware
18	Software	is_processing	Software
19	Software	is_storedAt	Hardware
20	Hardware Software	is_trustedBy	Human

Table 9 – Object properties defined and modelled for asset driven perspective.

Business Driven Properties.

Table 10 summarizes all object properties related to the business-driven perspective in the ontology.

	Domain (Class)	Object Property (Relationship)	Range (Class)
1	Node	has_container	Business
2	Sequence_Flow	has_inclusiveGateway	Inclusive
3	Sequence_Flow	has_exclusiveGateway	Exclusive
4	Business	has_flowObject	Node
5	Node	has_incoming	Sequence_Flow
6	Activity	has_input	Input
7	Activity	has_output	Output
8	Node	has_outgoing	Sequence_Flow
9	Process	has_part	Activity Event Gateway
10	Node	has_sequenceFlow	Sequence_Flow
11	Sequence_Flow	has_source	Node
12	Sequence_Flow	has_target	Node
13	Activity Event Gateway	is_partOf	Process
14	Process Activity Event Gateway	is_precededBy	Process Activity Event Gateway
15	Process Activity Event Gateway	is_succeededBy	Process Activity Event Gateway

Table 10 - Object properties defined and modeled for the business-driven perspective.

Sector Driven Properties.

Table 11 summarizes all object properties related to the sector-driven perspective in OntoCyrene.

	Domain (Class)	Object Property (Relationship)	Range (Class)
1	SCSP	has_partnershipWith	Partners
2	SCSP	has_department	Departments
3	SCSP	has_linkage	Internal
4	SCSP	has_linkage	External
5	SCSP	runs_process	Process

Table 11 – Object properties defined and modeled for the sector-driven perspective.

Security Related Properties.

In addition to the above-mentioned relationship, a number of object properties were defined and modeled to reflect the relationship among threat, vulnerability, weakness, and attack. Table 12 summarizes these properties.

	Domain (Class)	Object Property (Relationship)	Range (Class)
1	Asset	has_vulnerability	Vulnerability
2	Asset	has_weakness	Weakness
3	Vulnerability	is_exploitedBy	Attack
4	Weakness	is_targetedBy	Vulnerability
5	Vulnerability	targets	Weakness

Table 12 – Object properties defined and modelled for security related concepts.

Data Properties.

A number of data properties have been defined for OntoCyrene. Figure 14 shows these properties.

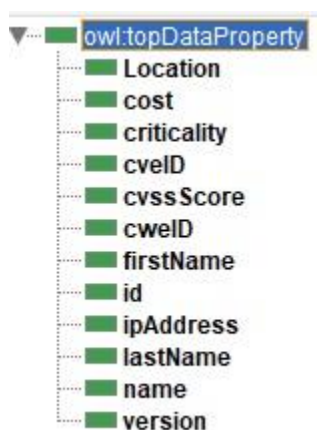


Figure 14 – OntoCyrene data properties.

For the asset-driven perspective, the following data properties are defined: Location of the asset, asset ID, CVE ID and CWE ID related to the asset, CVSS score related to the asset, a value of criticality assigned to the asset, the cost of the asset, etc. Moreover, the first name and last name of individuals are kept through these properties. For hardware, name, id, and IP address are recorded according to the defined properties. For software, ID, version, and name can be stored in the ontology. For a business perspective, all BPMN elements involved in the ontology may have ID and name. For sector-specific view, name, ID, and location can be recorded in the ontology.

Connecting Points of Three Perspectives.

By considering all relationships defined for an asset, business, and sector perspectives, Figure 15 depicts the connecting points of these perspectives in the ontology.

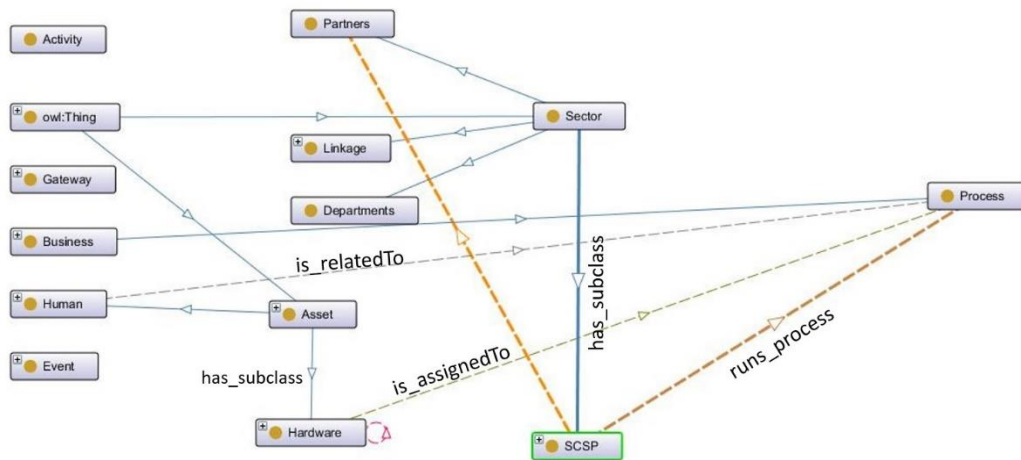


Figure 15 – Connecting points of the three perspectives.

As shown in the picture, asset-driven perspective has two explicit relationships with business-driven perspective through hardware and human. In other words, by asserting i) Human “is_relatedTo” the process and ii) Hardware “is_assignedTo” the process both business and asset driven perspectives are joined to each other. Furthermore, the sector view is connected to the business view via supply chain service provider (SCS-P). Each process is owned and run by “SCSP” so by asserting the following properties sector-driven perspective is connected to the business-driven perspective: “SCSP runs_process the process”.

3.2.3 Ontology Population and Validation

OntoCyrene ontology was populated using a real-world scenario in the field of vehicle transport supply chain. This scenario consists of a process called “Port Call Request”.

This process was implemented using Protégé software and validated by CRF. The rest of this section explains the process and the instantiation phase of this process for three different perspectives including Sector, Asset and Business.

3.2.3.1 Description of “Port Call Request” 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.

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. authorised

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, tugboats, and mooring), and other relevant data.

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.

The port calls information is used by Port Authority and the Terminal Operators to manage their resources accordingly preparing equipment, personnel, etc. These communications are done using the Port Community System (PCS).

3.2.3.2 Ontology Population: Sector Perspective

As mentioned earlier, the populated example is in the field of the Vehicles Transport supply chain service. It concerns the vehicles import processes engaging the shipment and receipt of various types of vehicles and equipment such as trucks, vans, truck trailers, gantry cranes etc. Three aspects have been populated as sector view in the ontology for this example: SCSP (names and specs), its departments and partners.

As discussed, the name of the supply chain service provider in this example is Vehicle Transport System.

The name and ID of the SCSP were specified using the corresponding data objects in the ontology.

The supply chain service provider has the following departments: Digital Transformation, Exploitation and Port Community System.

The following relationship has been used to populate the ontology with these departments:

Individual	Relationship	Individual
------------	--------------	------------

SCSP	has_department	Digital Transformation Exploitation Port Community System
------	----------------	---

Table 13 – Object properties used to implement departments of the SCS-P.

The main stakeholders/partners of this supply chain service provider are as follows:

- Port Authority
- Ship Owner
- Customs
- Terminal Agent

Figure 16 shows the populated instances for the partner class.



Figure 16 – Instances for partners of the SCS-P in the example.

In order to populate the ontology, a number of relationships (Object Properties) were used. Table 14 shows them.

Instance	Relationship	Instance
SCSP	has_partnershipWith	Customs Port Authority Ship_Owner Terminal Agent

Table 14 – Object properties used to implement partners of the SCS-P.

Figure 17 shows the main elements (instances and relationships) developed for the sector view based on the given example.

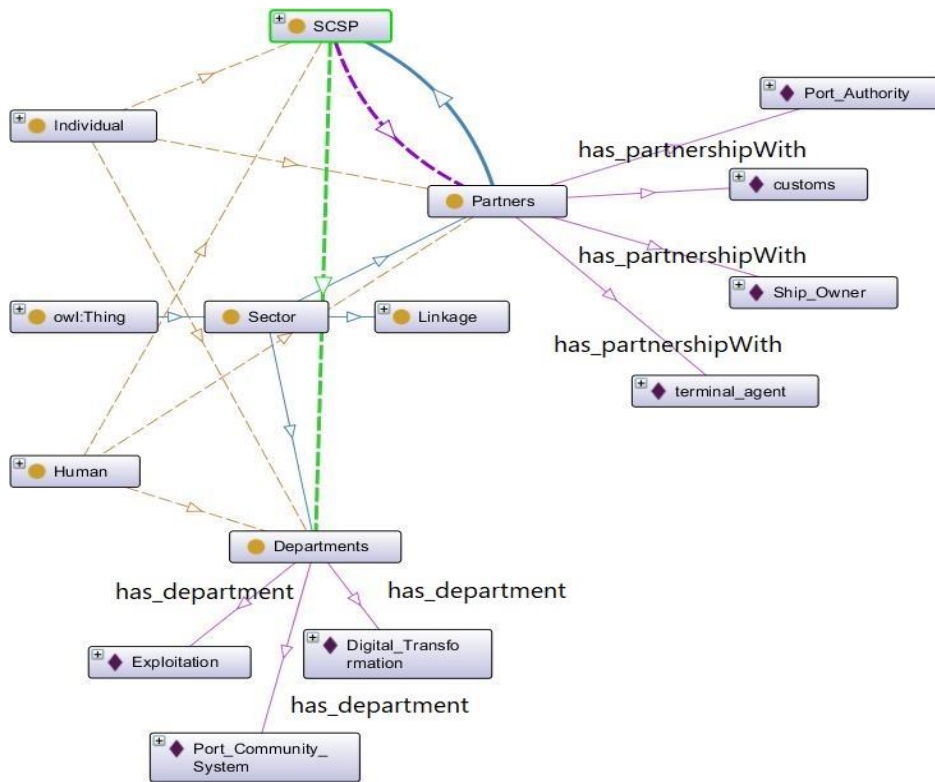


Figure 17 – Sector view instantiation.

3.2.3.3 Ontology Population: Business perspective

The process discussed in 5.1 was designed and implemented using BPMN. Figure 18 demonstrates this process with BPMN symbols and semantic.

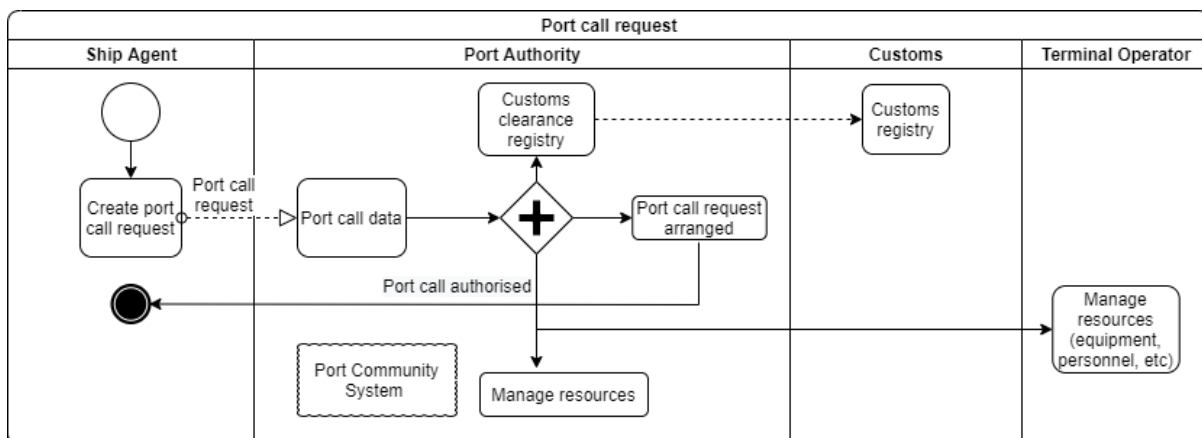


Figure 18 – BPMN diagram of “Port Call Request” process.

The diagram includes a number of activities and a parallel gateway with start/stop events to depict the procedure of the “Port Call Request”. In order to implement this scheme, an encoded layout of this diagram was designed. Figure 19 shows the encoded diagram of this process.

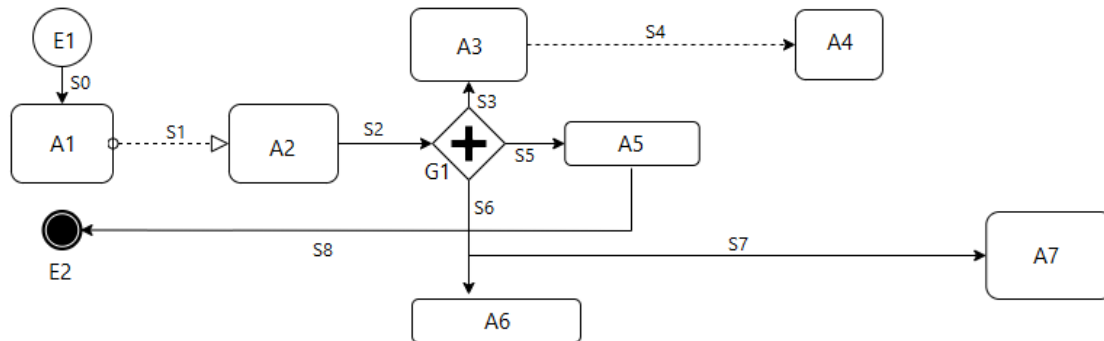


Figure 19 – Encoded BPMN diagram of “Port Call Request” process.

As shown in Figure 19, the label of all activities starts with “A”. Moreover, the tags of the sequence/message flows start with “S” and the only gateway of the process is tagged using “G”. start and stop events in this process starts with “E”.

In order to implement this scheme, all of the encoded building blocks in Figure 19 were populated. For activities, A1...A7 were defined and implemented as instances of Activity class. S0, S2, S3, S5, S6, S7 and S8 were implemented as instances for sequence flow class. Moreover, S1 and S4 were populated as instances of the class “message flow”. The only gateway of this process was created as an instance of the “parallel gateway” class. All these entities were joined to the “Port Call Request” process (P1) using the following assertion: “is_partOf”. As an example: (A1, is_partOf, P1). Furthermore, for all mentioned entities, another relationship was asserted in the ontology to connect them to the “Port Call” process which is: “has_part”. As an example: (P1, has_part , A1)

After defining and implementing all building blocks of the scheme depicted in Figure 19, different types of relationships among them were defined and implemented. Table 15 gives details on relationships defined for activities inside the process.

Instance	Relationship	Instance
A1	is_precededBy	E1
A1	is_succeededBy	A2
A1	has_incoming	S0
A1	has_outgoing	S1
A2	is_precededBy	A1
A2	is_succeededBy	G1

A2	has_incoming	S1
A2	has_outgoing	S2
A2	is_proceededBy	A1
A2	is_succeededBy	G1
A2	has_incoming	S1
A2	has_outgoing	S2
A3	is_proceededBy	G1
A3	is_succeededBy	A4
A3	has_incoming	S3
A3	has_outgoing	S4
A4	is_proceededBy	A3
A4	has_incoming	S4
A5	is_proceededBy	G1
A5	is_succeededBy	E2
A5	has_incoming	S5
A5	has_outgoing	S8
A6	is_proceededBy	G1
A6	has_incoming	S6
A7	is_proceededBy	G1
A7	has_incoming	S7

Table 15 – Object properties used to implement activity instance.

For connecting objects (sequence and message flow), the following relationships listed in Table 16 have been defined and asserted in the ontology.

Instance	Relationship	Instance
S0	has_source	E1
S0	has_target	A1
S1	has_source	A1
S1	has_target	A2
S2	has_source	A2
S2	has_target	G1
S3	has_source	G1
S3	has_target	A3
S4	has_source	A3
S4	has_target	A4
S5	has_source	G1
S5	has_target	A5

S6	has_source	G1
S6	has_target	A6
S7	has_source	G1
S7	has_target	A7
S8	has_source	A5
S8	has_target	E2

Table 16 – Object properties used to implement connecting objects.

3.2.3.4 Ontology Population: Asset perspective

As defined in the ontology, an asset can be human, hardware and software. According to the analysis of the “Port Call Request” process, four individuals are involved in the process including *ship agent operator*, *port authority operator*, *customs operator*, and *terminal operator*. Furthermore, for each of these individuals a number of resources in terms of hardware and software were assigned based on the description of the process. Table 17 lists the details of assigned hardware and software based on the description of P1 process.

Instance	Relationship	Instance (HW/SW)
ship_agent_operator	has_accessTo	PCS
ship_agent_operator	has_accessTo	Office365
ship_agent_operator	has_accessTo	MS_Edge
ship_agent_operator	has_accessTo	AVG_av
ship_agent_operator	has_accessTo	Lap_Lenovo_C930
ship_agent_operator	has_accessTo	Windows_10_x64
port_authority_operator	has_accessTo	Exchange_Server
port_authority_operator	has_accessTo	FTP_Server
port_authority_operator	has_accessTo	SMTP_Server
port_authority_operator	has_accessTo	SQL_Server_2019
port_authority_operator	has_accessTo	Windows_Server_2019
port_authority_operator	has_accessTo	PCS
port_authority_operator	has_accessTo	HP_DL850
port_authority_operator	has_accessTo	IIS10
port_authority_operator	has_accessTo	Router_SLX_9640
customs_operator	has_accessTo	PCS
customs_operator	has_accessTo	Office365
customs_operator	has_accessTo	Windows_Server_2019
customs_operator	has_accessTo	Dell_PE_R740
customs_operator	has_accessTo	Kaspersky_av
terminal_operator	has_accessTo	PCS
terminal_operator	has_accessTo	Chrome
terminal_operator	has_accessTo	Office365
terminal_operator	has_accessTo	Lap_HP_G6

terminal_operator	has_accessTo	Windows_10_x64
terminal_operator	has_accessTo	Norton_av

Table 17 – List of asset-driven instances and relationships implemented for P1n the example.

The relationships among hardware and software are asserted using the following object property: “is_installedOn”. For example: (Kaspersky_av, is_installedOn, Dell_PE_R740).

3.2.3.5 Ontology Population: Connecting three perspectives.

In order to connect asset perspective to business perspective the following relationships were extracted out and asserted in the ontology. Table 18 presents these entities and relationships

Instance Asset View	Relationship	Instance (Business/Sector) view
ship_agent_operator	is_relatedTo	(Business View) A1 P1 E1 E2 S0 S1
ship_agent_operator	belongs	(Sector View) Ship_Owner
port_authority_operator	is_relatedTo	(Business View) A2 A3 A5 A6 G1 S2 S3 S5 S6 S7 P1
port_authority_operator	belongs	(Sector View) Port_Authority
customs_operator	is_relatedTo	(Business View) P1 A4
customs_operator	belongs	Customs
terminal_operator	is_relatedTo	(Business View)

		P1 A7
terminal_operator	belongs	Port_Authority

Table 18 – Implementing connecting points for three perspectives in the example.

3.2.3.6 Validating the OntoCyrene

In order to validate the ontology, we ran a number of queries against ontology and the results were analysed by the SCSP to investigate how OntoCyrene works in action. In the rest of this chapter, some of the results are presented.

The first example is from business perspective. Figure 20 shows the result of the query that was implemented against the ontology to search for A6.

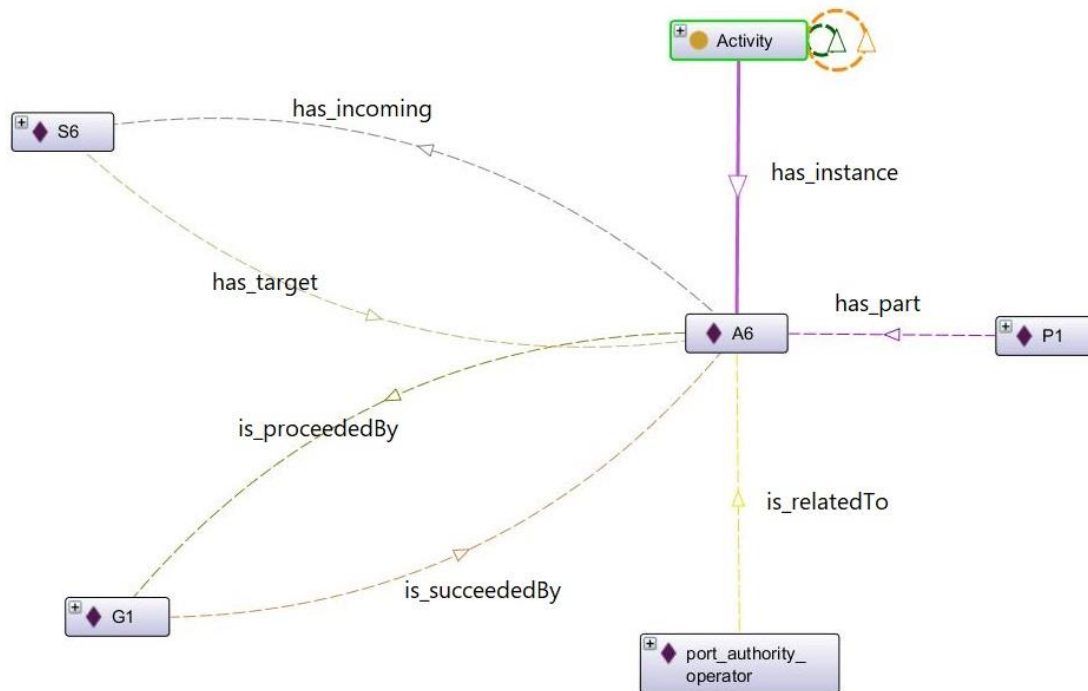


Figure 20 – All relationships for A6 in the ontology.

As shown in the above figure, the result is in the form of a graph in which vertices are the entities from business and sector perspective which are related to A6. Edges are different types of relationship between these building blocks.

Another example is shown in Figure 21. In this example, an entity from sector perspective (Ship_Owner) has been queried against ontology. The result indicated that the ontology is rich enough to show the model of the entities from different perspectives and their dependencies for the queried object.

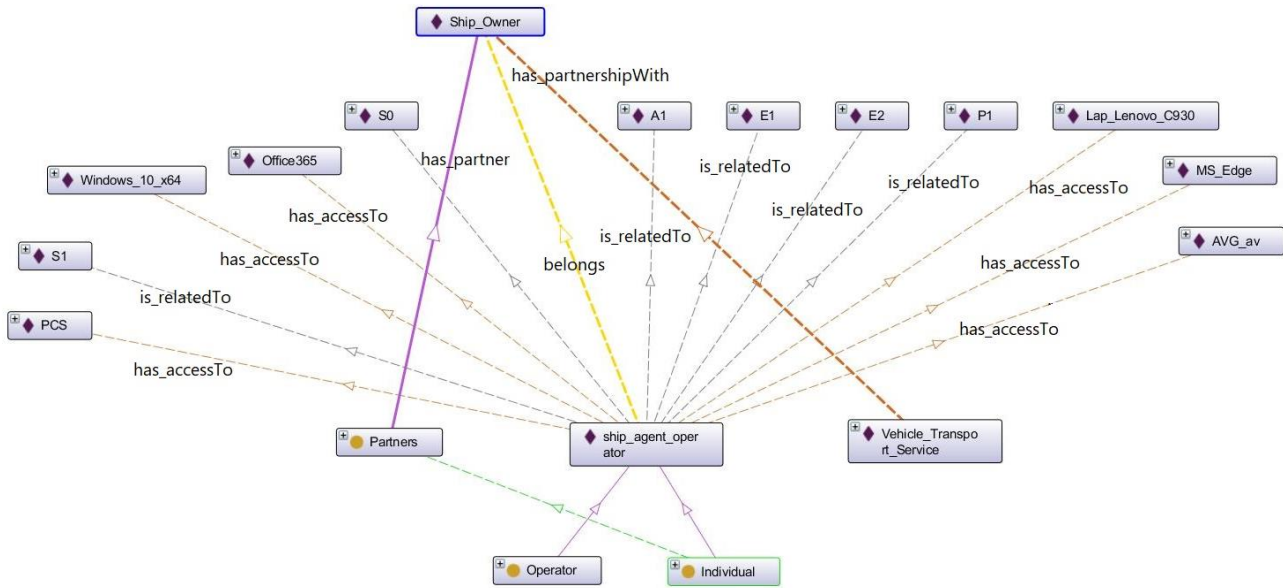


Figure 21 – All relationships for Ship_Owner in the ontology.

The last query example is from asset perspective. HP_DL850 which is a hardware involved in the process was queried against the ontology. The result shows all dependent entities and their types of relationship. Figure 22 demonstrates the result of this query in the form of a graph.

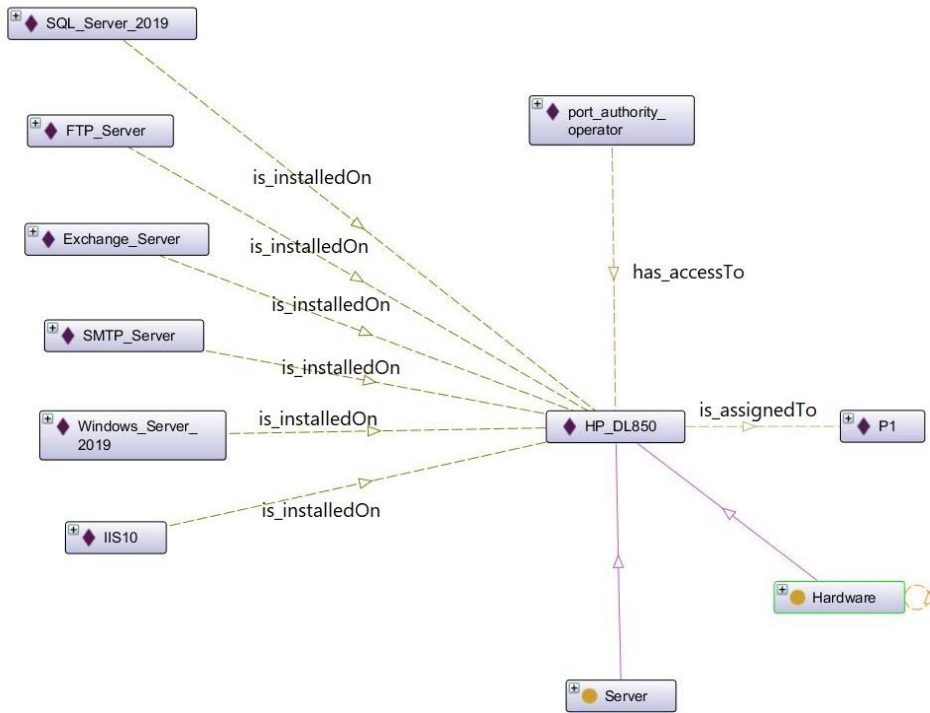


Figure 22 – All relationships for HP_DL850 in the ontology.

The results of the queries confirmed that the populated scenario (Port Call Request) was modelled correctly. Furthermore, the granularity of details reflected in the results revealed that the OntoCyrene has enough rich to show the asset model and its dependencies.

3.3 Use of the Methodology

CYRENE methodology can be used by the SCS-P and SCS-BPs, as well as by any third-party assessor. As presented in section 2.1 and section 3.1.3, the CYRENE RCA methodology has a twofold purpose of use (to perform either an enhanced risk assessment or a conformity assessment process). This dual use of the methodology can be beneficial to a majority of SCS entities, such as SCS-BPs, ICT/Security experts, sector-specific parties, and SCS-assessors. The following sections present how the use of the methodology can leverage these parties.

3.3.1 *SCS Business Partners*

During the Supply Chain Services (SCS) performance several actors may be involved, undertaking numerous processes and operating miscellaneous systems, especially when the provision of the service engages stakeholders coming from multiple industry sectors, such as in SCS related to port and transportation domain.

For instance, the Vehicle Transport Service (described in CYRENE Report 1), is supported by multiple actors, where some representative business partners are considered the automotive importer, ship agent, port authority, customs, terminal operator, freight forwarder, hauler company, etc. All these companies involved need to exchange several documentation and data during the physical transportation of the vehicles through different channels, digital platforms, email, etc. Therefore, they are supported by heterogeneous interconnected ICT infrastructures and cyber networks.

To protect their own infrastructures these companies should have the proper tools and protocols. Nonetheless, that's not enough. In order to guarantee security in the entire Supply Chain, it is necessary a security methodology that is focused on cybersecurity assessments on supply chain environments addressing business partners' security requirements in terms of the provision and normal operation of the entire supply chain service they are involved.

CYRENE RCA methodology aims to support this, facilitating SCS enterprises to self-assess their SCS processes, assets, and systems, harmonize their security efforts following a common scheme (i.e: the EUSCS proposed in CYRENE Report 1) that will allow them to cover security certification requirements, whereas reaching a security certification guarantee will raise their level of security and their confidence and resilience within the digital EU market.

3.3.2 *ICT / Security Experts*

Usually, the ICT / Security Experts of a company/organization are the ones who know their ICT systems, networks, and interdependencies better. They have awareness of SCS ICT assets concerning their technical specificities and security particularities. Their role also includes the responsibility of keeping everything up and running securely and testing specific systems when needed.

The ICT / Security Experts can use the CYRENE RCA methodology as a guide either to implement a risk assessment on ICT infrastructures or self-assess the ICT-related security claims of a developed protection profile and thereby facilitate SCS-BPs to better support the security certification requirements.

3.3.3 *Sector Specific Parties*

Following CYRENE Report 2, it should be noted that the proposed CYRENE EUSCS scheme facilitates the implementation of the Service Level Agreements (SLAs) that should be signed among the involved SCS-BP in order to ensure that the security controls and recommendations derived from the certification process are properly orchestrated and executed across the SCS. In the same way, CYRENE RCA methodology considers contextual information for specific horizontal sectors and can be applied in two ways in order to certify two different types of SCS – it can either be:

- Horizontally applicable across various sectors for ensuring the security and resilience of SCS, or
- Sector-specific applicable, i.e., vertically along with sectors, for ensuring the security and resilience of SCS (e.g., automobile industry, maritime, transportation).

3.3.4 *SCS Assessors*

The CYRENE RCA methodology is also developed for assessors (either self-assessors or CABs) to follow specific guidelines in a step-by-step format in order to evaluate the conformance of the claims included in the SCS-PP to issue an SCS-certificate according to each of the above mentioned for SCS stakeholders as well as to the SCS as a whole.

4 Supply Chain Service (SCS) as Target of Evaluation (TOE)

In this chapter, the Supply Chain Service (SCS) is viewed as Target of Evaluation (TOE) that can be subject to the CYRENE RCA methodology and is decomposed into its generic elements.

4.1 SCS at a glance

Supply chain service (SCS) is a complex system of organizations, people, technology, activities, information that creates an interdependent set of resources and processes (nodes) triggered by the sourcing of raw material and extended to fulfill the delivery of products or services to the end-customer by transport [20],[21].

According to ISO 28001²⁴ international standard of supply chain security management, the security assessment (that can lead to certification) of the SCS requires its decomposition to its generic elements: business processes, business partners, and SCS assets (physical, cyber, and people) engaged in the provision of the SCS. SCS processes are executed by various business partners who utilize a number of assets to operate their tasks and accomplish their business goals for the provision of the SCS. Such business partners can be vendors, manufacturing entities, logistics providers, internal distribution centers, distributors, wholesalers, authorities, and other entities) ending up with the end-user.

With regards to CYRENE Report 2, for establishing the Cybersecurity Certification proposed Scheme for SCS (EUCC), SCS business partners (SCS-BPs) are distinct into four main categories (also defined in the Glossary of section 8 of the current document): SCS Provider (SCS-P) (Business Partner A), SCS Commercial Business Partner (Business Partner B) and Governmental Business Partner (Business Partner C) and SCS Self-Assessor (Business Partner D). Within this framework, the SCS provider is the entity, that seeks assessment for an SCS, in order to receive security certification for the SCS.

As presented in the proposed EUSCS of CYRENE Report 2 [2] and in CYRENE Report 1 [12], an SCS can be classified, viewed and security evaluated in the following different perspectives (SCS evaluation views see also the Glossary in section 8):

- the **overall business view** (which scrutinizes the business aspect of the SCS): relies on the identification, analysis, and assessment of any business-driven SCS element that has a direct input for the provision of the SCS. As such, in this view, details of processes, business partners (i.e. suppliers, stakeholders, importers, vendors,

²⁴ ISO 28001:2007 international standard, "Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance", 1st Edition 2007-09. Online available: <https://www.iso.org/standard/45654.html>, accessed on April 20 2021.

manufacturers, authorities, governmental bodies) and their third parties, facilities, related business logic (e.g., data and information flows, decision making), and any legal/regulatory restrictions are considered. The components of the under evaluation SCS 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 SCS-TOE.

- the **holistic-technical view** (which embed the previous business aspect along with an asset-based interdependent view and all the activities undertaken for the provisions of the SCS). It builds upon the previous view, i.e., it embeds all business processes, business partners, and all cyber and physical assets hosted by the different business partners for the provision of the SCS processes. SCS asset models revealing asset-interdependencies accompany the presentation of the SCS under this view. The components 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.
- the **sector-specific technical view** (the individual snap-shot an SCS-BP adopts to analyze the SCS):
it is considered under the scope of a single SCS-BP's involved in the SCS. The components under evaluation are the SCS processes and SCS assets that one of the business partners host and operates in order to participate in the entire SCS.

4.2 SCS Scheme Elements

In order for the evaluation to be conducted, a few preliminary steps shall be taken, including the provision of a few documents to the assessor.

First, an analytical description of the TOE (see Glossary in section 8) shall be provided, which will include a clear definition of the perimeter of the SCS, its services, processes, and assets, depending on the SCS view – TOE mentioned in the previous section.

Second, a Protection Profile of the SCS (SCS-PP) (see Glossary in section 8) shall be created, in which the ToE overview and Conformance Claims (see Glossary in section 8) will be described, the security problem and the extended components will be defined and the security objectives and requirements will be clarified.

Third, an SCS Security Declaration and Application Statement (SDA) shall be created and signed by all business partners (BP), as described in the CYRENE Report 2, along with all the documents that may exist and accompany the SDA, such as certificates.

Templates of the SCS SDA and SCS-PP are proposed in Appendices A and B respectively.

4.3 SCS Security Declaration and Application Statement (SDA)

Every SCS is (or should be) accompanied by a Service Level Agreement (SLA) or a Statement of Application (describing the portion of the global supply chain that it claims to be in compliance with ISO 28001:2007) between all business partners involved in the SCS.

The SCS provider that seeks assessment to evaluate the conformity of an SCS, with respect to the proposed EUSCS, needs to agree with the business partners involved in the under examination SCS upon the specificities that are followed to describe the SCS-TOE (i.e security-relevant sites explicitly required by a Protection Profile (PP), the Risk and Conformity Assessment (RCA) performance and the cybersecurity certification schema that will be adopted. Such agreement is called a Supply Chain Service (SCS) Security Declaration and Application Statement (SCS SDA).

The SCS SDA contains information, such as the business partners that participate, declare who is designated as the SCS provider, the conditions for the recognition of certificates, the conditions to provide a consistent application of the criteria and methods between evaluation and certification schemes, the assurance level that will drive the conformity assessment process and whether any limitations exist concerning the assurance level of the certificates subject to recognition and what they have agreed upon the selection for an external assessor to conduct the CA process (in case RCA is used to conduct a conformity assessment upon certification request).

In addition, the SCS SDA incorporates the security information and documentation (addressing the SCS-TOE) assigning at a high level the security requirements, security objectives, and security problems. Moreover, the SCS SDA must declare that all business partners have agreed upon developing or assessing the Protection Profile (PP) with a reference to the PP and for undertaking the commitment to map the SCS-TOE assets with vulnerabilities and implemented controls, to identify security gaps.

Furthermore, all business partners declare their commitment to undertaking appropriate controls (whether required) in order to reach the SCS desired security level according to what they have agreed. Additional conventions and privacy considerations upon the SCS-TOE and the evaluation process are described as well, which can be referred to or further analyzed in the conformance claim.

As a consequence, SDA in the CYRENE RCA methodology is considered a document signed between the SCS-BPs to declare that every SCS-BP has submitted his organizational security policies in the developed SCS-ISMS along with the SCS-assets that they host and implemented controls documentation (i.e. implementation report, patches, exploits available, penetration testing results, certificates from vendors). In addition, the document includes a statement describing the SCS that it claims to be under examination for security certification and defines the SCS boundaries of application.

5 CYRENE RCA Methodology

This chapter presents the CYRENE RCA methodology. At first, an overview model of the methodology is provided to allow the reader to gain a general idea of the methodology. Then, the CYRENE RCA methodology is explained as an extended security model promoting a hybrid assessment process; the enhanced risk assessment and the conformity assessment process indicating its enhancements upon other adopted approaches. Afterward, the methodology is thoroughly analyzed in every single step.

5.1 Overview Model of the CYRENE RCA Methodology

The CYRENE enhanced Risk and Conformity Assessment methodology is a dual-use evaluation process. At first site, it aims to assess and manage risks and threats providing mitigation strategies and countermeasures policies to facilitate SCS business partners prepare a Protection Profile (PP). On the other hand, it aims to assist assessors to evaluate the claims of a given PP. The RCA methodology is divided into seven super steps. Some of them are further decomposed into sub-steps, in order to better illustrate the process of the step.

Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
<p>Step 0: Scope of the SCS RCA</p>	<p>Step 1: Analysis of the SCS</p> <p>Step 1.1: Scope, objectives, and requirements of the SCS</p> <p>Step 1.2: SCS Business Partners</p> <p>Step 1.3: SCS modeling</p> <p>Step 1.3.1: Identification and description of SCS business processes</p> <p>Step 1.3.2 Identification and description of SCS business partners</p> <p>Step 1.3.3 SCS-TOE's infrastructure description</p> <p>Step 1.3.4 Business process model generation</p> <p>Step 1.3.5 Identification of SCS components criticality and asset model generation</p> <p>Step 1.3.5.1 SCS asset modelling</p> <p>Step 1.3.5.2 Identification of SCS components criticality</p>	<p>Step 2: SCS Threat Analysis</p> <p>Step 2.1: Identification of Threat Scenarios/ Threats</p> <p>Step 2.2: SCS Threat Assessment</p>	<p>Step 3: Vulnerability and Impact Analysis</p> <p>Step 3.1: Estimation of Attack Potential</p> <p>Step 3.2: Vulnerability Severity Estimation</p> <p>Step 3.3: Evidence-based Vulnerability Analysis (VA)</p> <p>Step 3.4: Identification of Confirmed & Zero-Day Vulnerabilities</p> <p>Step 3.5 Building all Vulnerability Chains within the SCS</p> <p>Step 3.6 Identification of Attack Methods & Attack Graphs</p> <p>Step 3.7 Attack Impact</p> <p>Step 3.8 Systematic documentation of vulnerabilities</p> <p>Step 3.8 Occurrence Likelihood & Impact Assessment</p>	<p>Step 4: Risk Assessment- Establishment of Risk</p>	<p>Step 5: Risk Compliance to Security Assurance Certification Scheme</p>	<p>Step 6: Risk Mitigation: Security Countermeasures Identification</p> <p>Step 6.1: Countermeasures in the SCS</p>

Table 19 – The CYRENE RCA methodology.

5.2 CYRENE enhancements

The CYRENE CA methodology is developed on an extended security model providing a hybrid enhanced Risk Assessment and Conformity Assessment process (cf. section 2.3) which has a double use (cf. section 2/section 3); for the SCS–P and SCS-BPs to assess their risks and develop the SCS-PP and for the assessor to check whether the SCS-PP claims are feasible and prepare an audit report and issue the SCS certification whether it fulfills the EUSCS.

The current methodology provides an enhanced risk assessment process, based on the MITIGATE methodology (cf. section 2.2.6), which has been extended regarding:

- Re-calculation of the vulnerability severity following the CVSS 3.1 vulnerability severity score to identify the exploitability of a vulnerability;
- The vulnerability assessment and the impact assessment are treated as a combined process because the updated version of CVSS 3.1 takes into account the impact that the exploitation of a vulnerability could cause to the under examination environment;
- The estimation of SCS risk is produced taking into account the adopted AP which is defined according to the followed assurance level of evaluation (as described in sections 2 and 3);
- The SCS can be evaluated in different views (business-, technical-, sectoral) depending on the SCS Providers and SCS BPs requirements;
- the SCS analysis and the asset model development are enhanced according to specific SCS asset characteristics and security configuration derived from the created SCS-ISMS inventory. In addition, SCS components (processes, BPs, and assets) are prioritized (analyzed in the next section) in relation to their criticality to the provision of the SCS (according to the adopted SCS evaluation view);
- As the adopted vulnerability analysis evaluation becomes higher, a more rigorous and focused vulnerability analysis is conducted to estimate the cascading effects and risk propagation in a more detailed manner.

The CYRENE RCA methodology in relation to the CVSS 3.1 vulnerability severity score (cf. section 2.2.7), has reconsidered this calculation. In particular, it has adjusted the decision-making for the selected environmental group metrics to the impact the exploitation of the vulnerability could cause on the SCS Environment. To this end, it explores specific characteristics from the developed SCS-ISMS inventory: the implemented security controls and the SCS asset model complexity according to specific criteria analyzed in the next section.

5.3 Step Analysis of the CYRENE CA Methodology

The steps and sub-steps of the methodology have been depicted in section 5.1 in Table 19. The current section presents in detail these consecutive steps of the CYRENE RCA methodology.

High-level steps follow the specific structure below if and where needed:

- **Scope/Goal:**

Description of the scope of the step

- **Input:**

Description of the main input of the step and the processes that have to be undertaken

- **Expected Outcome:**

Information or other sources or documents or results that set the accomplishment of the step.

Example: An example is given in each step wherever required for better comprehension of the reader.

Table 20 – Step analysis structure of the CYRENE RCA methodology.

The steps of the current RCA methodology shall be implemented whether they are applicable or not to the adopted SCS evaluation view.

Step 0: Scope of the SCS RCA

The current step aims to identify the scope and the boundaries of the CYRENE SCS RCA.

- **Scope:**
 - **The selection of the Supply Chain Service (SCS) and the scope of the assessment** must be determined (if the SCS-P and SCS-BPs aim to assess the SCS risks and prepare the SCS-PP, then the enhanced Risk Assessment (RA) use of the CYRENE methodology should be undertaken, whereas if an assessor (self-assessor or CAB depending on the assurance level that will be adopted) aims to assess the claims of a given SCS-PP, then the Conformity Assessment (CA) use of the CYRENE methodology must be performed as described in section 2.3. In addition, **the SCS evaluation view that will be adopted** (overall business, technical, sectoral-technical) must be defined (see section 4.1).
 - Definition of the **boundaries** for the assessment (overall scope, main goals, expected outcome). The SCS-P and the SCS-BPs have

signed an SCS Security Declaration and Application Statement (SDA) that considers all above obligations (see section 0). In case the CA use of the CYRENE methodology will be carried out, a mutual recognition of certification schemes must be provided by the SCS-BPs via signing a Mutual Recognition Agreement (MRA) in case there are SCS-BPs who reside in non EU member countries, as described in the respective MRA section of the proposed EUSCS of CYRENE Report 2.

- Definition of the assurance level according to the SCS criticality identification (see section 2.4.4) and thus attacker’s maturity level/ AP for the SCS is identified as well (see section 2.4.3)

- **Input:** SCS SDA signed from SCS-BPs and SCS MRA signed if it is required
- **Expected Outcome:** Specification of the boundaries for the SCS enhanced RCA

Example:

Supply Chain Risk Assessment (SCS-RA): Vehicles Transport Service Risk Assessment (VTS-RA)	
Scope of the SCS-RA	<ul style="list-style-type: none"> • The Vehicles Transport Service (VTS) is selected and RA will be provided to assess the VTS risks and prepare the VTS-PP • All ICT assets and components required for the provision of the VTS, its Assurance Level (AL), the SCS evaluation view, the level of the Attack Potential (AP) that has to be reached. • Identification, analysis, assessment, and migration of all cyber risks associated with the VTS.
Input	<ul style="list-style-type: none"> • Signed SDA by the VTS business partners. • Assessment of VTS criticality to define the evaluation type and assurance levels
Expected outcome	<ul style="list-style-type: none"> • Specification of the VTS boundaries (e.g. VTS Criticality: Low, AL: Basic Evaluation view: SCS holistic-technical view, AP: Basic) • Evaluation of the ICT-related element of the VTS.

Table 21 – Step 0 example.

In this example, the selected SCS is the Vehicle Transport Service (VTS) the overall scope of the assessment is identified (e.g. the purpose is to assess risks and develop the VTS Protection Profile (SCS-PP), the SCS evaluation view is determined (cf. section 4.1 and Glossary of section 8), the SCS assurance levels that will be followed are estimated.

The VTS-P is the “entity” (see Glossary in section 8), who initiates the SCS-RA, seeking to manage the SCS risks, develop the SCS-PP in compliance with the proposed EUSCS of CYRENE Report 2 to request security certification for the SCS.

The SCS-BPs shall sign the SCS-SDA (see section 4.3). The SCS-SDA document shall follow the template found in Appendix “A” of section 9 of this report.

The VTS criticality, the AL, and the AP are identified following the evaluation criteria of CYRENE assurance scales, presented in Table 6 and Table 7 of section 2.4.4 and the CYRENE SCS criticality, shown in Appendix G-IV. As a consequence, in this example VTS is considered an important and international service, the VTS-P is the Automotive Manufacturer, and thus he is an Operator of Important Services (OIS) regarding NIS 2 Directive [13]. Moreover, VTS is considered of “Low” criticality and the AL “substantial” of the proposed EUSCS shall be followed which is related to AVA_VAN 2 and AP “enhanced-basic”.

Step 1: Analysis of the SCS

The current step aims to thoroughly analyze the under examination SCS and delve into each main component according to the adopted type of SCS evaluation view (see section 4.1).

The current step is divided into the following subsequent steps:

Step 1.1 Scope, objectives, and requirements of the SCS

Step 1.2 SCS Business Partners

Step 1.3 SCS modeling

This step falls into the following scope, input and outcome.

- **Scope:**
 - Description of the SCS, identification of SCS, scope, security objective, and requirements (step 1.1)
 - Identification of the business partners (BPs) participating in the SCS (step 1.2)
 - Identification and modeling of the SCS-processes/ BPs/assets involved in the SCS (step 1.3)
- **Input:**

Each SCS-BP has submitted their security policies in the SCS-ISMS along with the SCS-assets that they host and implemented controls documentation (implementation report, patches, exploits available, penetration testing results, certificates from vendors)
- **Expected Outcome:**
 - Textual description of the SCS (step 1.1) and SCS processes (step 1.3)
 - SCS-asset and SCS business models revealing interdependencies according to asset criticality rules identified in step 1.3
 - SCS-assets implemented security controls lists (step 1.3)
 - SCS-processes criticality (step 1.3)
 - SCS-assets criticality
 - SCS-ISMS inventory hosting all the above

Step 1.1: Scope, objectives, and requirements of the SCS

Within this step, a concrete definition of the SCS, its scope, security objectives, and assurance requirements shall be provided. Based on concepts of section 4 and the SCS-TOE analysis of

CYRENE Report 1 [12], a comprehensive description of the SCS as TOE and its environment (e.g., maritime, pharmaceutical, food) should be produced. The security objectives of the SCS will be specified.

According to the Common Criteria (CC, part1)²⁵ TOE (see Glossary in section 8.2) is “flexible in what to evaluate, therefore, it is not tied to the boundaries of IT products”.

As defined in CYRENE Report 2 [2], the proposed CYRENE EUSCS scheme aims at improving the Internal Market conditions, and at enhancing the level of security of a wide range of supply chain services, of the supply chain capabilities they implement, including business partners, supply chain processes/sub-processes, assets (hosted by different business partners) used for the provision of the SCS.

In the CYRENE project, the TOE is the SCS (SCS-ToE). To evaluate the SCS-TOE it must be decomposed into its main generic components: SCS processes, SCS business partners, and SCS assets. Definitions on the SCS and each embedded component are provided in the Glossary of section 8.1. Within this step, the following security and assurance requirements of the SCS-TOE will be provided, taking into account its environment:

- Requirement for identifying SCS components criticality
- Requirements on security controls implemented on the SCS assets
- Requirements for SCS-PP

Requirement for identifying SCS components criticality

An SCS process disruption (interruption, cancellation, or delay) may cause-effect to the provision of the SCS ranging from low consequences (e.g. a logistics process delay of ten minutes) to serious consequences that could harm even human life (e.g. a three-hour power outage due to a cyber attack on a power system application in a port terminal can cause serious delays in the delivery of the vehicles to the end consumer).

Therefore, to avoid such circumstances, a first step is to evaluate the criticality of the SCS process towards the impact it can cause in the provision of the SCS.

Moreover, SCS processes shall be investigated to identify their importance towards the SCS provision and if their interruption, cancellation, or delay can affect the provision of the SCS (e.g. which will be the impact to the final consumer if the vehicles and loading process is disrupted).

The *SCS process criticality* in the provision of the SCS should be explored in relation to the specific criteria, analyzed in step 1.3.5.2, concerning the SCS process Confidentiality, Integrity or Availability (see Glossary of section 8), the existence of a business continuity plan, the existence of a disaster recovery plan.

In this regard, the SCS-P/Assessor shall prepare the SCS-PP/assess the SCS-PP provided by the SCS-P according to the following:

²⁵ <https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf>

- the criticality of each SCS-TOE process shall be identified with respect to the impact it could cause in the provision of the SCS in view of a disruption concerning the specific factors abovementioned
- the prioritization of the SCS-TOE processes in terms of their criticality in the provision of the SCS should meet the specific conditions described in step 1.3.5.2 of the current methodology:

SCS business partners should be evaluated based on their *importance* in the SCS process, to illustrate their importance to the process execution.

In this regard, the SCS-P/Assessor shall prepare the SCS-PP/assess the SCS-PP provided by the SCS-P according to the following:

- the business partners participating in a given SCS process of the SCS-TOE are assessed in terms of their impact on the SCS process execution, i.e. against the potential of a process termination, cancellation, or delay
- the identified business partners' importance for each SCS process of the SCS-TOE shall meet the conditions presented in step 1.3.5.2 of the current methodology

Despite the SCS overall business evaluation view, where *SCS asset criticality* in the SCS provision is N/A, *SCS assets* shall be explored concerning their impact in the SCS in terms of disruption. Furthermore, SCS assets criticality shall be evaluated:

- against their *business value* in the provision of the SCS taking into account a set of criticality rules described in step 1.3.5.2
- against their security impact in the provision of SCS. The loss of an SCS asset's Confidentiality, Integrity, and Availability (CIA) could have a serious even tremendous impact on the SCS performance. For, instance the loss of a SCADA remote control unit availability that communicates with a gantry crane that carries a number of automotive vehicles in a port terminal could lead them to fall resulting in the disruption of the Vehicle Transport Service (VTS) that could cause serious damage to the port premises even human injuries to the stevedoring personnel. To avoid such situations, SCS assets can be checked in terms of their Confidentiality, Integrity, and Availability (CIA), namely their security impact, in the SCS performance. The SCS assets security impact is assessed in step 3.4.

In this regard, the SCS-P/Assessor shall prepare the SCS-PP/assess the SCS-PP provided by the SCS-P according to the following:

- SCS-TOE assets criticality identification and SCS assets prioritization according to their level of criticality according to step 1.3.5.2
- SCS-TOE assets CIA maintenance need in the SCS performance following step 1.3.5.2.

Requirements for security controls implemented on the SCS assets.

The SCS-P/Assessor to prepare the SCS-PP/assess the SCS-PP provided by the SCS-P shall check whether the security controls applied on the SCS assets, as described in the SCS- SDA (see section 0) and reported in the developed SCS-ISMS inventory, meet the predefined SCS

security objectives. The security controls shall be checked exploring their updating history, their effectiveness on the weaknesses, and their strength.

Requirements for SCS-PP.

The SCS-PP shall be prepared by the SCS-P in collaboration with the SCS-BPs according to the description of section 4.2 and the SCS-PP template presented in Appendix B of section 9.

The claims of the SCS-PP shall be assessed by the Assessor according to the description of section 4.2 and the SCS-PP template presented in Appendix B of section 9.

The SCS-PP must follow the prerequisites for scheme adoption described in the proposed EUSCS (see CYRENE Report 2 [2])

According to the abovementioned step 1.1, a short example is presented in the following table for the Vehicle Transport Service (VTS). Security objectives and requirements of the VTS could be plenty. This example presents very few indicatively.

Example:

Scope, objectives and assurance requirements of the Vehicle Transport Service (VTS)	
VTS description	The Vehicles Transport Chain Service is a massively complex system with numerous players, including shippers, transport operators aiming at the shipment and receipt of various types of vehicles and equipment such as trucks, vans, truck trailers, threshing machines etc. This Service is a relatively long and complicated process that involves domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology.
VTS scope	Deliver the Vehicles to the Source Port and complete all the required preparations for shipping.
VTS objective (indicatively)	VTS processes must be operated by the VTS-BPs identified by the VTS-P and SCS assets presented in the SCS-ISMS inventory
VTS security objective (indicatively)	The SCS-TOE must advise SCS-BPs users of possible unauthorized use on their SCS-assets and restrict security management functions from unauthorized use
VTS requirement (indicatively)	<ul style="list-style-type: none"> • Requirement for VTS assets security architecture description • Requirement for vulnerability analysis on SCS-TOE assets following the evaluation assurance class AVA_VAN 2 of CC in line with the proposed EUSCS

Table 22 – Step 1.1 example.

Step 1.2: SCS Business Partners

Within this step **Identification of BP-s**: Port Authority, Customs, Ship Agent, the SCS-BPs involved in the SCS are specified following the indications given by the proposed EUSCS [2]. To this aim, SCS business partners are distinguished into the following categories, clarified in section 4.1 as well:

- SCS Provider (Business Partner A)
- SCS Commercial Business Partner (Business Partner B)
- Governmental Business Partner (Business Partner C)
- SCS Self-Assessor (Business Partner D)

Example:

VTS Business partners (BPs)	
SCS-P (Business Partner A)	Automotive Manufacturer
SCS Commercial BP (Business Partner B)	Shipping Company, Port Local Agent
Governmental BP (Business Partner C)	Customs
SCS Self-Assessor (Business Partner C)	Port Local Agent

Table 23 –Step 1.2 example.

Step 1.3: SCS Modelling

In Appendix C of section 9, a template is given that can be used for the description of an SCS-TOE entailing the development of the SCS-ISMS inventory incorporating the business SCS partners/processes/assets/security controls/mitigation measures given from the SCS-SDA.

Every SCS-process or SCS-asset will be documented in a systematic approach (e.g. process, physical, network, ICT system/component, service, data, human) by all business partners hosting them. For every SCS-process/asset all implemented controls and their documentation (implementation of controls, certifications, penetration testing reports) will be reported.

The SCS-TOE will be gradually developed depending on the adopted SCS evaluation view: overall business view, holistic-technical view, and sector-specific technical view described in CYRENE Report 2 [12], which is structured as presented in the following sub-steps:

- Step 1.3.1: Identification and description of SCS business processes.
- Step 1.3.2: Identification and description of SCS business partners
- Step 1.3.3 SCS-TOE's infrastructure description (if applicable)
- Step 1.3.4 Business process model generation
- Step 1.3.5 Identification of SCS components criticality and asset model generation

Step 1.3.1: Identification and description of SCS business processes.

In this section, a brief description of each identified business process of the SCS along with the business goal is provided as presented in CYRENE Report 1.

Step 1.3.2: Identification and description of SCS business partners

Identification and description of the business partners involved in the SCS processes. Within this section, the identified SCS-TOE processes are further analyzed into their embedded steps recognizing all the business partners participated together with their interactions and their business roles to fulfill these processes as presented in CYRENE Report 1.

Step 1.3.3 SCS-TOE's infrastructure description (if applicable)

The current section is N/A if SCS's overall business evaluation view is adopted. 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 as presented in CYRENE Report 1.

Step 1.3.4 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 SCS-TOE. To this aim, SCS process models are generated following the formatting presented in CYRENE Report 1.

Step 1.3.5 Identification of SCS components criticality and asset model generation

In this step SCS assets' technical characteristics are identified, the security controls undertaken (which shall be further checked if they meet the security requirements reported in step 1.1) and the asset interdependencies to develop the SCS asset model.

In addition, the criticality of SCS components (SCS process criticality, SCS-BPs importance, and SCS assets criticality) is identified. The goal is to prioritize the SCS components according to their impact on the provision of the SCS.

In Appendix C of section 9, a template that can be used for the description of an SCS-TOE where the systematic inventory of the business partners/processes/assets/controls/mitigation measures is described.

The current step consists of the following sub-steps:

- Step 1.3.5.1 SCS Asset modeling.
- Step 1.3.5.2 Identification of SCS components criticality

Step 1.3.5.1 SCS Asset modeling.

The current sub-step aims to model the SCS assets providing a technical analysis that incorporates the identification of SCS assets security controls and the identification of SCS assets interdependencies.

SCS assets technical analysis.

As long as a high-level infrastructure representation is obtained, a more detailed and deeper analysis is required to decompose the infrastructure to its individual SCS assets operating in a given SCS process and define the SCS asset technical specificities (asset type, vendor, version, and other technical characteristics). The SCS assessor should review the given asset inventory attached in the SCS-TOE and whether it reflects the content of the specific template of the SCS-ISMS presented in Appendix C of section 9.

Identification of SCS assets security controls

The SCS Assessor shall check from the asset inventory, the security controls undertaken of the SCS assets to investigate the security requirements are met in a later step whether the undertaken countermeasures referred to the SDA are capable. The documentation of controls will include all info/evidence regarding implementation and effectiveness (as mentioned before).

Identification of SCS assets interdependencies

SCS assets interdependencies [22] are estimated based on two vectors **Error! Reference source not found.:**

- *the dependency type*: illustrating the type of cyber dependency between two assets (i.e. 1. hosting, 2. Exchange, data/information, 3. storing, 4. controlling, 5. Processing, 6. Accessing, 7. Installing, 8. Trusted 9. Connecting)
- *the dependency access vector*: showing in which location the assets they are able to interact (Network, Adjacent Network, Local). The utility of this table presentation is to deal with security issues such as estimating the level of the overall cyber assets exposure in cyber risks.

Within this framework, SCS assets interdependency graphs should be developed illustrating

1. the SCS assets operating within an SCS process of the SCS-TOE (Figure 23)
2. the SCS assets operating among different SCS processes of the SCS-TOE (Figure 24)
3. the SCS asset interdependencies within an SCS process and between different SCS processes (Figure 25)

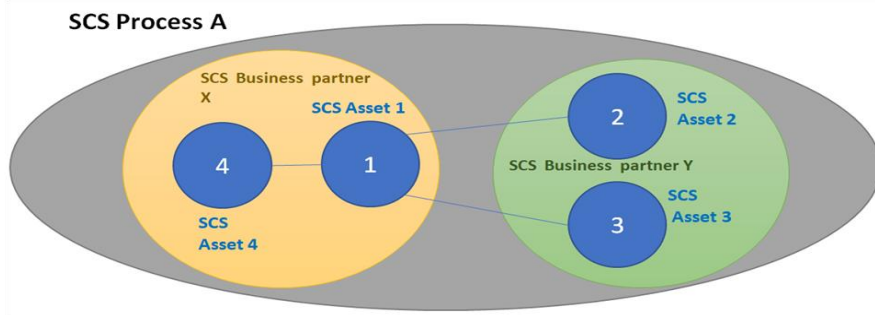


Figure 23 – Example of SCS assets operating within an SCS process among different SCS business partners.

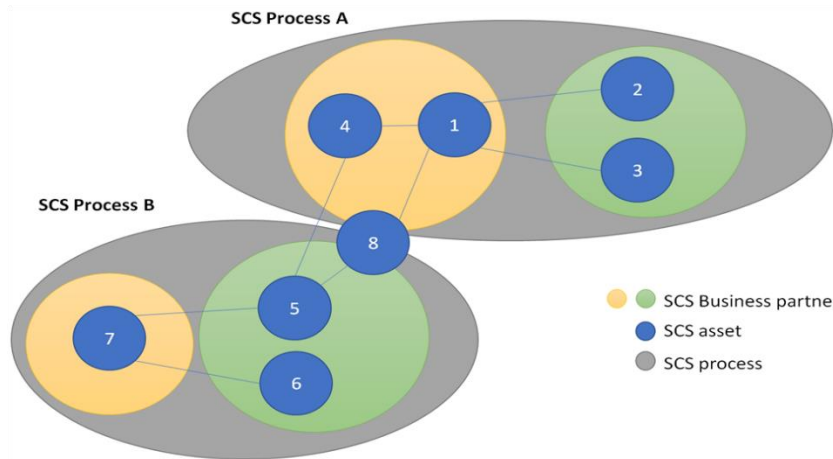


Figure 24 – Example of SCS assets operating within different SCS process among different SCS business partners.

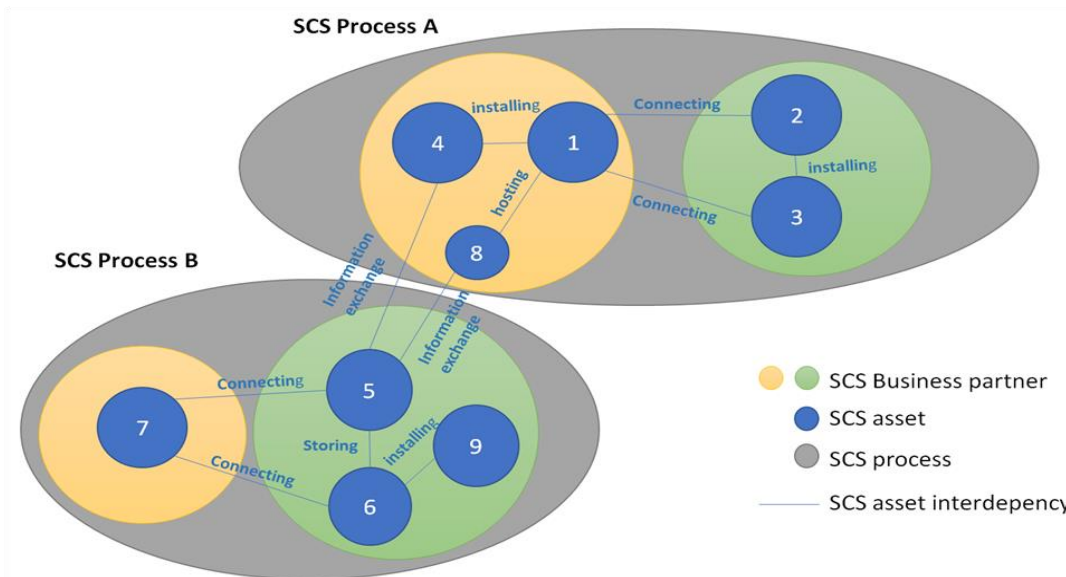


Figure 25 – Example of asset interdependencies of SCS assets operations within a specific SCS Business partner of an SCS process, between different SCS Business partners of an SCS process, and between different SCS Business partners participating in different SCS processes.

Example:

Source Asset	Destination Asset	Asset Cyberdependency	
		Dependency Type 1. hosting, 2. Exchange, data/information, 3. storing, 4. controlling, 5. Processing, 6. Accessing, 7. Installing, 8. Trusted 9. Connecting	Access Vector Network, Adjacent Network, Local
Web Server (A _{1,2})	Operating System (OS) (A _{1,3})	installing	Local (L)
Web Application (A _{1,4})	Web Server (A _{1,2})	hosting	Local (L)
DataBase (A _{2,1})	Web Application (A _{1,4})	exchange data/information	Network (N)

Table 24 – SCS asset cyber dependencies identification.

Concerning the VTS-assets technical specification must follow the SCS-ISMS inventory template provided in Appendix C of section 9.

With respect to the asset interdependencies identification, Table 24 illustrates the cyber dependencies between a Web Server installed on an OS, a Web Server hosting a Web Application, and a Database that exchanges information with the Web Application. Every asset is presented in $A_{i,j}$ format, where i indicates the SCS-BP which resides and j refers to asset numbering. The Web Server, the OS, and the Web Application are connected locally whereas the database with the Web Application is interconnected through the Network.

Step 1.3.5.2 Identification of SCS components criticality

SCS components (processes, business partners, and assets) should be evaluated in relation to the provision of the under examination SCS, to explore if the corresponding requirements described in Step 1.1 are met.

SCS process criticality in the provision of the SCS.

Given that the provision of the SCS depends on the performance of SCS processes, an abnormality or absence of their execution could lead to the SCS disruption (interruption or cancellation, or delay). With this respect, the SCS process criticality is considered the estimation of the SCS process importance in the SCS provision (in terms of causing an SCS disruption), as described in Step 1.1.

The SCS process criticality is assessed by the SCS-P and SCS-BPs, by filling the template SCS process criticality table presented in Appendix D-I of section 9. To identify the SCS process criticality the CYRENE RCA methodology considers the SCS process criticality rules described in the following.

The SCS process criticality should be explored under the following evaluation criteria:

(1) the SCS process Confidentiality, Integrity or Availability

QUESTION A: How important is the SCS process for the provision of the SCS in terms of SCS, Integrity, or Availability (CIA)? (in case the SCS process loses its Confidentiality, Integrity, or Availability (CIA) will it affect negatively the provision of the SCS?)

SCS process criticality rule 1:

- If the loss of the SCS process CIA does not affect the normal provision of the SCS, the SCS process Criticality, can be assessed with a value either “Very Low” or “Low”.
- If the loss of the SCS process CIA affects the normal provision of the SCS, the SCS process Criticality, can be assessed with a value either “Medium” or “High” or “Very High”

(2) the existence of a backup/business continuity/disaster plan or an alternative SCS process

QUESTION B: Is there a backup/business continuity/disaster plan for the SCS process or an alternative SCS process in case of SCS process disruption or cancellation? (Yes / No)

QUESTION C: In case there is a backup plan or an alternative SCS process is it sufficient to the normal provision of the SCS? (Yes/ No)

(Question C applies only in case the adopted EUSCS AL is “High”)

SCS process criticality rule 2:

- If a backup/business continuity/disaster plan exists, SCS process Criticality decreases (-1) (if it is Very Low from the previous rule stays Very Low)
- If a backup/business continuity/disaster plan does not exist, SCS process Criticality increases (+1) (if it is Very High from the previous rule stays Very High)
- If the backup plan or the alternative SCS process is sufficient, the SCS process Criticality decreases (-1) (if it is Very Low from the previous rule stays Very Low) *(applies only in case the adopted EUSCS AL is “High”)*
- If the backup plan or the alternative SCS process is not sufficient, the SCS process Criticality increases (+1) (if it is Very High from the previous rule stays Very High) *(applies only in case the adopted EUSCS AL is “High”)*

Example:

VTS process “Entry Summary Declaration” for EUSCS AL “Substantial”

Question A				
Importance of the SCS process for the provision of the SCS in terms of SCS, Integrity or Availability (CIA)?				
In case the SCS process loses its Confidentiality, Integrity or Availability (CIA) it does not affect negatively the provision of the SCS		In case the SCS process loses its Confidentiality, Integrity or Availability (CIA) it affects negatively the provision of the SCS		
Very Low	Low	Medium	High	Very High
			X	
Question B				
Is there a backup/business continuity/disaster plan for the SCS process or an alternative SCS process in case of disruption or cancellation?				
Yes		No		
X				
Question C (if only Question B is "Yes" and adopted EUSCS Assurance Level (AL) is "High")				
Is the backup plan for the SCS process or the alternative SCS process sufficient for the normal execution of the SCS?				
Yes		No		

Table 25 – Example for identification of SCS process criticality.

In the current example, the VTS process “Entry Summary Declaration” is characterized by the VTS-BP of “High” value for QUESTION A. Regarding QUESTION B since an alternative process exists according to the 2nd process criticality rule, CYRENE RCA methodology decreases its criticality at one level turning it to “Medium”. As the adopted EUSCS AL is “Substantial”, QUESTION C is ignored and thus the VTS process “Entry Summary Declaration” is assessed of “Medium” level criticality in the provision of the VTS.

SCS business partner importance to the SCS process.

SCS business partners who participate in an SCS process can affect the process execution depending on their importance on the SCS process operation. In step 1.1, it is indicated that business partners should be assessed according to their importance on an SCS process

execution. This should be evaluated from SCS-BPs by filling the template depicted in Appendix D-II.

Example:

	Impact to the “Entry Summary Declaration” process execution				
	Very Low	Low	Medium	High	Very High
Business partner A				X	
Business partner B			X		
Business partner C					X

Table 26 – Example of identification of SCS business partners' importance to the “Entry Summary Declaration” process.

In the above example, SCS-BPs have estimated their importance for the normal execution of the Entry Summary Declaration process.

SCS asset criticality in the provision of the SCS.

(N/A for the evaluation of SCS-TOE process view)

SCS assets shall be explored concerning the business impact value they could have to the SCS in light of an SCS disruption.

In this regard, SCS assets' criticality shall be evaluated against their *business impact* in the provision of the SCS.

To identify the SCS assets' criticality in the provision of the SCS, SCS assets interdependency graphs should be developed illustrating the SCS assets' position within the SCS process.

Asset business impact.

The SCS asset is evaluated based on the SCS asset's relation to the SCS process(es) of the SC-TOE.

In this vein, the asset business impact is determined depending on the identification of the criticality of SCS assets in the provision of the SCS with respect to:

- *the SCS process criticality* it resides,
- *the number of the appearance of the SCS asset in different SCS processes*
- *the number of interdependencies* it has with *other SCS assets*.

Upon this, the SCS-P and the SCS BPs/SCS Assessor should fill/check a respective form of a questionnaire on SCS assets.

CYRENE RCA methodology with the calculation of asset criticality rules re-estimates assets criticality to ensure that all-important factors are considered to determine the asset criticality within the SCS network.

By implementing the following asset criticality rules on the SCS assets that reside in the SCS-ISMS inventory (see Appendix C of section 9) assets are prioritized according to their criticality in the provision of the SCS. The evaluation scale follows again a five-level qualitative structure: Very Low/Low /Medium/High/Very High.

Asset Criticality Rule 1: The SCS asset should inherit the SCS process criticality of the SCS process that operates.

Example: If an SCS process A where SCS asset 1 operates has been assessed of “Medium” criticality, the SCS asset 1 has also “Medium” criticality to the provision of the SCS.

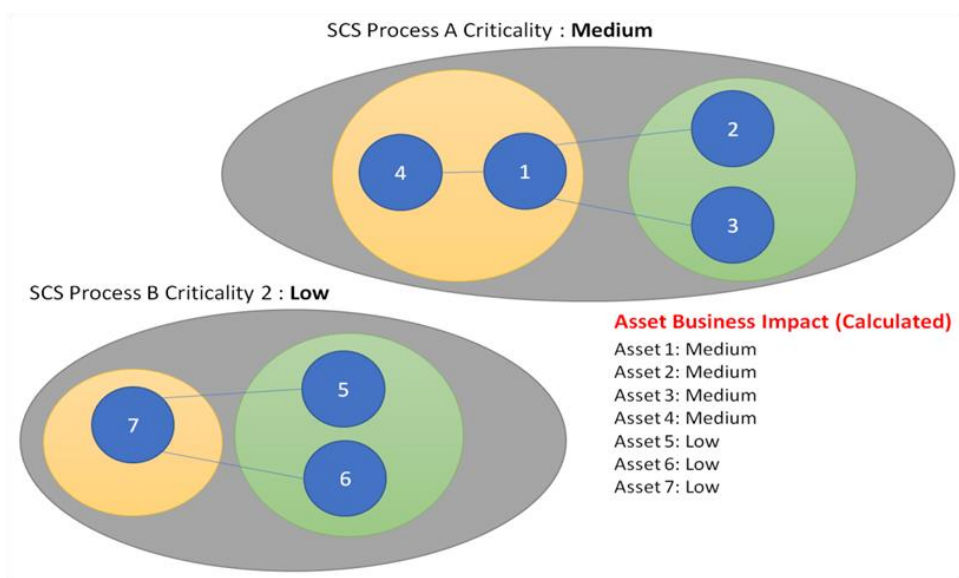


Figure 26 – SCS assets inherit SCS process criticality to which they belong (Rule 1).

Asset Criticality Rule 2: In case the SCS asset operates for the execution of more than one SCS process, the SCS asset should inherit the SCS process criticality of the worst-case scenario.

Example: SCS asset 8 operates both for the execution of SCS process A and SCS process B. According to the above, it inherits the highest criticality of the SCS process it is involved in (worst-case scenario), which value “Medium” of SCS process A according to the example in the following Figure 27.

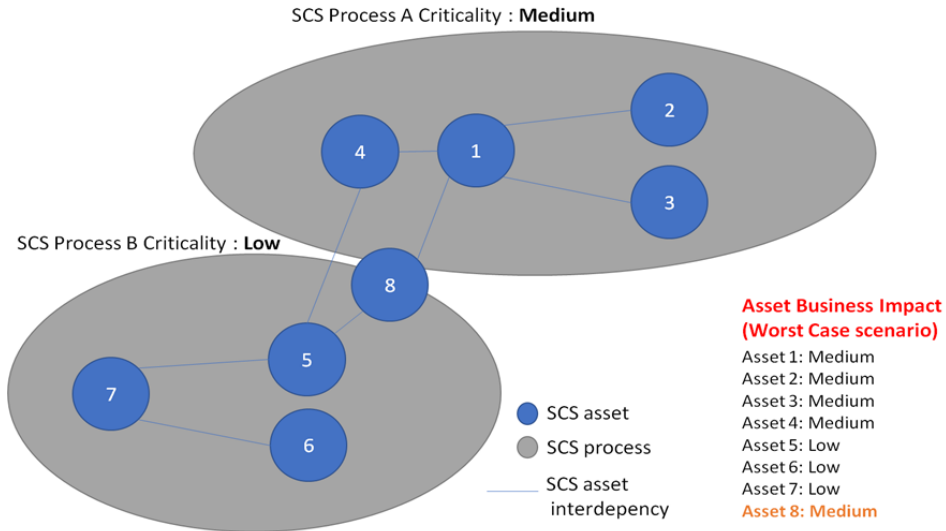


Figure 27 – SCS asset 8 that operates in SCS process A and SCS process B inherits the worst-case scenario of SCS criticality, which “Medium” level of criticality of SCS Process A.

Asset Criticality Rule 3: In case the SCS asset appears to operate in a number of SCS processes, the SCS asset criticality should be assessed according to the number of the SCS processes the SCS asset appears towards the overall number of SCS processes that participate in the provision of the SCS (if SCS asset operates in more than 50% SCS processes then the value of its criticality is increased at one level (x+1) otherwise stays as it is)

Thereby,

If

SCS asset ‘Y’ appears more than 50% and the SCS asset criticality is ‘X’

Then

SCS asset criticality turns to ‘X+1’

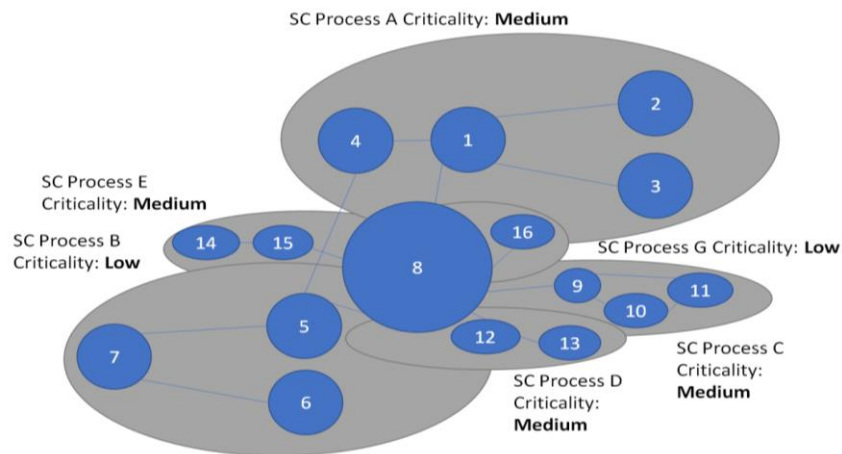


Figure 28 – SCS asset criticality depends on the frequency of its appearance in the overall number of the SCS processes.

Example:

If an SCS asset which has been characterized with “Medium” criticality as a result of the previous criticality rules it operates in 6 SCS processes and the overall processes for the provision of the SCS is 10, this means that the SCS asset it is involved to the 60% of the SCS processes, thus its criticality is increased at one level and the SCS asset criticality turns to “High” (see Figure 28 and Table 27).

SCS asset	Asset participation in the overall SCS processes	SCS Asset criticality value from the implementation of previous rules	SCS criticality when the number of appearance in the overall SCS processes is > = 50%
asset 8	Participates in 6 SCS processes out of 10 SCS processes (6/10)	Medium	High

Table 27 – Example of asset criticality ‘Rule 3’ for ‘SCS asset 8’.

Asset Criticality Rule 4: If there is a sufficient backup plan or an alternative procedure for the use of the SCS asset, then the SCS asset criticality decreases at one level (-1), but it cannot turn to a lower level than the SCS process criticality. In case it does not have a backup plan, the SCS asset criticality increases at one level (+1).

Examples:

(i) the SCS asset is characterized from the implementation of previous rules with “High” criticality, the SCS process criticality it operates is “Medium” and the SCS asset has a sufficient backup plan or an alternative procedure for the SCS process it operates, then the SCS asset criticality turns to “Medium”.

(ii) the SCS asset is characterized from the implementation of previous rules with “Medium” criticality, the SCS process criticality it operates is “Medium” and the SCS asset has a sufficient backup plan or an alternative procedure for the SCS process it operates, then the SCS asset criticality stays to level “Medium”.

(iii) the SCS asset is characterized from the implementation of previous rules with “High” criticality, the SCS process criticality it operates is “High” and the SCS asset does not have a sufficient backup plan or an alternative procedure for the SCS process it operates, then the SCS asset criticality turns to “Very High”.

Asset Criticality Rule 5: Asset complexity.

A SCS engages a great variety of BPs upon which numerous assets operate to execute multiple processes. Such asset networks consist of heterogeneous interconnected dispersed nodes. In this vein, asset model complexity shall be checked. Moreover, to assess the SCS assets criticality, whether and which group of rules exists (concerning the above) as well as the SCS asset accessibility within the network must be taken into account, to identify

- from how many entries point the targeted SCS asset can be reached. A high number of asset entry points that are mission-critical to reaching the targeted asset shall raise the SCS asset level of criticality;
- the SCS asset path, namely, the length between an SCS asset entry point and the SCS asset target point. A long length between an SCS asset entry point and the SCS targeted asset shall increase the SCS asset level of criticality.

Taking into consideration that the asset model is represented as a graph, its complexity can be estimated using the Betweenness centrality metric [24] for every asset in that graph. The metric defines and measures the importance of a node in a network-based on how many times it occurs in the shortest path between all pairs of nodes in a graph. Nodes with the highest betweenness centrality are crucial to the communication in a graph as they connect a high number of nodes with each other. Removing these nodes from the network would lead to huge disruption in the linkage or communication of the network.

A Betweenness centrality metric numeric value is assigned to every asset so it is necessary to determine the mapping of numerical values to qualitative values (Very Low, Low, Medium, High, Very High). Calculated numerical value depends on a number of assets and their interconnections so this mapping needs to be determined with respect to those aspects.

On this account, we consider that the SCS asset criticality already estimated from previous rules implementation increases at one level (+1) if the calculated SCS asset betweenness centrality is equal to or above the 60th percentile. Nevertheless, if the Betweenness centrality of an asset is below the 60th percentile, then it decreases one level (-1).

All of the above SCS assets rules of criticality are explored to estimate assets' importance to the provision of the SCS in qualitative/quantitative values as presented in the CYRENE probability scale ranging from Very Low, to Very High (see Appendix G of section 9).

Example:

If the asset complexity calculation belongs to (a), then the SCS asset criticality turns to “Very High”. If the asset complexity calculation belongs to (b), then the SCS asset criticality turns to “Medium”

SCS asset	SCS Asset criticality value from the implementation of previous rules	(a) Asset complexity is found \geq 60 th percentile	(b) SCS Asset complexity is found $<$ 60 th percentile
-----------	---	--	---

$A_{i,j}$	High	Very High	Medium
-----------	------	-----------	--------

Table 28 - Example of asset criticality 'Rule 5' for SCS asset model complexity.

Step 2: SCS Threat Analysis

In this step, assets are tested and evaluated against the information gathered to determine where potential threats could be. For each threat identified, the probability that the threat will be realized as well as the potential impact(s) if the threat is exploited will be also determined. The current step is divided into the following sub-steps:

Step 2.1 Identification of Threat Scenarios/Threats

Step 2.2 SCS Threat Assessment

Step 2.1: Identification of Threat Scenarios/Threats

This step aims to identify individual threats and explore threat scenarios.

- **Scope:**

A threat can be anything that can exploit a vulnerability to breach security and negatively affect the organization's critical data or systems. A threat can be defined as "intentional" (e.g., an individual hacker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning). According to ETSI-TVRA methodology [25], threats in ICT systems may be classified into several groups:

- Interception - the concept of interception refers to the situation that an unauthorized party has gained access to a service or data. An example of interception is unauthorized monitoring of communication (eavesdropping).
- Manipulation – it includes changing transmitted data, the pretense of an entity to be a different entity, unauthorized access, forgery.
- Interruption - it refers to the situation in which services or data become unavailable, unusable, destroyed, and so on (e.g., Denial of service)
- Repudiation - it assumes that an entity involved in an exchange denies the fact

The same classification may be applied for supply chains if they are considered on the level of infrastructure and assets (see CYRENE SCS-TOE II and SCS-TOE III in CYRENE Report 2).

- **Input**

to realize the threat scenarios or identify threats within SCS, we need to identify all the information for individual cyber threats against the SCS- cyber assets deriving from:

- **business partners** (based on their reported threats, expertise),
- existing **repositories** of cyber threats,
- from **crowdsourcing** (a community of online users/security, experts/stakeholders),
- from **social media** (discussion groups or forums),
- intrusion incidents,
- detection system logs,
- reported exploitations,
- firewall logs,
- the reverse engineering of malware,
- internal policies and procedures,

- system configuration information.

In the case of the CYRENE system, the identification of the actual source and type of a security threat will be carried out using MITRE ATT&CK knowledge base of adversary tactics and techniques based on real-world observations²⁶.

Next, the use of the Deep and Dark Web mining and knowledge inference from social networking services will allow the exploitation and analysis of threats related information embedded in user-generated content.

In addition, various log files and network traffic data will be examined by applying anomaly detection and classification algorithms. The anomalies identification functions will be supported by reasoning mechanisms, data mining methods, ontology, and global AI inference models.

- **Expected Outcome:**

- List of individual cyber threats applicable to the SCS assets. Every threat should be documented by providing threat description, threat target, attack techniques, countermeasures
- Set of correspondences of individual cyber threats to the cyber assets within the SCS

Example:

Threat ($T_{i,j}$)	Cyber Threat Name
$T_{1,1}$	XML Passer Attack
$T_{1,2}$	Buffer Overflow in Local Command-Line Utilities
$T_{1,3}$	Signature Spoofing by Key Theft
$T_{1,4}$	Manipulating Web Input to File System Calls

Table 29 – Step 2.1 example

Step 2.2: SCS Threat Assessment

- **Scope:**

In this step, every identified threat should be rated based on the risk they carry out. Different techniques for threat assessment may be used. It is possible to prioritize a threat using Low, Medium, or High scale or by applying a more sophisticated approach like the one proposed by MITRE [26]. The MITRE approach, for example, characterizes threats using qualitative levels: advanced, significant, moderate, limited, and unsophisticated. Accordingly, to estimate the probability of occurrence, the MITIGATE approach can be

²⁶ MITRE ATT&CK, <https://attack.mitre.org/>

utilized as well. In this direction, we will identify the scope of the assets, services, business workflows, and systems of SCS to perform the Threat Assessment and the set of CYRENE layers that will support this task. Based on the CYRENE layers and their functionalities, several datasets and logs will be collected and harvested to uncover and identify vulnerabilities resulting in potential threats (i.e., unauthorized access, misuse of information, data leakage, loss of data, disruption of service) from monitoring probes, networking devices, firewall records, dark and deep web sites, etc. Based on their criticality, the threats can be then prioritized to take further actions or decisions.

- **Input:**

List of cyber assets, services, business workflows, and systems of the SCS infrastructure

- **Expected Outcome:**

List of Threat levels per asset, service, and system prioritized for **every identified threat**

In this step, the probability of occurrence of each cyber threat to each SCS cyber asset shall be assessed. It can be calculated based on the following criteria:

- (a) The expected frequency of appearance according to the history of previous incidents;
- (b) The participants' knowledge and intuition;
- (c) Information gathered from social media and existing repositories will be used in order to draw conclusions

To assess threats, The MITIGATE threat scale can be used as follow (see Table 30):

It consists of the following values:

- The Threat Class: Very High (5), High (4), Medium (3), Low (2), Very Low (1);
- The Value Range: (80-100%], (60-80%], (40-60%], (20-40%], [1-20%];
- The Default Value: 100%, 80%, 60%, 40%, 20%.
- The History of Incidents: describes how many times an incident of a specific threat was realized during a specific period;
- The Intuition & Knowledge: depicts the probability that this threat is expected to occur within the assets of the business partner, based on the knowledge and intuition of the participants;
- Social Information: depicts the probability that this threat is expected to occur within the assets of the business partner, based on the information gathered from social media and existing repositories.

Threat scale			Description of threat level		
Threat class	Value Range (%)	Default Value (%)	History of incidents	Intuition & knowledge	Social Information
Very High (5)	(80-100]	100	1 in the last year (12-month period)	Very high probability (> 80%)	Very high probability (> 80%)
High (4)	(60-80]	80	1 in the last year (12-month period)	High probability (61-80%)	High probability (61-80%)

Medium (3)	(40-60]	60	> 1 in the last 2 years	Medium probability (41-60%)	Medium probability (41-60%)
Low (2)	(20-40]	40	<= 1 in the last 2 years	Low probability (21-40%)	Low probability (21-40%)
Very low (1)	[1 –20]	20	<= 1 in the last 3 years	Very low probability (<= 20%)	Very low probability (>= 20%)

Table 30 – MITIGATE Threat scale

Example:

Threat	Threat name	Threat Level
T _{1,3}	Signature Spoofing by Key Theft	High

Table 31 – Step 2.2 Example

An SCS-BP identifies a threat of signature spoofing by key and from the newsfeed (s)he has been informed that it was observed twice within the last two years. Based on this threat appearance, the probability of occurrence according to the threat scale is considered “High”.

Step 3: Vulnerability and Impact Analysis

The current step aims to conduct vulnerability analysis and to estimate the security impact on an SCS asset of vulnerability exploitation.

- **Scope:**
 - Estimation of the **severity of all identified vulnerabilities using CVSS 3.1** (see section 2.2.7)
 - Calculation of the (qualitative) probability of successfully exploiting each vulnerability
 - Using the CVSS 3.1 Base, temporal and Environmental Metrics (the CVSS calculator)
 - Taking into account the SCS-environment, SCS-assurance level, attack potential, asset/control documentation in the SCS-ISMS,
 - Propagation is being considered since we use CVSS 3.1 if the adopted EUSCS AL is either “basic” or “substantial”. In case EUSCS AL is “High”, a deeper vulnerability analysis shall be undertaken estimating more accurately the propagation by exploring vulnerability chains – see step 3.4)
- **Input:**
 - Collaboratively assess the implemented controls towards the existing patches.
 - Consider SCS-asset interdependency graphs derived from Step 1 and SCS assets criticality to estimate assets importance within the provision of the SCS
- **Expected Outcome:**
 - The CVSS total score reveals the **Vulnerability Levels+Impact levels (VL)** of each (confirmed and zero-day) vulnerability to each SCS-cyber assets

Vulnerability and Impact Analysis consists of the following steps which are analysed hereafter:

3.1 Estimation of Attack Potential

3.2 Vulnerability Severity Estimation

3.3 Evidence-based Vulnerability Analysis (VA)

3.4 Identification of Confirmed and Zero-Day Vulnerabilities

3.5 Building all Vulnerability Chains within the SCS

3.6 Identification of Attack Methods and Attack Graphs

3.7 Attack Impact

3.8 Systematic Documentation of Vulnerabilities

3.9 Occurrence Likelihood and Impact Assessment

Step 3.1 Estimation of Attack Potential

Considering the analysis of section regarding the Attack Potential (AP) its mapping to Assurance Levels and the respective attacker’s profiles is therein identified according to these factors.

The Attack Potential (AP) can be considered from two views:

- Estimating the AP which can be defeated according to a specific vulnerability evaluation analysis (AVA_VAN.xx) conduction implemented in terms of the adopted SCS assurance level requirements
- Estimating a threshold of the AP required above from which the adversary is capable of successfully intruding the desired target

Having identified in section 2.4 the concept of Attack Potential (AP) and its dependencies with SCS assurance levels, the vulnerability evaluation levels, and attacker’s profile, we have recognized **the level of resistance of the SCS-TOE to the possibility of an intrusion possessing AP either “Basic” or “Enhanced-Basic” or “Moderate” or “High”**. In addition, the AP has been mapped to the evaluation levels that apply to the SCS. Within this framework, in step 1 of the CYRENE RCA methodology, we’ve considered that the value of the AP is dependent and identified according to the adopted SCS assurance level (which is determined with regards to the SCS-TOE criticality).

Example:

According to what has been described previously and to the assurance scales of section 2, if the adopted EUSCS Assurance Level (AL) is “High” it can

EUSCS AL	SCS-TOE meets assurance components	SCS-TOE Failure of assurance components	SCS-TOE is resistant to attackers with AP	SCS-TOE can be intruded with attacker’s possessing AP
Substantial	AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5	Basic, Enhanced Basic	Moderate, High, Beyond High

Table 32 – Step 3.1 example.

Step 3.2: Vulnerability Severity Estimation

In this step the individual vulnerability level is calculated. CYRENE uses the CVSS 3.1 score metrics as a common reference framework for discussing the severity and impact of cyber vulnerabilities in the SCS.

Similarly, the CVSS 3.1 score has been used by the Food and Drug Administration (FDA) as a reference to the medical device supply chain and by NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations to characterize, categorize, and score SCS vulnerabilities.

The current step does not apply to the overall business SCS evaluation view.

The step estimates the *Vulnerability Severity Level (VSL)* which measures:

the probability of an attacker successfully reaches and exploits a specific vulnerability (either confirmed or unknown) taking into account temporal vulnerability characteristics and the impact according to the user's environment to a specific asset.

The CVSS 3.1 Environmental Group metric calculates the vulnerability severity of an asset exploitation to the business (organizational) environment. The CYRENE RCA methodology, as defined in section 2.3, takes into account a set of features that can affect the level of exploitability in order to estimate the vulnerability severity of a SCS asset to the impact that can cause to the SCS environment. According to Section 2.4, the SCS provider and the collaborating SCS-BPs when conducting the assessment should consider the following features in order to fill the environmental group metrics of the CVSS 3.1 score:

- The SCS asset criticality (see Step 1.3.5.2)
- The SCS asset model complexity (see Step 1.3.5.2)
- The security controls effectiveness (strength)
- The security controls updates
- Modified Scope (MS)

The CVSS 3.1 environmental Group considers the impact of a vulnerability exploitability on an SCS asset to the entire SCS environment as it investigates the SCS asset location within the SCS network, the SCS asset accessibility, the specific assets configurations, the SCS assets implemented security controls, and their strength. Thus, the current CVSS 3.1 Environmental Group in accordance with the CYRENE considerations described previously suffice for estimating the cascading effects of the vulnerability's exploitability when adopting a low level of assurance (in that case steps 3.4 and 3.5 aren't needed to be performed). Notwithstanding, as the selected AVA_VAN gets higher, the vulnerability analysis shall be more rigorous and accurate, thus, vulnerability chains and attack paths shall be specifically calculated, and thereby the steps 3.4 and 3.5 are applicable.

Step 3.3. Evidence-Based Vulnerability Analysis (VA)

The current step describes the process that shall be followed for evidence-based vulnerability analysis.

- **Scope:**

This step aims to detect and identify cybersecurity vulnerabilities located in the ICT systems which support the operation of SCS. This can be done by analyzing historical data coming from network data logs, host-based scans, application or database scans, or by real-time inspecting supply chain services via monitoring probes. Evidence will be also recorded and timestamped by identifying incidents, massive calls for cyber-attacks (e.g., DDoS attacks, etc.), stolen credentials, and data breaches in social media, dark web forums, sites, and marketplaces.

- **Input:**
 - non-intrusive network data and meta-data analysis
 - host-based indicators collected in real-time
 - application or database logs
 - real-time monitoring probes and agents
 - dark web URLs to instantiate content retrieval
- **Outcome:**
 - extracted vulnerability indicators,
 - mapping of vulnerability indicators on the corresponding CVEs,
 - timestamped evidence collection based on the category (i.e., derived from cyber-attacks, data, or user space)

Step 3.4: Identification of Confirmed & Zero-Day Vulnerabilities

A zero-day vulnerability refers to a cybersecurity “hole” in the Supply Chain infrastructure that is either unknown to the vendor or has not yet been patched by the vendor. This security “hole” is usually exploited by hackers before the vendor becomes aware and fixes it. There are various methods to identify zero-day vulnerabilities for the SC systems [28]. These methods are broadly classified into statistical-based, signature-based, behavior-based, and hybrid techniques.

- The statistical-based techniques [29] use various statistical methods, i.e. Principal Component Analysis (PCA), to detect zero-day polymorphic issues. As these techniques are dependent on attack profiles built from historical data, they are based on static nature, thus, the vulnerabilities detection techniques are unable to adapt to the timely changes in the environment. **This factor limits the statistical identification approaches to work in off-line mode, hence, they cannot be used for instant detection and protection in the real-time CYRENE SC framework.**
- Signature-based detection methods [30] are based on a library of malware signatures, which are cross-referenced with local/network files, emails, or web material. These libraries can be continuously updated with new signatures that often represent the signatures of new exploited vulnerabilities. In general, signatures-based techniques need an improvement to generate high-class signatures. On the other hand, such type of methods has been used as part of layered architectures for detection and analysis of zero-day attacks. **This leads CYRENE to move towards the use of signature-based methods, i.e., SNORT framework, for identifying zero-day vulnerabilities.**
- Behavior-based techniques sniff essential characteristics of malware in order to predict the future behavior of victim machines and deny any behavior that is not expected [31]. These methods try to predict the flow of network traffic but they suffer as they cannot effectively capture the context in which the worm program interacts with the real victim machine.

At last, the hybrid-based techniques overcome the weaknesses of the above techniques by combining them in various formulations [32]. **CYRENE framework will focus on the hybrid-base framework as it combines the different anomaly and signature-based detection CYRENE implementations in order to identify SC zero-day vulnerabilities.**

Step 3.5: Building all Vulnerability Chains within the SCS

- **Scope:**

Vulnerability chaining is defined by the Common Vulnerability Scoring System (CVSS) User Guide as a situation where multiple vulnerabilities are used in a single attack to compromise a host²⁷. Usually, individual vulnerabilities may not appear to be critical, however, when they are skillfully linked together, they may have a critical impact. Term Vulnerability Chaining refers to the scoring of multiple vulnerabilities in this manner. Vulnerability Chaining is not a formal CVSS metric, but the standard includes guidance for analysts to score these kinds of attacks. The responsibility of the analyst who scores a chain of vulnerabilities is to identify which vulnerabilities are combined to form the chained score. Also, during the vulnerability scoring, the analyst may define other types of related vulnerabilities that are often chained together and can be connected with the vulnerabilities being scored. In order to score the Vulnerability Chain, the analyst should take into consideration the Exploitability, Scope, and Impact metrics of each vulnerability included in the chain. It is recommended by CVSS to take the least-restrictive Exploitability sub-score metrics and the most-impactful Impact sub-score metrics.

Table 33 presents an example of calculating a vulnerability chaining score according to the previously explained recommendation. Table 33 contains two vulnerabilities A and B with their CVSS metric’s scores as well as the calculated score of vulnerability chain B -> A.

		Vulnerability A	Vulnerability B	Chain B -> A
Exploitability Metrics	Attack Vector	Local	Network	Network
	Attack Complexity	Low	Low	Low
	Privileges Required	Low	None	None
	User Interaction	None	Required	Required
Scope Metric	Scope	Unchanged	Unchanged	Unchanged
Impact Metrics	Confidentiality	High	Low	High
	Integrity	High	Low	High
	Availability	High	Low	High

Table 33 - Example of vulnerability chaining

- **Input:**
 - Attack graph
- **Outcome**
 - List of vulnerabilities that can be chained

Example:

It is assumed that we have the following assets operating for the VTS:

²⁷ <https://www.first.org/cvss/v3.1/user-guide>

A Port Community System (PCS) application installed on a PCS OS and hosted by a PCS Web server, which exchanges data with a web Customs application. To analyze this scenario, at first the assets cyber dependencies are identified:

Source Asset	Destination Asset	Asset Cyber dependency	
		Dependency Type 1. hosting, 2. Exchange, data/information, 3. storing, 4. controlling, 5. Processing, 6. Accessing, 7. Installing, 8. Trusted 9. Connecting	Access Vector Network, Adjacent Network, Local
PCS Web Application (A _{2,1})	Operating System (OS) (A _{2,3})	installing	Local (L)
PCS Web Application (A _{2,1})	Web Server (A _{2,2})	hosting	Local (L)
PCS Web Application (A _{2,1})	Customs Web Application (A _{3,1})	exchange data/information	Network (N)

Table 34 – SCS Asset interdependencies example

In addition, the following vulnerabilities (V_i) have been identified on the SCS assets:

- V₁, V₂, and V₃ on the PCS Web Application
- V₄, V₅ on the PCS Web Server
- V₆, V₇, V₈ on the OS

To identify vulnerability chains the figure below is considered where an assets/vulnerability combinations graph is depicted. Following this figure, we can explore vulnerability sequential combinations (vulnerability chains), such as V₁ -> V₄ -> V₈, and V₃ -> V₅ -> V₆.

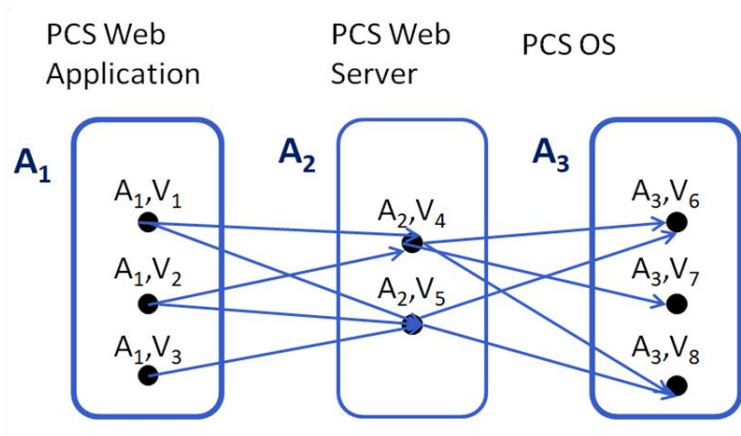


Figure 29 – Asset vulnerabilities combinations graph.

As described in step 3.1, if lower EUSCS ALs are adopted (basic or substantial) the estimation of the propagation is covered by the CVSS 3.1 score calculation. If the EUSCS AL is “High”, then a further vulnerability analysis is required to assess the cumulative and propagated impact:

To estimate the exploitation of sequential vulnerability chains, an attacker could commit on an SCS the following measurements are considered [4],[5],[6],**Error! Reference source not found.:**

- The **Individual Chain Vulnerability Level (ICVL)** which measures the probability a vulnerability *z* which resides in an asset Target Point can be exploited *assuming that the specific Vulnerability Chain is initiated from an asset entry point with vulnerability v*.
- The **Cumulative Vulnerability Level (CVL)** measures the probability that a vulnerability *z* that resides in an asset Target point can be exploited *concerning all ICVLs originated from all asset Entry Points*.

Moreover, the cumulative measurement shows how much access an asset can be within the SCS network taking into account all asset entry points [4],[5],[6],**Error! Reference source not found.:**

- The **Individual Propagated Vulnerability Level (IPVL)** measures the weakness of the **Individual Propagated Vulnerability Chain** to be exploited due to exposure of a specific vulnerability *v* in an asset entry point.
- The **Propagated Vulnerability Level (PVL)** measures the weakness of *all independent propagated vulnerability chains* to be exploited due to exposure of a specific vulnerability *v* in an asset entry point.

The propagated measurement estimates how deep in the SCS network an attacker can infiltrate starting from a specific entry point.

Step 3.6 Identification of Attack Methods & Attack Graphs

- **Scope:**

Attack vectors are the methods that attackers use to infiltrate a supply chain network. Attack vectors may take many different forms, for example:

- Compromised credentials,
- Weak and stolen credentials,
- Ransomware,
- Phishing,
- Zero-Day vulnerabilities,
- Missing or poor encryption,
- Misconfiguration,
- Trust relationships,
- Brute force attack,
- Distributed Denial of Service (DDoS).

Attack graphs represent possible paths that a potential attacker can use to intrude into a target network. In order to create an attack graph, it is necessary to analyze vulnerability information

associated with a particular asset, network topology, and reachability conditions among network hosts.

Attack graphs can be a highly effective vulnerability analysis tool, as they provide an insight into the possible behavior of the attacker, before the occurrence of an attack. They enable the identification and defense of nodes that are possibly at risk. For example, it is possible to apply graph metrics such as Page Rank [33] and to identify the node which has the highest impact on the other nodes in the graph. It means that the effect of an attack on that node would be more easily propagated to other nodes and at the same time, it means that the security officer should pay more attention to protect that particular node.

- **Input:**
 - List of all assets and their interconnections, vulnerabilities connected to those assets, and implemented controls
- **Outcome:**
 - List of attack methods applicable to given SCS
 - Attack paths for the given entry and target assets
 - Calculated scores for every asset according to selected graph metric
 - List of the most important assets in the network

Since not all vulnerabilities can or will be exploited a further analysis of the exploitability of the vulnerabilities will be considered here in order to identify all possible attacks of the SCS, their potential to be exploited and propagated through the SCS.

Step 3.7 Attack Impact

- **Scope:**

The attack impact reflects the direct consequence of a successful exploit, and the respective impact metrics represent the qualitative and quantitative consequence to the thing that suffers the impact. In the CYRENE context, this consequence refers to an impacted asset. While the vulnerable asset is typically a software application, module, driver, etc. (or possibly a hardware device), the impacted asset could be a software application, a hardware device or a network resource. This potential for measuring the attack impact of a vulnerability other than the vulnerable asset was a key feature introduced with CVSS v3.0 and re-used in CVSS 3.1.

- **Input:**

The attack impact takes into account the **Confidentiality, Integrity, and Availability metrics**. The **Confidentiality metric** measures the impact (i.e., categorical or encoded as numerical for easier representation as High (H), Low (L), None (N)) to the confidentiality of the information resources managed by a software asset due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The **Integrity metric** measures the impact (i.e., categorical or encoded as numerical for easier representation as High (H), Low (L), None (N)) to the integrity of a successfully exploited vulnerability. Integrity refers to the

trustworthiness and veracity of information. The **Availability metric** measures the impact (i.e., categorical or encoded as numerical for easier representation as High (H), Low (L), None (N)) to the availability of the impacted asset resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted asset, this metric refers to the loss of availability of the impacted asset itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted asset.

- **Outcome:**

The outcome should constrain an attack impact to a reasonable value, only when a security officer or SCS provider is confident an attacker is able to achieve. For example, let's consider a vulnerability that requires read-only permissions prior to being able to exploit the vulnerability. After successful exploitation, the attacker maintains the same level of reading access, and gains write access. In this case, only the Integrity impact metric should be scored, and the Confidentiality and Availability Impact metrics should be set as None.

Step 3.8 Systematic Documentation of Vulnerabilities

The systematic documentation of vulnerabilities will take into consideration all the identified metrics specified and reported in steps 3.1-3.6. These include the three parts of the CVSS 3.1 scoring system (i.e., Base, Temporal and Environmental metric), the list of attacks, the calculations of attack potentials, and the calculated attack impact. For reuse purposes, we will structure the documentation of vulnerabilities in an XML-based language to enable different stakeholders across different organizations to share critical security-related information in a single format, speeding up information exchange and digestion. The Common Vulnerability Reporting Framework (CVRF)²⁸ will be used as a reference format to structure the documentation of vulnerabilities in the CYRENE context. We provide an indicative template in Appendix D.

Step 3.9 Occurrence Likelihood & Impact Assessment

- **Scope:**

This step aims to estimate the attack intensity and re-calculate the SCS assets impact to deliver an overall resulting impact.

- **Input:** Impact assessment report
- **Outcome:** Lists of Resulting impact reports

²⁸ <https://www.icasi.org/the-common-vulnerability-reporting-framework-cvrf-v1-1/>

The likelihood of a threat occurring depends upon the attacker's profile. A highly capable attacker will be able to attack successfully even if the vulnerability level is "Low".

Intensity is defined according to ETSI-TVRA methodology as the metric to estimate the severity of a successful attack on an asset. Thus, the overall impact on an asset can vary concerning the intensity an attack is mounted. According to ETSI-TVRA, the summation of asset impact and attack intensity shall give the overall "Resulting Impact".

Example:

If the Attack intensity has value 2 and the asset impact has been assessed 2, then the resulting impact will be of value 3.

Step 4: Risk Assessment- Establishment of Risk

- **Scope:**
Calculate risk using the CVSS 3.1 scores of each vulnerability of all SCS assets
 - Vulnerability Level (VL) and Impact Level (IL) as a whole
 - Threat Level
 - Multiply with the Attack Potential (AP) value
- **Outcome:**
 - **SCS-asset risk Levels (RL)** for a specific threat on specific SCS-asset considering the propagation rates and attack paths
 - SCS-asset risk Levels considering **a specified AP level, assurance level and a vulnerability evaluation level (AVA_VAN.xx)**

Risk level estimates are a *how dangerous threat to a specific SCS asset* within the SCS. The individual risk metric estimates how dangerous are all threats to a specific asset.

Having estimated threat, vulnerability, and impact levels for each identified ICT asset the risk level can be calculated for each particular asset following the well-known multiplication of risk equation presented below:

$$\text{Risk Level} = \text{Threat Level} \times \text{Vulnerability Level} \times \text{Impact Level}$$

In order to include the score of the AP to risk calculation, we enhance the general multiplication risk estimation shown above by multiplying these values with the AP as shown below:

$$\text{Risk Level} = (\text{Threat Level} \times \text{Vulnerability Level} \times \text{Impact Level}) \times \text{Attack Potential}$$

To estimate the risk:

- The Threat Level is derived from step 2 (threat assessment) and it is assessed in the 5 tier qualitative scale from “Very Low” to “Very High”
- The Vulnerability Level and the Impact Level are estimated into one qualitative value using the CVSS 3.1 score and specification as a result of step 3.2
- The AP is defined according to the adopted EUSCS AL in a nominal scale basic, Enhanced –Basic, Moderate, High. To convert the AP value to a quantitative, numeric scale we use the AP scale of ISO/IEC 15408 presented in Appendix F of section 9.
- The qualitative Threat and Vulnerability-Impact values are mapped to quantitative values following Table 44 of Appendix F- III of section 9 in order to be estimated with the AP.
- In case of the EUSCS AL adopted is “High”, risk should be estimated in cumulative and propagation values [4],[5],[6],**Error! Reference source not found..**

Example:

Assuming for adopted EUSCS AL Substantial AP = Enhanced-Basic
that Threat Level = Medium, Severity Vulnerability Level (V+I) = High

Then, according to the above risk equation:

Risk Level = (Medium x High) **x Enhanced Basic**

With regards to Table 44 of Appendix G- III of section 9:

Risk Level = (0,39 x 0,69) **x 0,29**

Risk Level = 0,08 (Very Low)

Step 5: Risk Compliance to Security Assurance Certification Scheme

This step sets the following scope, input, and expected outcome.

- **Scope:**

Identified risks of Step 4 must be compliant to the Security Assurance Certification Scheme

- **Input:**

- List of SCS asset risks
- Security Assurance Certification Scheme directives

- **Expected output:**

- List of all the CYRENE measures focusing on risk compliance through security assurance certification scheme

The Security Assurance Certification scheme provides an extra layer of confidence and certification to Supply Chain members demonstrating that the Supply Chain system is in alignment with best cybersecurity practices^{29,30}. This scheme has been developed by the industry with the goal to accelerate the industry-wide improvement of cybersecurity for industrial systems. The Cyber supply chain security assurance scheme focuses on managing risks related to the people, processes, and technologies which are used to design, develop, produce, distribute, and implement hardware, software, and IT services.

The cybersecurity supply chain assurance certification scheme includes some specific directives, which need to be followed by the Supply Chain system in order to offer risk compliance³¹. These directives are presented below:

- **Secure product development**

This includes a secure development lifecycle, assessment, and testing of open source and third-party components included in SC products. Also, cybersecurity practices need to be followed by all assets that participate in SC products development.

- **Adequate security skills**

SC assets and members, i.e. developers, testers, need to have suitable and up-to-date cybersecurity skills in order to minimize risks associated with error actions.

²⁹ <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>

³⁰ https://lexparency.org/eu/32019R0881/ART_51/

³¹ <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vmware-esg-cyber-supply-chain-security-assurance-white-paper.pdf>

- **Right cybersecurity processes and procedures.**

SC components need to back their daily operations with cybersecurity best practices for risk management, threat prevention, and incident response. Also, SC IT members need to employ cybersecurity best practices for internal safety.

- **Field-level cybersecurity expertise.**

Many of the SC assets do not have the correct cybersecurity configurations of the embedded IT systems. This creates problems to the whole SC processing. Based on the above, the assets need to improve their cyber supply chain security assurance settings and they need to be updated by field-level employees or partners who can adjust SC security features and functionality upon deployment over time.

- **Strong cybersecurity customer support.**

Assets develop, distribute, and deploy their products through the SC framework. On the other hand, they need to have the right preparation for inevitable security vulnerabilities. In particular, cybersecurity supply chain assurance demands that the assets should monitor the latest attack trends and work with the greater security community to ensure timely awareness of new vulnerabilities that could impact the SC process. Once vulnerabilities are detected, assets must also have highly efficient processes for developing, testing, and distributing patches. Finally, supply chains must have a highly trained staff to guide customers through security fixes as needed.

All the CYRENE measures that focus on risk compliance through the security assurance certification scheme are presented in Table 35.

Goal	Security Assurance Certification Scheme measures
Secure product development	Follow cybersecurity practices for SC development lifecycle, assessment, and testing of activities
	Cybersecurity practices should be considered for all the contractors and the suppliers, i.e., assets that participate in SC products development.
Adequate security skills	SC assets and members must use suitable and up-to-date cybersecurity skills.
Right cybersecurity processes	SC assets must use the best cybersecurity practices during their day-to-day operations for risk management, threat prevention, and incident response.
	SC IT members must employ cybersecurity best practices for internal IT services.
Field-level cybersecurity expertise	SC vendors need to have employees with supply chain security assurance skills in order to benefit for product security features and functionality upon deployment.
	SC assets should be prepared for inevitable security vulnerabilities.

Strong cybersecurity customer support	Assets' security teams should monitor the latest attack trends and work with the greater security community to ensure timely awareness of new vulnerabilities that could impact their products.
	Detected vulnerabilities should be treated by SC assets using highly efficient processes for developing, testing, and distributing patches.
	Assets must have a highly trained staff to guide customers through security fixes.

Table 35 – CYRENE Security Assurance Certification Scheme measures.

Step 6: Risk Mitigation: Security Countermeasure Identification

The last step of the CYRENE CA methodology focuses on identifying security countermeasures for risk mitigation. Risk mitigation is the process of developing strategies and actions for lessening the negative effects and impacts of threats for a system. There are different risk mitigation strategies, which can be combined depending on the risk landscape and offering a broader practice of cybersecurity risk management. The four types of risk mitigation strategies³² are described below:

- **Risk avoidance strategy** is used by systems when the consequences are deemed too high to justify the cost of mitigating the problem. In such cases, the platform tries not to get involved in any scenario that its results can lead to cybersecurity issues.
- **Risk acceptance strategy** is based on the acceptance of specific risk for a given period due to the prioritization mitigation efforts on other risks.
- **Risk transfer strategy** is based on the sharing/transfer of the risks, which have a low probability to take place but a great impact when it takes between the different components of the supply chain structure. In such a case, the responsibility for a certain fraction of the risk is transferred to a third party, which may not be a basic role structure in the supply chain system.
- **Risk monitoring strategy** is the act of monitoring the project environment for potentially increasing impact from low-impact to high impact.

All the above strategies focus on solving the platform vulnerabilities using specific directions. The next section presents and analyses the countermeasures that can be used by the CYRENE Cybersecurity Supply Chain framework in order to mitigate the consequences of cyber security events.

Step 6.1: Countermeasures in the SCS

As presented in Appendix G, cybersecurity organizations offer various mitigation strategies for IoT platforms³³. Although it is important to prevent the presence of malicious or vulnerable content within Supply Chains, not all vulnerabilities can be eliminated. This section focuses on the countermeasures proposed within the context of CYRENE, which take place after an SC cybersecurity breach. These countermeasures can be grouped into 6 independent stages that focus on limiting the following cybersecurity issues.

- First step: Survey issue

The first step focuses on the survey about the status of Supply Chain security events. Following the discovery of the cybersecurity issue, the countermeasure that needs to take place is the investigation for internal Supply Chain weaknesses. Specifically, this runtime research will try to find out the impact of the cybersecurity issue on the critical Supply Chain components and it will identify the attacker, the security vulnerabilities from the specific issue, and, finally, possible

³² <https://accendoreliability.com/4-effective-risk-mitigation-strategies/>

³³ <https://cyberwatching.eu/risk-mitigation>

solutions. This survey will take place by specific processes into Supply Chain, which have full access to the CYRENE data management layer.

- Second step: Limit issue

This second step includes countermeasures that focus on limiting the attack that takes place within a supply chain system. The proposed countermeasures can take place concurrently or independently based on the cyberattack and the status of the SC.

- Vulnerability scan modules

A CYRENE countermeasure that focuses on limiting the consequences of security events is the implementation and integration of independent small vulnerability management modules into the Supply Chain structure. These modules will be responsible for scanning, identifying, triaging, and mitigating discovered system security events. Specifically, these modules will be intermediate components between the SC assets and the network. Based on their position, they will use vulnerability management guidelines, which will hinder access to software, operating systems, and firmware from malicious objects. In addition, when a security event in a Supply Chain framework is discovered, the vulnerability scan modules will collect all the information and they will forward it through reports to the system administrators for possible solutions. Lastly, the supply chain will also include independent mechanisms that can be used by the SC assets within their environments.

- Software/Hardware patches

Another security event countermeasure includes the existence and mapping of internal Supply Chain System processes and tools that provision and apply software/hardware patches. In particular, the CYRENE Supply Chain framework will include specific modules, i.e. simple network SC nodes, which will apply security patches to software and hardware systems on a prompt and routine schedule. This process will keep the CYRENE platform updated.

- Filtering or blocking traffic

This countermeasure includes internal Supply Chain processes that will be responsible for filtering or blocking the traffic between the assets. This process takes place through specific and predefined Supply Chain configurations, which will be established under control changes and will be mapped onto specific management components. Hence, when a serious change takes place, i.e. an asset suddenly creates great traffic in a Supply Chain, the management components will change the SC network configuration based on some pre-defined schemes in order to reduce the consequences, e.g. temporarily block all the network activities from the problematic asset. In addition, as the complete blocking of the Supply Chain nodes can lead to great issues, filtering solutions can be a possible measure to reduce the problem, i.e. deep data exchange filtering can take place for the packets/messages from the problematic nodes.

- Re-routing network traffic

The SCs maintain an internal information system about component inventory, which describes the exact status of the SC components. When the status or the behavior of a specific SC component changes, i.e. a problematic asset, the module needs to be isolated. This process can

take place by re-routing the network traffic through different routing schemes. The information about the connections of the Supply Chain structure is stored internally to SC data management layers and from where this information can be used for building different internal routes, which will be applied for changing routing schemes. In addition to the above, all the problematic modules need to be immediately isolated in order to reduce attack consequences. Finally, the asset information that is kept on the Supply Chain data management layers will be updated.

- Isolating all or parts of the compromised network

Another CYRENE countermeasure is based on the module isolation using deliberate network SC structure segmentation. Specifically, this countermeasure is based on the idea of splitting the Supply Chain system into inter-connected smaller structures, e.g. a separate network for guest users or separate networks used by different functional areas of the Supply Chain, which use different vendors to cover the network segments. As analyzed in Step 3.5, CYRENE supports graph-based clustering methodology in order to find possible paths that a potential attacker can use to intrude into the SC system. Based on this cluster information, the proposed CYRENE countermeasure will use mechanisms that remove or isolate single assets (or cluster graph-based assets) that have cybersecurity issues. Also, this countermeasure can help organizations achieve higher cybersecurity mitigation by implementing endpoint-based micro-segmentation with host-based firewalls.

- Supply Chain “reconfiguration”

Another countermeasure that focuses on reducing the Supply Chain’s issues is structure “reconfiguration”. Based on this measure, the Supply Chain has to pre-identify and establish two or more alternative assets that cover, in exactly the same way, the critical network segments. When a critical asset becomes unavailable or presents a high risk, the system should “reconfigure” its structure and the “dangerous” assets should be replaced by new “clean” assets in order to reduce, as much as possible, the expansion of the cybersecurity issue. Based on this measure, different assets increase the resilience and decrease the overall enterprise risk from vulnerabilities of a single asset in the Supply Chain.

- Impact reduction schemes

Another countermeasure that can take place in order to reduce the impact of this cybersecurity issue over Supply Chains is the identification of failover processes. Hence, when the cybersecurity issue appears, each Supply Chain will have ready pre-defined failover processes, which will describe exactly the steps that need to take place in order to reduce the impact. These processes will have come out from periodical exercises or walk-throughs into the Supply Chain framework or even with coordination with external vendors or stakeholders.

- Third step: Record issue

The third step of countermeasures focuses on mechanisms for the collection of the information that is needed to solve the issue. In particular, the Supply Chain framework should keep and store all the logs, which are produced from the different parts of the SC when a cybersecurity issue appears. This information needs to include all the data about the SC-affected systems, the compromised accounts, the disrupted services, the data and the network nodes that are affected

by the malicious object, and the amount and type of damage that took place on the SC system. All this information is collected on central SC data management structures and it is finally forwarded to the information security team, which is responsible for checking the SC status and solving the corresponding issues.

- Fourth step: Law enforcement

This step includes the measure that focuses on reporting the supply chain issues to law enforcement. When a supply chain issue occurs, then the information security team should immediately forward the issue and contact the law enforcement agencies that are established in the Supply Chain region. Once the incident is reported, the law enforcement agency should contact the media and ensure that sensitive information is not disclosed.

- Fifth step: Asset notifications

If a security issue puts the Supply Chain members' information at risk, they need to be notified. This quick response can help them to take immediate steps to protect themselves. However, if law enforcement is involved, they should advise the company as to whether or not the notification should be delayed to make sure that the investigation is not compromised. To avoid further unauthorized disclosure, the notification should not include unnecessary personal information.

- Sixth step: Issue documentation

Since cybersecurity events are becoming a way of life, it is important to develop organizational processes to learn from discovered vulnerabilities. This countermeasure includes identifying and making vulnerability mitigations available through documentation to all supply chain parts as quickly as possible (and ideally prior to or simultaneous to a disclosure). In addition, the issues should include the documentation of all the mistakes that took place with the previous attempts to solve the problem. Finally, the documentation should also be submitted to the international cybersecurity communities. The output of this step will be directed to the relevant assessment authorities and services.

All the CYRENE proposed measures are described in Table 36.

Stage	Measures	Responsible for running the measure
Survey	Internal Supply Chain weaknesses investigation	Cybersecurity processes over Supply Chain framework
Limit	Scan, identify, triage, and mitigate discovered system security events between the SC assets and the network.	SC integrated vulnerability scan modules will collect the information and they will forward the information to the system administrators.
	Provision and apply software/hardware patches	SC nodes that focus on applying security patches to software and hardware assets on a prompt and routine schedule.
	Filter or block the data traffic from problematic assets that create	Supply Chain cybersecurity processes, which will filter or block data exchange

	issues to the normal operation of Supply Chain	between “problematic” assets and the rest of CYRENE assets
	Re-route the total network traffic through routes that do not include problematic assets.	The Supply Chain data management layer will re-route the data in order to avoid cybersecurity issues using asset connection information from the databases.
	Use cluster-based information on graphs assets and isolate the problematic nodes using network SC structure segmentation.	The CYRENE processes run graph-based clustering methodology over the SC assets-nodes.
	Establish multiple alternative assets that cover exactly the same way the critical network segments. If any of the critical assets presents a risk, the supply chain structure should be reconfigured in order to reduce the cybersecurity issues.	The CYRENE Supply Chain data management layer, which will keep the information about the nature of the assets and their status.
	Analytical pre-defined schemes (describe exactly the steps) for Supply Chain system failover processes.	The CYRENE processes will focus on periodical SC walk-through and will pre-define processes to reduce the impact.
Record	Mechanisms for collecting the information (compromised accounts, the disrupted services, the affected data, and network nodes) that are affected by the malicious supply chain asset	The information is collected to the CYRENE data management layer by specific running tasks and it is forwarded to the SC information security team
Law enforcement	Mechanisms that forward the report for the supply chain issues to the corresponding law enforcement agencies.	The SC information security team should immediately forward the issue and contact the corresponding law enforcement agencies
Asset notification	Mechanisms for immediate notification of the SC assets as far as cybersecurity issues and make them take immediate steps to protect themselves.	The SC information security team should immediately forward the issue and contact all the SC assets representatives.
Issue Documentation	Mechanisms for documenting all SC mistakes and proactively ensure learning.	Internal SC security group will forward the documentation to the involved assets and the relevant authorities.

Table 36 – CYRENE Supply Chain countermeasures.

6 Conclusions

This report presents an enhanced Risk Assessment and Conformity Assessment (RCA) methodology which reports the process of Conformity Evaluation as well as the multi-level evidence-driven Supply Chain Risk Assessment. It constitutes an innovative method that aims to have a dual-use. It can be either used:

1. by BP and SCS-P to be prepared for a certification, or/and
2. by the assessors to demonstrate the validity of the claims provided in a PP.

7 References

- [1] European Parliament and Council, Regulation (EU) 2008/765 on setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, July 2008.
- [2] CYRENE H2020 project. Report 2 - A Cybersecurity Certification proposed Scheme for Supply Chain Services, 2021.
- [3] European Parliament and Council, Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), April 2019.
- [4] Kalogeraki, E.-M., Papastergiou, S., Mouratidis, H., Polemi N., (2018) "A novel risk assessment methodology for SCADA maritime logistics environments", Applied Sciences, MDPI AG, Switzerland, 8(9): 1477, ISSN: 2076-3417, <https://doi.org/10.3390/app8091477Mentzer>, John T. Supply chain management. Sage, 2001
- [5] Papastergiou S. and Polemi N., (2017). "MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology", Proceedings of World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2017), In: Yang X.S., Nagar A., Joshi A. (eds) Smart Trends in Systems, Security and Sustainability, "Lecture Notes in Networks and Systems" (LNNS), Springer, Online ISBN: 978-981-10-6916-1, Vol 18, pp. 1-9.
- [6] Schauer, S., Polemi, N. & Mouratidis, H. MITIGATE: a dynamic supply chain cyber risk assessment methodology. J Transp Secur 12, 1–35 (2019). <https://doi.org/10.1007/s12198-018-0195-z>
- [7] Common Criteria for Information Technology Security Evaluation (CC) (2017), Part 1: Introduction and general model, v3.1, Rev.5, CCMB-2017-04-001
- [8] Cord Bartels (Coordinator), ENISA AHWG on Risk Assessment, 2020
- [9] K. Kioskli and N. Polemi, "A Socio-Technical Approach to Cyber-Risk Assessment", International Journal of Electrical and Computer Engineering, Vol.14(10), 2020
- [10] NIST Special Publication 800-30 Rev.1 (2012) "Guide for Conducting Risk Assessments" Available online: <https://doi.org/10.6028/NIST.SP.800-30r1>
- [11] ENISA, "Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS", v1.0, July 2020, Online available: <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>, accessed on April 29 2021.
- [12] CYRENE H2020 project. Report 1 - Supply Chain Analysis and Requirements, 2021.
- [13] The Directive on security of network and information systems (NIS 2 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>.
- [14] A. Annane, N. Aussenac-Gilles, and M. Kamel., "BBO: BPMN 2.0 based ontology for business process representation", in 20th European Conference on Knowledge Management, 2019.
- [15] Amina Annane, Mouna Kamel, Nathalie Aussenac-Gilles, "Comparing Business Process Ontologies for Task Monitoring," in *International Conference on Agents and Artificial Intelligence (ICAART 2020)*, 2020
- [16] Hinkelmann, Knut & fanesi, Diego & Cacciagrano, Diletta, "Semantic Business Process Representation to Enhance the Degree of BPM Mechanization - An Ontology," 2015.)

- [17] Sanfilippo, Emilio & Borgo, Stefano & Masolo, Claudio, "Events and Activities: Is there an Ontology behind BPMN?," *Frontiers in AI and its applications*, 2014.
- [18] Adamo G., Borgo S., Di Francescomarino C., Ghidini C., Guarino N., Sanfilippo E.M., "Business Processes and Their Participants: An Ontological Perspective," *Lecture Notes in Computer Science*, vol 10640, 2017.
- [19] Doynikova, Elena & Fedorchenko, Andrey & Kotenko, Igor, "Ontology of Metrics for Cyber Security Assessment," in *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019.
- [20] Bowersox, D. J. (1997). "Integrated Supply Chain Management: A Strategic Imperative" In *Annual Conference Proceedings, Council of Logistics Management*, Chicago, Illinois, pp 181–189.
- [21] ENISA report (2015) "Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward", Online available: <https://www.enisa.europa.eu/publications/sci-2015>
- [22] N. Polemi, P. Kotzanikolaou, S. Papastergiou (2016) "Design and Validation of the MEDUSA Supply Chain Risk Assessment Methodology and System", *Elsevier International Journal of Critical Infrastructure Protection (IJIP)*, 14(1), 1-39
- [23] 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
- [24] White, D. R., & Borgatti, S. P. (1994). Betweenness centrality measures for directed graphs. *Social networks*, 16(4), 335-346.
- [25] ETSI, TS. "102 165-1 V5. 2.3 (2017-10) CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability." *Risk Analysis (TVRA)*. Standard, European Telecommunications Standards Institute (ETSI) (2017).
- [26] Bodeau, D., Fabius-Greene, J., & Graubart, R. (2011). *How Do You Assess Your Organization's Cyber Threat Level?*. MITRE CORP MCLEAN VA.
- [27] Polatidis, N.; Pimenidis, E.; Pavlidis, M.; Papastergiou, S.; Mouratidis, H., (2018). "From Product Recommendation to Cyber-Attack Prediction: Generating Attack Graphs and Predicting Future Attacks". In *Evolving Systems*; Pavlidis; Springer: Berlin, Germany, pp. 1–12
- [28] Singh, Umesh Kumar, Chanchala Joshi, and Dimitris Kanellopoulos. "A framework for zero-day vulnerabilities detection and prioritization." *Journal of Information Security and Applications* 46 (2019): 164-172.
- [29] Kaur, Ratinder, and Maninder Singh. "Automatic evaluation and signature generation technique for thwarting zero-day attacks." *International Conference on Security in Computer Networks and Distributed Systems*. Springer, Berlin, Heidelberg, 2014.
- [30] Holm, Hannes. "Signature based intrusion detection for zero-day attacks:(not) a closed chapter?." *2014 47th Hawaii international conference on system sciences*. IEEE, 2014.
- [31] Hammarberg, David. "The best defenses against zero-day exploits for various-sized organizations." *SANS Institute InfoSec Reading Room* 21 (2014).
- [32] Kaur, Ratinder, and Maninder Singh. "Efficient hybrid technique for detecting zero-day polymorphic worms." *2014 IEEE International Advance Computing Conference (IACC)*. IEEE, 2014.
- [33] Gleich, D. F. (2015). PageRank beyond the web. *Siam Review*, 57(3), 321-363.

- [34] Available Online: <https://cybercoretech.com/buyer-beware-do-you-know-how-much-supply-chain-assurance-is-enough/> last accessed 11-09-2
- [35] Available Online:: <https://securityboulevard.com/2020/11/cyber-security-assurance-levels-in-the-automotive-supply-chain/EUCS> – Cloud Services Scheme (<https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>)
- [36] Public Consultations on Cybersecurity Candidate Schemes, (<https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes>)

[37]

8 Glossary & Examples

This section contains the glossary used in this report. The current glossary is an excerpt of the online glossary available and continuously updated on the CYRENE project website³⁴. 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.

The glossary is split into two parts to distinguish all terms related to business and supply chain concepts (see section 8.1) from terms referring to security and certification concepts (see section 8.2) that are considered important in the context of the proposed EUSCS and CYRENE RCA methodology. The reader is recommended to consult it to better comprehend the content of the report.

The current glossary can be considered an enhancement of the definition of terms provided in Annex A of the ENISA report “Methodology for Sectoral Cybersecurity Assessments”³⁵ as it supplements the specification of some terms provided and introduces additional terms related to supply chain and business-oriented concepts, information security, cybersecurity, security certification, and assurance.

³⁴ <https://www.cyrene.eu/glossary/>

³⁵ <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

8.1 Supply chain and business concepts

This section provides the glossary of this report related to supply chain and business concepts.

Term	Abbreviation	Definition	Reference	Example	Notes / Remarks
Supply Chain and Business Concepts					
Entity	-	Any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.	NIS 2 Directive		
Essential entity	-	Any entity of a type referred to as an essential entity in Annex I of NIS 2 Directive.	NIS 2 Directive		
Operator of Essential Service	OES	Any operator that resides to the Member States when laying down security and incident reporting requirements for the types of essential services referred to Annex I of NIS 2 Directive.	NIS 2 Directive		NIS 2 Directive essential services are also presented in xx of this report.
Important entity	-	Any entity of a type referred to as an important entity in Annex II of NIS 2 Directive.	NIS 2 Directive		
Operator of Important Service	OIS	Any operator that resides to the Member States when laying down security and incident reporting requirements for the types of important services referred to Annex II of NIS 2 Directive.	NIS 2 Directive		NIS 2 Directive important services are also presented in xx of this report.

Supply Chain Service	SCS	It is considered the service that entails a linked 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.	ISO 28000:2007	The vehicle transport service is a massively complex system with numerous players for the manufacturing, shipment and delivery of various types of vehicles.	SCS business partners are the main actors for the provision of the SCS and they are considered in CYRENE under the following perspectives: 1. SCS Commercial Business Partner, 2. SCS Governmental Business Partner, 3. SCS provider.
International Supply Chain Service	-	1. A supply chain that at some point crosses an international or economic border 2. A SCS that consists of EU and non-EU SCS-BP.	1. ISO 28001:2007 2. EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology.		
SCS Business Partner	SCS-BP	1. Those contractors, suppliers or service providers that an organization contracts with to assist the organization in its function as an "Organization in the Supply Chain". 2. A stakeholder that participates in the provision of the supply chain service".	1. ISO 28001:2007 2. EU H2020-ICT-02-2020 project "CYRENE"		CYRENE delves into a service approach definition, whereas ISO 28001 defines it from a supply chain perspective.
SCS provider	SCS-P	The main actor in the supply chain (originator) that identifies all business partners (of type B, C, D), SCS processes / sub-processes to be followed, agreements (e.g., protection profile) and records (e.g., self-assessment conformity statements).	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology	in the vehicle transport SCS, the automotive industry and all its third parties/sub-contractors belong in this type.	(Business Partner A)
SCS Commercial Business Partner	-	Participating in the provision of the supply chain service, undertaking an operational role, related to the operation of the	EU H2020-ICT-02-2020 project "CYRENE": EUSCS,	in the vehicle transport SCS, the importers, transport/maritime companies and any third-party	(Business Partner B)

		supply chain service, including ordering, transporting, importing, and other processes.	CYRENE RCA Methodology	commercial partner reflect this category.	
SCS Governmental Business Partner	-	Participating in the provision of the supply chain service, undertaking an operational role, related to the operation of the supply chain service, including ordering, provisioning, storing, and other processes.	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology	in the vehicle transport SCS, the Ministry of Transport, Customs and other related authorities fall in this category.	(Business Partner C)
SCS Self-Assessor	-	Every business partner (A or B or C) is allowed to undertake the compliance role which covers the activities related to the verification of compliance to standards and regulations, including documentation, self-assessment, interfaces with third party assessor or CABs (if needed) and management of EU statements of conformity (for SCs with AL Basic).	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology		(Business Partner D)
SCS Assessor	-	can be either the SCS Self-Assessor (Business Partner D) that is every business partner (A or B or C) who undertakes the compliance role which covers the activities related to the verification of compliance to standards and regulations, including documentation, self-assessment, interfaces with third party assessor or CABs (if needed) and management of EU statements of conformity (for SCs with assurance level Basic).	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology		

Mutual Recognition Agreement	SCS-MRA	It is considered an agreement between the SCS business partners (EU and non-EU business partners) which is set up to establish and support the mutual recognition of the EU SCS certification schema (EUSCS) with third countries.	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology		
SCS process	-	It is a group of interconnected sets or interacting activities, capable of turning inputs into outputs for the provision of the SCS	ISO/IEC 27000:2018	Within the vehicle transport service performance, a transportation order or ship formalities arrangements are considered SCS processes.	
SCS asset	-	1. 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 20000-1: 2018] 2. Information asset: Anything that has value to an individual, an organization or a government. [ISO/IEC 27032: 2012].	1. ISO/IEC 27001: 2013 2. ISO/IEC 20000-1: 2018	an asset can be for example: an application server, a presence sensor, a mobile or a municipal building, a Human Machine Interface (HMI), a vehicle or a vessel traffic web application.	The only difference of the two terms is that the second makes provision for individuals and the separation of governments from organizations.
Information Security Management System	ISMS	Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.	ISO/IEC 27000:2018, ISO/IEC 27001		

SCS evaluation view	-	It is considered the different options that can be utilized to assess the SCS using three different conformity assessment profiles according to the different views 'process' (overall business), 'holistic-technical', 'sector-specific' the SCS can be represented or described.	EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology		
Security Declaration	-	A documented commitment by a business partner, which specifies security measures implemented by that business partner, including, at a minimum, how goods and physical instruments of international trade are safeguarded, associated information is protected and security measures are demonstrated and verified.	ISO 28001:2007		
Statement of Applicability	-	document that contains the selection and implementation of controls in order to assist with compliance requirements.	ISO/IEC 27000:2018		
Statement of Application	-	The organization in the supply chain shall describe the portion of the international supply chain that it claims to be in compliance with this standard in a Statement of Application.	ISO 28001:2007		

Table 37 – Extracted from Supply Chain and Business Concepts CYRENE online glossary.

8.2 Security and certification concepts

This section provides the glossary of this report related to security and certification concepts.

Term	Abbreviation	Definition(s)	Reference	Example(s)	Notes/ Remarks
Security Concepts					
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		
Information security	-	Preservation of the CIA triad (Confidentiality, Integrity and Availability) of information involving also the ensurance of other properties such as authenticity, accountability, non-repudiation, and reliability.	ISO/IEC 27000:2018		

<p>Vulnerability</p>	<p>-</p>	<p>1. Weakness in the TOE that can be used to violate the SFRs in some environment. 2. Weakness of an asset or control that can be exploited by one or more threats. 3. In the context of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service (functional) that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.</p>	<p>1. ISO/IEC 15408-1:2009 (CC) , 2. ISO/IEC 27000:2018, 3. ISO/IEC 29147:2018</p>	<ul style="list-style-type: none"> • Poor encryption in digital signatures. • Target Row Refresh (TRR), aka the TRRespass issue (CVE-2020-10255) • The DNS bugs (CVE-2020-11901) 	<p>A term 'vulnerability' is functioning in different context in ISO/IEC 15408 as it reflects the perspective of the TOE (*see line 94). - Multiple vulnerabilities can impact a supply chain as a whole, compromising multiple interconnected assets by exploiting a series of assets' vulnerabilities. See more: "Hacking the Supply Chain" [https://i.blackhat.com/USA-20/Wednesday/us-20-Oberman-Hacking-The-Supply-Chain-The-Ripple20-Vulnerabilities-Haunt-Tens-Of-Millions-Of-Critical-Devices.pdf]</p>
<p>-Potential (unknown) Vulnerability</p>	<p>-</p>	<p>1. Potential: Suspected, but not confirmed, weakness 2. Unknown: There are reports of impacts that indicate a vulnerability is present, but that the cause of the vulnerability is unknown or they may differ on the cause or impacts of the vulnerability. Reporters are uncertain of the true nature of the vulnerability, and there is little confidence in the validity of the reports.</p>	<p>1. ISO/IEC 15408-1:2009 (CC), 2. CVSS v3.1 NIST NVD (FIRST)</p>	<p>An unknown/zero day vulnerability could be an adversary that sneaks in an asset through a backdoor that was left unlocked by accident.</p>	<p>Suspicion is by virtue of a postulated attack path to violate the SFRs. A sub-category of this is the "zero-day" vulnerability, which is related to a security flaw in the software that is known to the software vendor, but with no patch in place to fix the flaw.</p>
<p>-Confirmed Vulnerability</p>	<p>-</p>	<p>Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the affected code has confirmed the presence of the vulnerability.</p>	<p>CVSS v3.1 NIST NVD (FIRST)</p>	<p>A confirmed vulnerability example is the vulnerability of Microsoft Teams Remote Code Execution, which was published on 11/11/2020.</p>	
<p>-Exploitable Vulnerability</p>	<p>-</p>	<p>Weakness in the TOE <i>that can be used to violate the SFRs in the operational environment</i> for the TOE.</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>		

-Residual Vulnerability	-	Weakness <i>that cannot be exploited in the operational environment for the TOE, but could be used to violate the SFRs</i> by an attacker with greater attack potential than is anticipated in the operational environment for the TOE.	ISO/IEC 15408-1:2009 (CC)		
Vulnerabilities Measurement/Labelling	-	Vulnerabilities are defined in terms of an attribute and the method for quantifying it	ISO/IEC 27000:2018, ISO/IEC/IEEE 15939:2017	<ul style="list-style-type: none"> - Common Vulnerabilities and Exposures - TOE-relevant CVE vulnerabilities - Common Weakness Enumeration - Common Vulnerability Scoring System - CVSS basic metric - CVSS temporal metric - CVSS environmental metric 	
Severity of vulnerability	-	The severity of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context-dependent.	NIST SP 800-30 Rev.1, 2012	CVSS 3.1	
Vulnerability Severity Level	VSL	<ol style="list-style-type: none"> 1. Qualitative severity rankings of "None" (0.0), "Low" (0.1-3.9), "Medium" (4.0-6.9), "High" (7.0-8.9), and "Critical" (9.0-10.0). 2. It measures the probability an attacker can successfully reach and exploit a specific vulnerability (either confirmed or unknown) taking into account temporal vulnerability characteristics and the impact according to the user's environment to a specific asset. 	<ol style="list-style-type: none"> 1. CVSS v3.1, 2. EU H2020-ICT-02-2020 project "CYRENE": CYRENE RCA Methodology 		

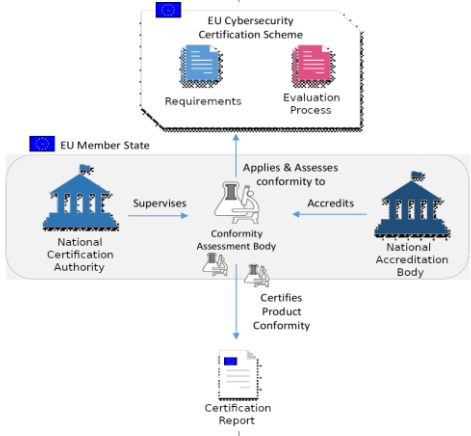
<p>Common Vulnerabilities and Exposures</p>	<p>CVE</p>	<p>1. A nomenclature and dictionary of security-related software flaws. 2. A list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.</p>	<p>1. NIST SP 800-126 Rev. 2, 2. MITRE: online available: https://cve.mitre.org/</p>	<p>The confirmed vulnerability example of Microsoft Teams Remote Code Execution has the CVE (Id) "CVE-2020-17091"</p>	<p>(1) CVEs are designated by the CVE Numbering Authorities (CNAs), namely organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. The MITRE Corporation functions as Editor and Primary CNA. (2) NIST repository for vulnerabilities NVD is utilized to identify vulnerability on an asset. Useful links to search for CVEs: https://nvd.nist.gov/vuln, https://www.cvedetails.com/</p>
<p>Common Weakness Enumeration</p>	<p>CWE</p>	<p>A community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.</p>	<p>[MITRE] online available: https://cwe.mitre.org/</p>	<p>CWE-20 Improper Input Validation: the asset does not validate or incorrectly validates input that can affect the control flow or data flow of a program. When software fails to validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.</p>	<p>CWE is assigned by MITRE. This leads to a mapping of vulnerabilities to the related threats.</p>

Common Vulnerability Scoring System	CVSS	The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. It mainly consists of three metric groups: Base, Temporal, and Environmental.	FIRST CVSS v3.1 Specification , Rev.1 online available: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf , [MITRE] https://nvd.nist.gov/vuln-metrics/cvss	For instance, the confirmed vulnerability "CVE-2020-17091" Microsoft Teams Remote Code Execution has <i>Basic score metrics</i> = 7.8 : Exploitability<AV= Local/AC=Low PR=None / UI=Required <i>Impact</i> <C= High I=High A=High <i>Temporal score metrics</i> = 6.8 : E= Unproven RL=Official fix RC=Confirmed	(1) CVSS is designed to measure the severity of a vulnerability. The score leverages Basic, Temporal and Environmental) CVSS is designed to measure the severity of a vulnerability. The score leverages Basic, Temporal and Environmental Metrics. (2) CVSS has been recognized as an international standard for scoring vulnerabilities.
Vulnerability Chain		Weaknesses existing in a group of assets that can be exploited by threats starting from an entry point in a successive manner which allows a progressive security impact or consequences to these assets that terminate(s) to a target point.	ANSI/API, 2013		
Attacker (adversary/ threat agent)	-	1. Adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities [NIST SP 800-30 Rev 1, 2012]. 2. Attacker: an actor who attempts to gain access to behaviors or resources that are outside of the product's intended control sphere for that actor [MITRE glossary]. 3. Threat agent: entity that can adversely act on assets [ISO/IEC 15408-1:2009].	1. NIST SP 800-30 Rev 1, 2012, 2. MITRE glossary online available: https://cwe.mitre.org/documents/glossary , 3.. ISO/IEC 15408-1:2009	For instance, an attacker can be a disgruntled employee (insider), a hacktivist, a cybercriminal, a terrorist group, a pirate or a hijacker, a cyber vandal, a government/industry spy.	
Attack	-	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.	ISO/IEC 27000:2018	Attack on a SCADA software (cyber), attack on a cruise terminal (physical).	
Cyber attack	-	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.	NIST SP 800-30 Rev 1, 2012	Man-In the-Middle attack cinderella attack ransomware attack	

Attack path (attack model/attack pattern/attack vector)	-	1. Attack path: Steps that a threat takes or may take to plan, prepare for, and execute an attack [API standard 780]. 2. Attack pattern: abstracted approach utilized to attack software [ISO/IEC TR 20004:2015]. 3. Attack vector: path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome [ISO/IEC 27032:2012].	1. API standard 780, 2. ISO/IEC TR 20004:2015, 3. ISO/IEC 27032:2012	attack path to compromise a CCTV system of an enterprise: compromise an e-mail account to gain access to an employee's workstation of an enterprise and after take advantage of a CCTV server that is installed in the workstation operating system	
Attack Potential (means, skills, opportunities)	-	(1) Measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation. (2) Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.	1. ISO/IEC 15408-1:2009 (CC) 2. ISO/IEC 27032:2012		- Attack potential can be estimated <i>Basic</i> or <i>Enhanced-basic</i> or <i>Moderate</i> or <i>High</i> . - 'Attack potential' is used to prove or deny the TOE security functionality remains in the secure state regardless if the vulnerability is identified or discovered.
Likelihood of occurrence	-	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Determining the likelihood of threat events causing adverse impacts.	NISTIR 7621 Rev. 1, 2016, CNSSI 4009-2015, NIST SP 800-30 Rev 1, 2012		
Threat	-	Potential cause of an unwanted incident, which can result in harm to a system or organization.	ISO/IEC 27000:2018	Example are a signature spoofing by key theft on an e-mail operating system and buffer overflow in Local Command-Line Utilities on an admin operating system.	
Threat assessment	-	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	CNSS, 2015, NIST SP 800-30 Rev.1, 2012		
Threat level	-	The expected probability of occurrence of a threat to a cyber asset.	EU H2020-DS-2014-01 project "MITIGATE"		

Security impact analysis	-	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.	NIST SP 800-37 Rev.2, 2018		
Impact	-	The result of an unwanted incident	ISO/IEC PDTR 13335-1		
Impact level	-	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.	NIST SP 800-37 Rev.2, 2018		
Risk Assessment	RA	1. The overall process of risk identification, risk analysis and risk evaluation 2. the process of identifying, estimating, and prioritizing information security risks.	1. ISO/IEC 27000:2018, 2. NIST SP 800-30 Rev.1, 2012		
Risk assessor	-	The individual, group, or organization responsible for conducting a risk assessment.	NIST SP 800-30 Rev.1, 2012		
Level of risk	-	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.	ISO/IEC 27000:2018		
Residual risk	-	Risk remaining after risk treatment. Residual risk can contain unidentified risk. It can also be referred to as "retained risk".	ISO/IEC 27000:2018		
Risk treatment	-	Process to modify risk.	ISO/IEC 27000:2018		
Risk mitigation	-	Risk treatments that deal with negative consequences.	ISO/IEC 27000:2018		

Control	-	<p>1. Measure that maintains and/or modifies risk [ISO 31000: 2018; ISO/IEC 27000:2018].</p> <p>2. Controls include any process, policy, device, practice, or other actions which modify risk. It is possible that controls not always exert the intended or assumed modifying effect. [ISO/IEC 27000:2018]</p>	<p>1. ISO 31000: 2018 1.,2. ISO/IEC 27000:2018</p>	<p>Control – term used in [CSA, Art. 52.4]: “The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.”</p> <p>This term can be seen as equivalent to the Security Functional Requirements (SFRs) defined in ISO15408.</p>	
Control objective	-	Statement describing what is to be achieved as a result of implementing controls.	ISO/IEC 27000:2018		
Security control	-	Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.	NIST SP 800-30 Rev.1, 2012 (FIPS 199, CNSSI No. 4009)		
Risk management	RM	<p>1. A systematic performance of policies, procedures and practices management on communicating, consulting activities, establishing the context and controlling identifying, analysing, evaluating, treating, monitoring and reviewing risk.</p> <p>2. Coordinated activities to direct and control an organization with regard to risk.</p>	<p>1. ISO/IEC 27000:2018 2. ISO 31000:2018</p>		
Risk owner	-	Person or entity with the accountability and authority to manage a risk.	ISO/IEC 27000:2018		
Security Management	SM	Security management includes all the activities and practices implemented by organizations to manage security risks, threats, and impacts. These activities and practices should be coordinated in a systematic, and optimized manner.	ISO 28000:2007		

Security management objective	-	Specific outcome or achievement required of security in order to meet the security management policy. It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.	ISO 28000:2007		
Security management policy	-	Overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.	ISO 28000:2007		
Certification concepts					
Conformity Assessment	CA	<ol style="list-style-type: none"> The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. A procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. 	<ol style="list-style-type: none"> Regulation (EC) No 765/2008 Regulation (EU) 2019/881 (EU Cybersecurity Act) 		
Conformity Self-assessment	-	An action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.	Regulation (EU) 2019/881 (EU Cybersecurity Act)		
Certification	-	Certification of a management system, such as the environmental management system, quality management system or information security management system of an organization, is one means of providing assurance that the organization has implemented a system for the management of the relevant aspects of its	ISO/IEC 17021-1:2015		

		activities, products and services, in line with the organization's policy and the requirements of the respective international management system standard.			
Certification scheme	-	Conformity assessment system related to management systems to which the same specified requirements, specific rules, and procedures apply.	ISO/IEC 17021-1:2015	EUCC, national schemes. (e.g. SOGIS-MRA, included NL (NLNCSA), FR (ANSSI), SE (FMV), DE (BSI).	
Accreditation	-	Attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.	Regulation (EC) No 765/2008		
Common Criteria	CC	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.	ISO/IEC 15408-1:2009 (CC)		"Common Criteria" is the ISO/IEC 15408-1:2009.
European Cybersecurity Certification Scheme	EUCC	A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.	Regulation (EU) 2019/881 (Cybersecurity Act)		It is an umbrella, which replaces SOG-IS. It covers the certification of ICT products, using the ISO/IEC 15408 (CC) and it is the foundation of a EU Cybersecurity certification framework. There are no examples of schemes according to ECCS yet - the EU is in the process of creating.
Conformance claim		The conformance claim indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation.	Common Criteria for Information Security Conformity Evaluation (CC) (Part I: Introduction and general model (2017), v3.1 Rev. 5		

<p>Conformity Assessment Body</p>	<p>CAB</p>	<p>A body that performs conformity assessment activities including calibration, testing, certification and inspection</p>	<p>Regulation (EC) No 765/2008</p>	<p>One that:</p> <ul style="list-style-type: none"> • Applies and assesses conformity to EU Cybersecurity Certification Scheme. • Certifies product conformity by a certification report. 																																																																																																																																																																																																																																																							
<p>Assurance Level</p>		<p>A basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned</p>	<p>Regulation (EU) 2019/881 (EU Cybersecurity Act)</p>		<ul style="list-style-type: none"> • Level 1: Little or no confidence; • Level 2: Some confidence; • Level 3: High confidence; 																																																																																																																																																																																																																																																						
<p>Evaluation Assurance Level</p>	<p>EAL</p>	<p>The definition of a scale for measuring assurance for component Targets of Evaluation (TOEs)</p>	<p>ISO/IEC 15408-3:2008 (CC)</p>	<table border="1"> <thead> <tr> <th rowspan="2">Assurance class</th> <th rowspan="2">Assurance Family</th> <th colspan="7">Assurance Components by Evaluation Assurance Level</th> </tr> <tr> <th>EAL1</th> <th>EAL2</th> <th>EAL3</th> <th>EAL4</th> <th>EAL5</th> <th>EAL6</th> <th>EAL7</th> </tr> </thead> <tbody> <tr> <td rowspan="7">Development</td> <td>ADV_ARC</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ADV_FSP</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>5</td> <td>6</td> </tr> <tr> <td>ADV_IMP</td> <td></td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> <td></td> <td></td> </tr> <tr> <td>ADV_INT</td> <td></td> <td></td> <td></td> <td>2</td> <td>3</td> <td>3</td> <td></td> </tr> <tr> <td>ADV_SPM</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>1</td> <td>1</td> </tr> <tr> <td>ADV_TDS</td> <td></td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> </tr> <tr> <td>ADV_TSS</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td rowspan="5">Guidance documents</td> <td>ASG_OPE</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ASG_PNE</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ALC_CMC</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>4</td> <td>5</td> <td>5</td> </tr> <tr> <td>ALC_CNS</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>5</td> <td>5</td> </tr> <tr> <td>ALC_DEL</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td rowspan="5">Life-cycle support</td> <td>ALC_DVS</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> <td></td> </tr> <tr> <td>ALC_FLR</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ALC_LSD</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td></td> </tr> <tr> <td>ALC_TAT</td> <td></td> <td></td> <td>1</td> <td>2</td> <td>3</td> <td>3</td> <td></td> </tr> <tr> <td>ASE_CCL</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td rowspan="7">Security Target evaluation</td> <td>ASE_ECP</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ASE_INT</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ASE_OBU</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>ASE_PNE</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>ASE_SPM</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ASE_TSS</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ATE_COV</td> <td></td> <td>1</td> <td>2</td> <td>2</td> <td>3</td> <td>3</td> <td></td> </tr> <tr> <td rowspan="3">Tests</td> <td>ATE_SPT</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>ATE_FUN</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> </tr> <tr> <td>ATE_IMP</td> <td></td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>3</td> </tr> <tr> <td rowspan="2">Vulnerability assessment</td> <td>AVA_VAN</td> <td>1</td> <td>2</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>5</td> </tr> </tbody> </table> <p><i>Assurance Levels (ISO/IEC 15408-3:2008 (CC))</i></p>	Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level							EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	Development	ADV_ARC	1	1	1	1	1	1	1	ADV_FSP	1	2	3	4	5	5	6	ADV_IMP		1	1	2	2			ADV_INT				2	3	3		ADV_SPM						1	1	ADV_TDS		1	2	3	4	5	6	ADV_TSS								Guidance documents	ASG_OPE	1	1	1	1	1	1	1	ASG_PNE	1	1	1	1	1	1	1	ALC_CMC	1	2	3	4	4	5	5	ALC_CNS	1	2	3	4	5	5	5	ALC_DEL		1	1	1	1	1	1	Life-cycle support	ALC_DVS		1	1	1	2	2		ALC_FLR								ALC_LSD		1	1	1	1	2		ALC_TAT			1	2	3	3		ASE_CCL	1	1	1	1	1	1	1	Security Target evaluation	ASE_ECP	1	1	1	1	1	1	1	ASE_INT	1	1	1	1	1	1	1	ASE_OBU	1	2	2	2	2	2	2	ASE_PNE	1	2	2	2	2	2	2	ASE_SPM		1	1	1	1	1	1	ASE_TSS	1	1	1	1	1	1	1	ATE_COV		1	2	2	3	3		Tests	ATE_SPT		1	1	1	1	1	1	ATE_FUN		1	1	1	1	2	2	ATE_IMP		1	2	2	2	2	3	Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level																																																																																																																																																																																																																																																									
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7																																																																																																																																																																																																																																																			
Development	ADV_ARC	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ADV_FSP	1	2	3	4	5	5	6																																																																																																																																																																																																																																																			
	ADV_IMP		1	1	2	2																																																																																																																																																																																																																																																					
	ADV_INT				2	3	3																																																																																																																																																																																																																																																				
	ADV_SPM						1	1																																																																																																																																																																																																																																																			
	ADV_TDS		1	2	3	4	5	6																																																																																																																																																																																																																																																			
	ADV_TSS																																																																																																																																																																																																																																																										
Guidance documents	ASG_OPE	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ASG_PNE	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ALC_CMC	1	2	3	4	4	5	5																																																																																																																																																																																																																																																			
	ALC_CNS	1	2	3	4	5	5	5																																																																																																																																																																																																																																																			
	ALC_DEL		1	1	1	1	1	1																																																																																																																																																																																																																																																			
Life-cycle support	ALC_DVS		1	1	1	2	2																																																																																																																																																																																																																																																				
	ALC_FLR																																																																																																																																																																																																																																																										
	ALC_LSD		1	1	1	1	2																																																																																																																																																																																																																																																				
	ALC_TAT			1	2	3	3																																																																																																																																																																																																																																																				
	ASE_CCL	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
Security Target evaluation	ASE_ECP	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ASE_INT	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ASE_OBU	1	2	2	2	2	2	2																																																																																																																																																																																																																																																			
	ASE_PNE	1	2	2	2	2	2	2																																																																																																																																																																																																																																																			
	ASE_SPM		1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ASE_TSS	1	1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ATE_COV		1	2	2	3	3																																																																																																																																																																																																																																																				
Tests	ATE_SPT		1	1	1	1	1	1																																																																																																																																																																																																																																																			
	ATE_FUN		1	1	1	1	2	2																																																																																																																																																																																																																																																			
	ATE_IMP		1	2	2	2	2	3																																																																																																																																																																																																																																																			
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5																																																																																																																																																																																																																																																			
	<p>Vulnerability Analysis AVA_VAN</p>	<p>AVA_VAN</p>	<p>An assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs. It deals with the threats that an attacker will be able to discover flaws allowing unauthorised access to data and functionality, allowing the ability to interfere with or alter the TSF, or interfere</p>	<p>ISO/IEC 15408-3:2008 (CC)</p>	<p>Levelling is based on an increasing rigour of vulnerability analysis by the evaluator and increased levels of attack potential required by an attacker to identify and exploit the potential vulnerabilities.</p> <ul style="list-style-type: none"> • AVA_VAN.1 Vulnerability survey (TOE Resistance against Basic Attack Potential); • AVA_VAN.2 (Unstructured) Vulnerability analysis (TOE Resistance against Basic AP); 																																																																																																																																																																																																																																																						

		with the authorised capabilities of other users. Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE. Assessment of development vulnerabilities is covered by the assurance family AVA_VAN.		<ul style="list-style-type: none"> • AVA_VAN.3 Focused vulnerability analysis (TOE Resistance against Enhanced-Basic AP); • AVA_VAN.4 Methodical vulnerability analysis (TOE Resistance against Moderate AP); • AVA_VAN.5 Advanced methodical vulnerability analysis (TOE Resistance against High AP). 	
Security objective		<ol style="list-style-type: none"> 1. Statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions. 2. Information security objective: Objectives that are set by the organization, consistent with the information security policy, to achieve specific results. 	<ol style="list-style-type: none"> 1. ISO/IEC 15408-1:2009 (CC) , 2. ISO/IEC 27000:2018 		cf. EU Cybersecurity Act 2019/881 (Article 51) on Security objectives of European cybersecurity certification schemes
Security Requirements	ASE_REQ	The security requirements consist of two groups of requirements: a) the security functional requirements (SFRs) b) the security assurance requirements (SARs)	ISO/IEC 15408-1:2009 (CC)		
Security Functional Requirements	SFR	A translation of the security objectives for the TOE into a standardised language	ISO/IEC 15408-1:2009 (CC)		
Security Assurance Requirements	SAR	A description of how assurance is to be gained that the TOE meets the SFRs	ISO/IEC 15408-1:2009 (CC)		
Security function	SF	Function that implement the security requirements.	ISO/IEC 15408 -2:2008 (CC)		
Target of Evaluation	TOE	A set of software, firmware, hardware and/or process possibly accompanied by guidance	ISO/IEC 15408-1:2009 (CC)	<ul style="list-style-type: none"> • A software application • An operating system; • A software application and an operating system; • A software application in combination with an operating system and a workstation; • An operating system in combination with a workstation; • A smart card integrated circuit; 	<p>- TOE shall be the ICT product as a whole or the elements of the ICT product.</p> <p>- While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.</p>

				<ul style="list-style-type: none"> • The cryptographic co-processor of a smart card integrated circuit; • A Local Area Network including all terminals, servers, network equipment and software; • A database application excluding the remote client software normally associated with that database application; • A supply chain. 	As far as ISO/IEC 15408 is concerned, the precise relation between the TOE and any IT products is only important in one aspect: the evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product.
Protection Profile	PP	Implementation-independent statement of security needs for a TOE type.	ISO/IEC 15408-1:2009 (CC)		<p>As a Protection Profile is not written for a specific product, in many cases only a general idea can be given of the available hardware/software/firmware. In some other cases, e.g. a requirements specification for a specific consumer where the platform is already known, (much) more specific information may be provided.</p> <p>All vendors must agree for the PP doc, which describes the security functions of the TOE, threats, etc. [https://www.commoncriteriaportal.org/pps/]</p>

Table 38 – Certification and Security Concepts of the updated CYRENE online glossary.

9 Appendices

Appendix A: Security Declaration & statement of Application (SDA) –template

The implementation of the CYRENE RCA methodology is bound with a signed Security Declaration and statement of Application (SDA) (cf. section 4.3) between all business partners that will be involved in the assessment process of the SCS-TOE. The structure of the SDA is herein presented:

1. **The scope and the boundaries of the SCS-TOE and of the assessment process are set.** Identify briefly the scope of the SCS-TOE and what will be gained from this evaluation, etc.; for further details, a reference to the SCS-TOE's overview content is required (in case a Conformity Assessment process is undertaken). In addition, SCS-BPs *have reached a consensus* on the risk level(s) of the SCS-TOE that they wish to achieve (the security level is reported referring to the SCS-TOE corresponding section, where an explicit description will be carried out).
2. **Identify accepted certifications within the entities involved in the SCS-TOE,** pertaining to the certifications of SCS assets involved for the provision of the underlined SCS
3. **Identify security plans** (OSP: Organisational Security Plans), policies, and countermeasures implemented within the boundaries of the SCS-TOE, i.e. declaration of implemented security controls and the level of their implementation on the underlined SCS assets referring to controls certificates documentation that an entity may have obtained, i.e. vendor certified, penetration testing certification, assets redesign, assets' hardening, including vendors/manufactures certifications (Reference to the respective section of the SCS-TOE whether a Conformity Assessment process is undertaken)
4. **Assign in high-level security requirements, security objectives, the security target, and the security problem,** namely, declare that all SCS-BPs have agreed upon developing/conducting an assessment on the claims of the Protection Profile (PP) (reference to the PP) and agreed to undertake the commitment to map them with vulnerabilities and implemented controls to identify security gaps.
5. **All business partners declare their commitment to undertaking appropriate security controls** (whether required) in order to reach the SCS desired security level (which they have agreed upon)
6. **Additional conventions and privacy considerations** upon the SCS-TOE and the evaluation process (whether will be a risk assessment or a conformity assessment) may be assigned here (that could be referred to as the conformance claim).

In the following, a proposed template for the SDA is presented. Nevertheless, this document is indicative and can be re-adjusted according to each specific case.

**SECURITY DECLARATION AND STATEMENT OF APPLICATION
(SDA)**

The current Security Declaration and statement of Application (hereafter referred to as "SDA") is made effective as of the following date _____ by and between the following business partners of the Supply Chain Service - Target of Evaluation (hereafter referred to as "SCS-TOE"):

Business Partner A (hereafter referred to as "Secured Party" A)

Business Partner B (hereafter referred to as "Secured Party" B)

Business Partner C (hereafter referred to as "Secured Party" C)

.....

- PART A -

The Secured Parties of this document **agree/declare/reached consensus upon** the following:

- the selected SCS-TOE (providing a short description)
- the designated SCS-provider (hereafter referred to as "SCS-P");
- the purpose of the assessment (Risk Assessment or Conformity Assessment);
- the conditions subject to the recognition of certificate (indicating the certification scheme that will be followed);

- the conditions of the consistent application of the criteria and methods between evaluation and certification scheme;
- the assurance level (hereafter referred to as “AL”) of certificate of the applied security certification scheme that will be adopted including existing limitations (if any);
- the designated assessor (in case of a Conformity Assessment performance);
- the assigned security requirements, security objectives, security target and security problem;
- on the specified risk level(s);
- rest content included in the current document

In addition, all Secured Parties **declare their commitment** upon:

- developing/ assessing the SCS Protection Profile (hereafter referred to as “SCS-PP”) [SCS-PP must be referred];
- mapping the SCS-TOE assets with vulnerabilities and implemented controls, to identify security gaps;
- undertaking appropriate controls wherever required to reach the previously defined security level;
- they have provided all the appropriate documentation of their organization that justifies all the above (included hereafter in the “Annex”)

- PART B -

Additional conventions and privacy considerations.

.....

Herewith, all the Secured Parties confirm that they have read and understood the entire SDA, acknowledge it as fully binding upon them. The undersigned, herewith, take the responsibility of informing the persons concerned accordingly.

IN WITNESS WHEREOF, the parties are bound by the SDA as follows:

_____ *Secured Party A (Organization name/Name of representative)*

Date Signature

_____ *Secured Party B (Organization name/Name of representative)*

Date Signature

_____ *Secured Party C (Organization name/Name of representative)*

Date Signature

.....
.....

Personal Data Handling Policy

The SDA applicants agree to share all personal information given through this application process, such as name, address and so on which will be protected under GDPR (EU) 2016/679 regulation.

- ANNEX -

The current SDA must be accompanied by documentation including but not limited to the following:

- Asset inventory of involved assets per organization or Statement of Applicability (SOA) (ISO 28001, ISO/IEC 27001)
- Business Partner Security Control Plan (SCP)
- Organizational Risk Assessment Report
- Implementation of Business continuity
- Implementation of Service continuity
- Implementation of the Security control plan
- Security control certification (whether exists)
- Other vendors/manufacturers certifications (whether exists)
- Penetration Testing certification (whether exists)

Appendix B: Protection Profile for an SCS-template

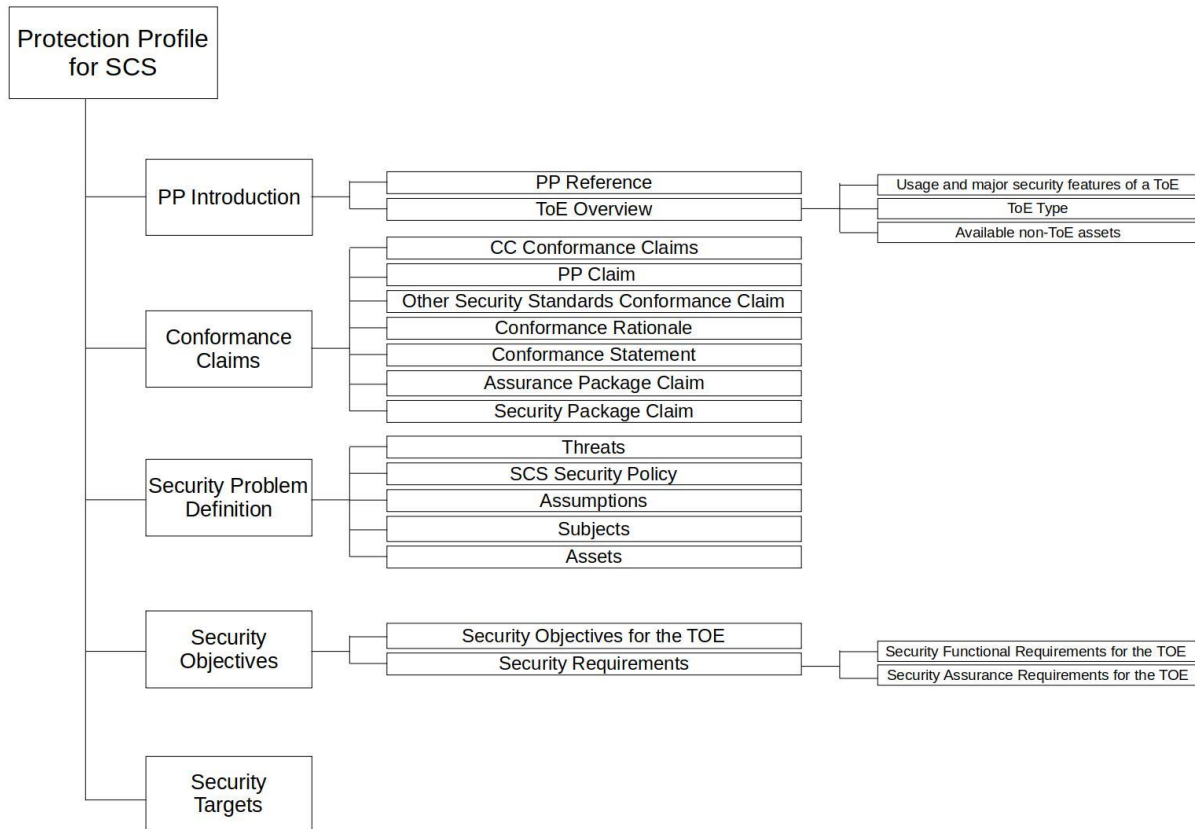


Figure 30 – CYRENE Protection Profile according to Common Criteria.

The following template illustrates a structure to develop the SCS Protection Profile (SCS-PP) which is in line with the proposed EUSCS (CYRENE Report 2). The SCS-PP shall follow the content of the PP defined in the Common Criteria (CC).

1. PP Introduction

This section presents the Common Criteria (CC) PP that is established as a basis for the development of Security Targets (STs) in order to perform a certification of a Supply Chain Service (SCS), the Target of Evaluation (TOE).

1.1. PP reference

In this section, a clear PP reference that identifies that particular PP is presented. A typical PP reference consists of title, version, authors and publication date, e.g. “TOE1 PP: Vehicle Transport Service from Business Perspective, version 1.1, Business Providers, February 10th, 2021”.

This reference is unique so that it can be distinguished from other PPs or different versions of the same PP.

1.2. TOE overview

The goal of this section is to present a brief overview of the ToE, such as its usage, major security features, type, as well as the major non-ToE assets available to this. This information is aimed at professionals or potential consumers who may either use this PP in designing a SCS, adapting parts or procedures of this ToE or looking for evaluated SCS to meet their security needs. The exact and complete description of the ToE can be found in section 4 of the current document.

1.2.1 Usage and major security features of a TOE

The description of this part aims to give a general idea of what this TOE can be used for and what is capable of, security-wise.

1.2.2. TOE Type

This subsection is to identify the general type of the TOE, e.g. SCS.

1.2.3. Available non-TOE assets

In this subsection, all the additional hardware/software/firmware, services or data that a TOE may rely on, which are related to the SCS without being part of that specific TOE, are described.

E.g. Vehicle Transport Service (VTS) has many procedures, such as port call requests. In the sector specific TOE (TOE III) this process will be reported in the context of VTS, but there is no interest in evaluating the process per se.

2. Conformance Claims

This section describes how the ST conforms to the CC and Packages.

2.1. CC Conformance Claims

This section presents the CC methodology that will be used in conformance claims. Conformance to ETSI methodology will also be examined in this part.

2.2. PP Claim

In this section, conformance claims to a protection profile is presented. SCS will be tested against a PP that defines how they should operate.

2.3. Other Security Standards Conformance Claim

This section presents all the Security Standards that this SCS is compliant to, apart from CC and ETSI methodologies, which are described in section 2.1.

2.4. Conformance Rationale

In this subsection it shall be demonstrated that the security requirements and objectives of a ST are equivalent or more restrictive than this PP.

The goal of this paragraph is to enable trustworthiness and marketing advantage in the SCS, especially for non-EU partners.

2.5. Conformance Statement

In this section, it is determined by the PP authors the allowed type of conformance (“strict” or “demonstrable”) of the ST to the PP and clarified that all business partners that are involved with this SCS shall comply with this.

2.6. Assurance Package Claim

In this section, the Assurance Levels (AL) are being identified. E.g. for TOE I, AL is basic. An approach on how to evaluate the assurance requirements (AVA_VAN). Specific assurance requirements are presented in 4.2.2.

2.7. Security Package Claim

In this section, an approach on how to evaluate the security requirements is presented.

3. Security Problem Definition

This chapter describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, SCS security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

3.1. Threats

In this section, threats, attackers, and attack potential will be estimated. E.g. an attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

3.2. SCS Security Policy

The SCS security policy describes the controls to be implemented by the business partners, addressing all the security functional requirements to be implemented by a TOE.

3.3. Assumptions

The usage assumptions that are applicable to this analysis are, for instance all cryptography implemented in the assets involved in TOE II will meet the requirements listed in this PP-Module.

3.4. Subjects

The types of subjects that are identified in a PP could be:

- an external business partner that is using TOE III who can be associated with one of the SCS partners
- administrators of SCS business partners who are responsible for operating TOE (I, II, III)

3.5. Assets

In this section, the assets of the TOEs under evaluation that need to be protected are described:

- for TOE I: Business processes
- for TOE II: SCS processes and ICT assets
- for TOE III: Sector-specific (Automotive sector) within the SCS and ICT assets

4. Security Objectives

This section defines the set of security objectives to be satisfied by the TOE in response to the problem defined by the security problem definition. The security objectives are to be fulfilled by a TOE claiming conformance to a PP.

4.1. Security Objectives for the TOE

In this section, the security objectives set for the TOE are for instance ensuring protected storage of SCS. For doing so, what is needed is to address the issue of loss of confidentiality of SCS business partners' data. This involves encrypting data to prevent unauthorized access to SCS data.

4.2. Security Requirements

This chapter specifies the security functional and assurance requirements that must be satisfied by the TOE.

4.2.1. Security Functional Requirements for the TOE

The security functional requirements are specified in the section. The PP-Configuration defines a baseline set of security functional requirements for SCS applications that specifically implement file encryption. File encryption is the process of encrypting individual files or sets of files (or volumes, or containers, etc.) on an end-user device and permitting access to the encrypted data only after proper authentication is provided. Encryption products that conform to this PP-Module must render information inaccessible to anyone that does not have the proper authentication credential.

4.2.2. Security Assurance Requirements for the TOE

In this section, assurance should be provided that developers' claims about security features of the TOE are valid and have been tested against the CC.

5. Security Targets

The STs shall be reviewed. The ST Evaluation shall include functional testing and penetration testing.

6. Reference

PP-Configuration for Application Software and File Encryption Version 1.0, Published on January 31, 2020, https://www.commoncriteriaportal.org/files/ppfiles/cfg_app-fe_v1.0-vr.pdf.

BSI-CC-PP-0056-V2-2012 for Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (BSI),
https://www.commoncriteriaportal.org/files/ppfiles/pp0056_V2a_pdf.pdf.

ISO/IEC 15408: 2008, 2009, Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria).

Appendix C: SCS inventory -template

The SCS inventory will keep records for Hardware and Software Assets (including Inventory and Controls). The type of information that we will maintain per asset is, as follows:

ID	Name	Description	Asset_Cost	Type	Editor	IP_Addresses
1	SCADA	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level supervision of machines and processes.	VH	Computer/Server	HARDWARE	192.168.X.X
2	System Administrator	A person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.	H	Organizational/Personnel	GENERIC	
...

Table 39 – SCS assets inventory (ISMS) template.

Attributes are clarified, as follows:

- ID: Unique identifier in the SCS inventory
- Name: Asset name
- Description: Asset description describing what the asset is
- Asset_Cost: Categorical data w.r.t. cost from VL, L, H, to VH
- Type: Type of asset
- Editor: HARDWARE, GENERIC, SOFTWARE
- IP_Address: The IP address that the asset is exposed

Appendix D: SCS Criticality -templates for SCS Business Partners

I. SCS process criticality – template

The following template shall be filled by the SCS-BPs to identify the SCS process criticality when running the CYRENE RCA methodology.

Question A				
Importance of the SCS process for the provision of the SCS in terms of SCS, Integrity or Availability (CIA)?				
In case the SCS process loses its Confidentiality, Integrity or Availability (CIA) it does not affect negatively the provision of the SCS		In case the SCS process loses its Confidentiality, Integrity or Availability (CIA) it affects negatively the provision of the SCS		
Very Low	Low	Medium	High	Very High
Question B				
Is there a backup/business continuity/disaster plan for the SCS process or an alternative SCS process in case of disruption or cancellation?				
Yes		No		
Question C (if only Question B is "Yes" and adopted EUSCS Assurance Level (AL) is "High")				
Is the backup plan for the SCS process or the alternative SCS process sufficient for the normal execution of the SCS?				
Yes		No		

Table 40 –SCS process criticality template.

II. SCS Business Partners importance to the SCS process – template

The following template shall be filled by the SCS-BPs to identify the Business Partners' importance for the normal execution of an SCS process.

	Impact on the SCS process execution				
	Very Low	Low	Medium	High	Very High
Business partner A					
Business partner B					
Business partner C					
Business partner D					

Table 41 –SCS Business Partners (SCS-BPs) assessment to the execution of the SCS process (template).

Appendix E: An introduction to BPMN and ontology

This appendix reviews the main concepts behind OntoCyrene. The rest of this chapter is dedicated to the concept of Business Process Model and Notation (BPMN) and the Ontology. The main contributions in the literature are reviewed at the end of the chapter.

Main standards and frameworks

I. Business Process Model and Notation (BPMN)

One of the perspectives that is considered in the asset modelling is business driven perspective. Business process is at the heart of this perspective. Therefore, finding a standard for modelling business processes is a crucial task.

In order to model the business process, there is a number of standards and languages. The most popular ones are UML, BPMN, EPC and CMMN.

In the Cyrene project, BPMN was used as the basis for modelling the business process. This is due to the fact that BPMN is a de-facto standard for business process representation. BPMN brings a uniform notation to visually model the steps of a business process from end to end. BPMN is proposed by the Object Management Group (OMG³⁶).

The concept of the process is at the core of BPMN. A process describes a sequence or flow of activities in an organization with the objective of carrying out work.

In BPMN a process is modelled as a graph of elements, including Activities, Events, Gateways, and Sequence Flows that define finite execution semantics. Processes can be defined at any level from enterprise-wide processes to processes performed by a single person.

To better understanding of BPMN, Figure 31 depicts the main elements of BPMN with their graphical symbols. The depicted classification in Figure 31 presents main elements in three categories: Flow Object, Data Object and Connecting Object.

³⁶ <https://www.omg.org/spec/BPMN/2.0>

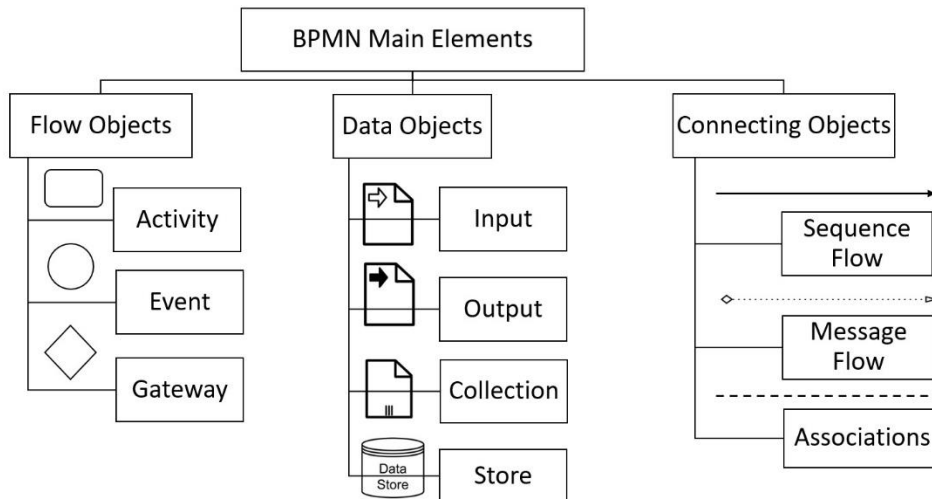


Figure 31 – BPMN 2.0 main elements.

Flow Objects defines the behaviour of the business process and consists of three elements including **Activity**, **Event** and **Gateway**.

An **Activity** is a work which is performed within a business process. An activity can be atomic or compound. The types of activities that are a part of a process are: Task, Sub-Process, and Call Activity.

Event is something that “happens” during the course of a process. Event affects the flow of the process and can be used to describe the event-driven process like **start event** (which indicate where a process will start), **intermediate event** (which indicate where something happens somewhere between the start and end of a process) and **stop event** (which indicate where a path of a process will end).

Gateway provides mechanism to control the sequence flow of the process. It implements gating checkpoint which allows/disallows passage through itself. Four types of gateways have been defined in OntoCyrene including exclusive gateway, inclusive gateway,

- **Exclusive Gateway** can be defined as diverging or converging block. Diverging exclusive gateway is the diversion point in sequence flow of a process and it is used to create alternative paths within a process flow. Converging exclusive gateway is used to merge alternative paths.
- **Inclusive Gateway** can be defined in both diverging and converging modes. Diverging inclusive gateway provides an alternative but also parallel paths within a process flow but converging inclusive gateway merges a combination of alternative and parallel paths.
- **Parallel Gateway** is used to combine parallel sequence flows without checking any conditions.
- **Event-Based Gateway** provides a branching checkpoint in the process where the alternative paths that follow the gateway are based on events that occur, rather than the evaluation of expressions.

Data object provides information about what activities need to be performed and/or what activities produce. It has four elements: **Data Input**, **Data Output**, **Data Store**, and **Data Collection**.

Connecting Objects make connection between flow objects. Three connecting objects are as follows:

- **Sequence Flow** is used to show the order that activities will be performed in a Process
- **Message Flow** is used to show the flow of Messages between two Participants that are prepared to send and receive them
- **Association** is used to annotate BPMN graphical elements in order to link information and artifacts with them.

Using the above-mentioned elements, any process can be formally modelled using BPMN.

II. *Ontology*

Semantic Web structure consists of layers which proposed by Professor Tim Berners Lee in 2001. Figure 32 demonstrates the software stack of the semantic web. As illustrated, ontology is placed at the heart of structure. The word ontology is derived from two Greek words: Onto -which means being - and Logia - which means discourse in the form of written or spoken. Ontology plays an important role to achieve interoperability and communication among software systems.

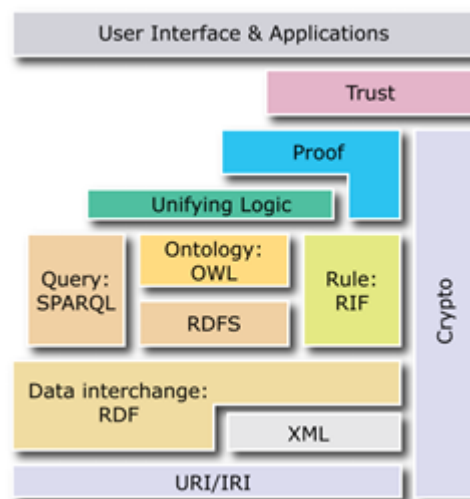


Figure 32 – Proposed stack for Semantic Web by W3C.

As depicted, the stack consists of a number of building blocks. The ontology relies on the number of them such as RDF, RDFS and SPARQL. In the rest of this sub section these components will be discussed briefly.

Resource Description Framework (RDF) was developed to standardize the definition and using of metadata. RDF designed to represent information in a flexible way. Expressing information using RDF makes it possible to exchange the information between applications without loss of meaning. RDF offers a graph data model to represent machine understandable metadata for resources. Graph data is a collection of triples, each consisting of a subject, a predicate and an object. RDF is constructed by a set of those triples.

RDFS is constructed based on the RDF and is recommended by W3C since 2004. It includes the mentioned triple <Subject, Predicate, Object>. RDFS is facilitated by some features like Object Oriented paradigm (class, subclass, and inheritance etc.). These changes make the relations in RDFS less dependent on concepts and make it better choice for definition and classification.

At the top of the RDFS, World Wide Web consortium (W3C) proposed a more powerful language to describe and publish Semantics in 2004 called Ontology Web Language (OWL). OWL was based on two previous efforts for creating ontology language. These two efforts were DARPA Agent Markup Language (DAML) and Ontology Inference Layer (OIL). According to the mentioned characteristics for RDF and RDFS, OWL was designed to fill the gap for expressing meaning and semantics in an effective way thus OWL goes beyond these languages in terms of ability to represent machine interpretable content.

In terms of rules and reasoning in semantic web, there are several efforts aiming at building rule-based standards for ontology such as RuleML³⁷ and SWRL³⁸. RuleML builds modular and hierarchical specification for different types of rules comprising facts, queries, integrity constraints, derivation, production and reaction rules and transformations from/to other rule standards. On the other side, Semantic Web Rule Language (SWRL) has become the de facto standard rule language for developing rules on the Semantic Web since 2004. It was designed as a language by combining the sub language of OWL and Rule Mark-up Language to work only with OWL rules language. Another rule-based language in semantic web stack is SPARQL which is a query language for RDF. SPARQL can be used to express queries across RDF and RDF graphs.

³⁷ The Rule Mark-up Initiative can be accessible at: www.ruleml.org

³⁸ Semantic web Rule Language accessible at : www.w3.org/Submission/SWRL

Appendix F: Vulnerability Documentation- template

As reported, regarding Vulnerability Documentation, we will follow and enrich if needed the Common Vulnerability Reporting Framework (CVRF)³⁹ which is an XML-based language that is designed to provide a standard format for the dissemination of security-related information. Current security documents such as vulnerability reports and security bulletins from different vendors (e.g., CISCO, Microsoft, etc.) are produced in different formats that typically require manual consumption. CVRF provides a standard, rigid language that document producers (such as vendors, coordinators, and researchers) can use to generate a document in a common and expected format. Document consumers (such as security practitioners and administrators) will be able to parse and understand this format. Additionally, because CVRF is XML-based, document consumers will be able to submit CVRF documents to automated parsers and processors for tasks such as priority escalation, trouble ticketing, patch management, and cataloging. A CVRF Mindmap⁴⁰ of version 1.1 snippet is presented in the following figure. A white paper providing all the details about the attributes of CVRF v1.1⁴¹ clarifies the decisions made about the inclusion of new elements since v1.0 of 2011.

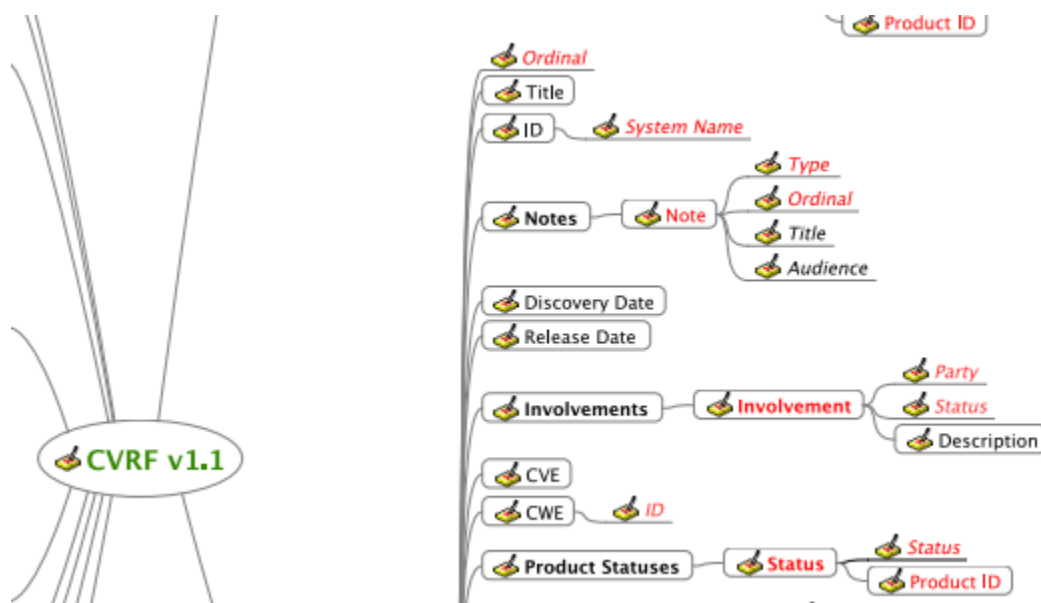


Figure 33 – CVRF 1.1 Attributes.

³⁹

http://stix.mitre.org/language/version1.2/xsddocs/XMLSchema/extensions/vulnerability/cvrf_1.1/1.2/cvrf_xsd.html

⁴⁰ <https://www.icas.org/wp-content/uploads/2015/06/CVRF-mindmap-1.1.pdf>

⁴¹ https://www.icas.org/wp-content/uploads/2015/06/ICASI_CVRF1.1_White_Paper.pdf

An indicative example is provided to show how we will proceed in structuring Vulnerabilities Documentation based on CVRF by using a real XML reported by CISCO which documents multiple vulnerabilities in OpenSSL, as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<cvrf:cvrfdoc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:cvrf-common="http://docs.oasis-open.org/csaf/ns/csaf-
cvrf/v1.2/common" xmlns:cvrf="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/cvrf">
  <cvrf:DocumentTitle>Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March
  2021</cvrf:DocumentTitle>
  <cvrf:DocumentType>Cisco-Security-Advisory</cvrf:DocumentType>
  <cvrf:DocumentPublisher Type="Vendor">
    <cvrf:ContactDetails>Emergency Support:
    +1-877-228-7302 (toll-free within North America)
    +1-408-525-6532 (International direct-dial)
    Non-emergency Support:
    Email: psirt@cisco.com
    Support requests that are received via e-mail are typically acknowledged within 48
    hours.</cvrf:ContactDetails>
    <cvrf:IssuingAuthority>Cisco product security incident response is the responsibility of the Cisco
    Product Security Incident Response Team (PSIRT). The Cisco PSIRT is a dedicated, global team that
    manages the receipt, investigation, and public reporting of security vulnerability information that is
    related to Cisco products and networks. The on-call Cisco PSIRT works 24x7 with Cisco customers,
    independent security researchers, consultants, industry organizations, and other vendors to identify
    possible security issues with Cisco products and networks.
    More information can be found in Cisco Security Vulnerability Policy available at
    http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html</cvrf:IssuingAuthority>
  </cvrf:DocumentPublisher>
  <cvrf:DocumentTracking>
  <cvrf:Identification>
    <cvrf:ID>cisco-sa-openssl-2021-GHY28dJd</cvrf:ID>
  </cvrf:Identification>
  <cvrf:Status>Final</cvrf:Status>
  <cvrf:Version>1.20</cvrf:Version>
  <cvrf:RevisionHistory>
    <cvrf:Revision>
      <cvrf:Number>1.0</cvrf:Number>
      <cvrf:Date>2021-03-25T16:09:54</cvrf:Date>
```

Figure 34 – CISCO XML vulnerabilities indicative report.

Appendix G: Scoring and Measurements

I. Assurance Components – Attack Potential Scale

ISO/IEC 18045 identifies the following quantitative values for estimating the level of the AP required to implement a threat scenario. AP is mapped to the assurance components of the AVA_VAN class according to the two views (SCS-TOE resistance and SCS-TOE failure of resistance)

Attack Potential (AP) required to implement a threat scenario Qualitative values	Attack Potential (AP) required to implement a threat scenario Quantitative values	SCS-TOE resistance to an attacker with AP	Meets assurance components	Fail to meet components
Basic	0-9	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
Enhanced Basic	10-13	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
Moderate	14-19	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
High	20-24	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
Beyond High	=>25	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Table 42 – Quantitative and qualitative values of AP according to ISO/IEC 15408.

II. Individual IA, Scale

The attack intensity shall be calculated to the assessed impact to estimate the overall SCS asset impact. According to ETSI-TVRA, the following table shall be filled by the SCS-P or the assessor ranging from value 1 to value 3. If the resulting impact is calculated in a value above 3 it keeps the value 3.

Asset impact	Attack intensity	Resulting impact
2	2	3
1	0	1
3	1	3
1	1	2

Table 43 – Estimation of the overall Resulting impact.

III. Conformity Assessment Quantitative and Qualitative Scales

The current scale presents the CYRENE probability scale that can be used to measure risk, threat, vulnerabilities, and asset SCS criticality.

CYRENE Probability scale				
Qualitative value	Range	Numeric Value	AP	EUSCS AL
Very Low	0.00-0.19	0,09	Basic	Basic/Substantial
Low	0.20-0.39	0,29	Enhanced-Basic	Substantial
Medium	0.40-0.59	0,39	Moderate	High
High	0.60-0.79	0,69	High	High
Very High	0.80-1.00	0,90	Beyond High	N/A

Table 44 – CYRENE probability scale.

IV. SCS Criticality Scales

In this appendix, two tables are presented that are utilized to identify the CYRENE SCS criticality scale, depicted in Table 7 of section 2. The first table shows a mapping of SCS Provider (SCS-P) to the industry sectors of essential and important services presented in the NIS 2 Directive **Error! Reference source not found..** The second table displays the CYRENE assurance of SCS in a qualitative scale mapped to the assurance level of the proposed EUSCS (see CYRENE [2]) to clarify the SCS criticality.

SCS Provider (SCS-P)	Industry sectors of essential and important services defined by NIS 2 Directive (Annexes I and II)
Operator of Important Services (OIS)	1. Postal and courier services, 2. Waste Management, 3. Manufacture, production, and distribution of chemicals, 4. Food production, processing, and distribution, 5. Manufacturing, 6. Digital Providers
Operator of Essential Services (OES)	1. Energy (electricity, oil, gas), 2. Transport (air, rail, water, road), 3. Banking, 4. Financial market infrastructures, 5. Health (including hospitals and private clinics), 6. Drinking water supply and distribution, 7. Waste Water, 8. Digital infrastructure, 9. Public Administration, 10. Space

Table 45 – Mapping SCS-P to the industry sectors of essential and important services of NIS 2 Directive *Error! Reference source not found..*

Assurance Level (EUSCS)	CYRENE Assurance of SCS	CYRENE SCS Criticality in qualitative values
Basic	SCS is neither an essential nor important service according to NIS 2 Directive Error! Reference source not found.. The SCS-P is not a provider of essential services (according to NIS).	Very Low
Substantial	SCS is an important service according to NIS 2 Directive. The SCS-P is a provider of important services (according to NIS).	Low
Substantial	SCS is an essential service according to NIS and European (the SCS-BPs involved are only EU) The SCS-P is a provider of essential services (according to NIS).	Medium

High	SCS is an international essential NIS service (including non EU SCS business partners) and the SCS-Provider is a provider of essential (international) services	High
High	SCS is a military/defense service. The SCS provider is a provider of essential service (national security, law enforcement)	Very High

Table 46 – SCS criticality qualitative scale of the CYRENE enhanced Risk and Conformity Assessment (RCA) methodology.

V. Assurance Levels

Supply chain assurance focuses on discovering and mitigating vulnerabilities, which are based on uncovered backdoors that allow an attacker to change SC configuration. SC assurance increases the flexibility and the automation of risk mitigation and helps to satisfy compliance mandates for the SC framework

Cybersecurity assurance levels are a classification system that outlines the requirements that should be met to ensure security at each stage of the Supply Chain framework. These levels are not technical specifications or requirements, but rather they are cybersecurity goals that are supported with justification and measured against a technical metric [35],[36].

Cybersecurity certification schemes⁴² specify one or more of the following assurance levels: basic, substantial, or high. The security requirements are provided in the relevant SC cybersecurity certification scheme, including the corresponding security functionalities and the corresponding depth of the evaluation that the SC service is to undergo.

- Basic Assurance level
 - A basic assurance level certificate provides assurances that SC products, services, and processes meet the corresponding security requirements, including security functionalities, which are evaluated at a level intended to minimize the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken include at least a review of technical documentation.
- Substantial Assurance level
 - A substantial assurance level provides services with security requirements, including security functionalities, that have been evaluated at a level intended to minimize the known risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities that are undertaken include at least the following: a review to demonstrate the absence of

⁴² https://lexparency.org/eu/32019R0881/ART_52/

publicly known vulnerabilities and testing to demonstrate that the SC services correctly implement the necessary security functionalities.

- High Assurance level
 - A high assurance level provides security requirements and security functionalities that have been evaluated at a level intended to minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities include at least a review to demonstrate the absence of publicly known vulnerabilities; a test to demonstrate that the SC services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing.

An SC certification scheme includes 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.

Appendix H: Cybersecurity Mitigation Strategies

This appendix section focuses on strategies that are proposed by various organizations for helping security professionals to mitigate cyber security incidents caused by cyber threats. First, the Australian Cyber Security Centre (ACSC) mitigation strategies, which are considered to be the new cyber security baseline for all Australian organizations, are presented. Next, the NSA cyber security mitigation strategies counter a broad range of exploitation techniques to minimize mission impact and they are analyzed [34],[35].

- **Australian Cyber Security Centre (ACSC) mitigation strategies**

The Australian Cyber Security Centre (ACSC) developed prioritized strategies to help cyber security professionals to mitigate cyber security incidents⁴³. The ACSC splits the mitigations strategies into five groups: mitigation strategies to prevent malware delivery and execution, mitigation strategies to limit the extent of cybersecurity incidents, mitigation strategies to detect cyber security incidents and respond, mitigation strategies to recover data and system availability and mitigation strategies to prevent malicious insiders.

As no single mitigation strategy is guaranteed to prevent cyber security incidents, ACSC recommends the Australian organizations to implement eight essential mitigation strategies as a baseline in order to increase their system security. These strategies belong into three of the sub-classifications that ACSC proposed.

- ✓ Mitigation strategies to prevent malware delivery and execution
 - Application whitelisting
 - Application whitelisting protects against malware executing on systems, ensuring that only authorized applications can run. It can also help identify attempts to execute malicious code on systems, and it generally prevents the installation or use of unauthorized applications.
 - Patch applications
 - Whenever a security flaw for a software code is uncovered, a “patch” is the software issued by a company in order to prevent exploitation by hackers. Applying patches in a timely way is critical to ensuring the security of systems. Also, the security of the system is the highest when the latest version of the application code is used.
 - Configure Microsoft Office macro settings
 - Microsoft Office applications execute macros to automate routine tasks. However, macros can contain malicious code resulting in unauthorized access to sensitive information as part of a targeted cyber intrusion. To manage the correct use of macros within an organization, all macros should be reviewed by an independent party to their developer and be assessed to be safe before being approved for use within the organization.
 - User application hardening

⁴³ <https://accendoreliability.com/4-effective-risk-mitigation-strategies/>

- Hardening applications that run on workstations is an important part of reducing the risk. Workstations are often targeted by adversaries using malicious web pages, malicious email attachments, and removable media with malicious content in an attempt to extract sensitive information. Based on the above, users need to configure properly web browsers and Java applications, which are particularly attractive to cyber adversaries seeking unauthorized access to computer networks. Also, it is important that Java applications are secured without impeding important business functions.
- ✓ Mitigation strategies to limit the extent of cybersecurity incidents
 - Restrict administrative privileges
 - Users with administrative privileges for operating systems and applications are able to make significant changes to IoT configurations and operations, bypassing critical security settings and accessing sensitive information. Restricting administrative privileges reduces the potential damage of an adversary's malware, minimizing the chances of them gaining full access.
 - Patch operating systems
 - One of the essential eight mitigation strategies is to specifically patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. The latest operating system version should be used, and unsupported versions should be avoided.
 - Multi-factor authentication
 - Multi-factor authentication helps to prevent a cyber adversary from gaining access to a device or network and accessing sensitive information. The Australian Cyber Security Centre (ACSC) recommends that multi-factor authentication is implemented for users using remote access solutions, users performing privileged actions, and users accessing sensitive information.
- ✓ Mitigation strategies to recover data and system availability
 - Daily backups
 - There should be daily backups of important new/changed data, software, and configuration settings, to ensure that information can be accessed again following a cyber security incident (e.g., after a ransomware attack). Also, restoration tests should take place at frequent time periods and when IT infrastructure changes.

The increasing prevalence of cybercrime leads organizations to be proactive in mitigating potential cyber threats. The ACSC essential eight directives provide a baseline of essential mitigation strategies, which can help corporations to secure their systems. Strategies may be implemented to an initial level, increasing the maturity of their implementation over time.

- **National Security Agency mitigation strategies**

NSA's cybersecurity mitigation strategies counter a broad range of exploitation techniques. These mitigation strategies focus on impact minimization and promote a defense-in-depth security posture. In more details, NSA proposes [32] ten generic strategies for securing all the kind of platforms from cyber security issues.

- ✓ **Update and Upgrade Software Immediately**

- All available software updates and upgrades should be applied. Both processes should be extended as far as possible and the update services should be automated and provided directly from the vendor. The automation is important as threat actors study patches and create exploits, often soon after a patch is released.
- ✓ **Defend Privileges and Accounts**
 - The proposed solution should use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. The system should offer procedures to securely reset credentials, e.g., passwords. Also, the privileged accounts and services should be controlled as it is a possible target administrator credential to access high-value assets, and to move laterally through the network.
- ✓ **Enforce Signed Software Execution Policies**
 - The platform should use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. A list of trusted certificates should be maintained in order to prevent and detect the use and injection of illegitimate executables. Applications should be used with signed software execution policies in conjunction with a secure boot capability, so that it can assure system integrity.
- ✓ **System Recovery Plan**
 - A system recovery plan should be defined in order to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs so that to ensure continuity of operations due to unexpected events. Also, for additional protection, backups should be encrypted, stored offline when possible, and support complete recovery and reconstitution of systems and devices. The backup plan should be performed and tested periodically in order to accommodate the ever-changing network environment.
- ✓ **Manage Systems and Configurations**
 - The system administrators are responsible for taking inventory of network devices and software. First, the administrators should remove unwanted, unneeded and unexpected hardware/software from the network. Thereafter, they should actively manage devices, applications, operating systems, and security configurations in order to ensure that systems can adapt to dynamic threat environments.
- ✓ **Continuously Hunt for Network Intrusions**
 - The proposed framework should take proactive steps to detect, contain, and remove any malicious presence within the network. The passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions are invaluable tools to find malicious or anomalous behaviors. The framework should support hunt operations and penetration testing using well-documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.
- ✓ **Leverage Modern Hardware Security Features**
 - The framework should use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. The system devices should be hardware refreshed, which

can increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment.

- ✓ **Segment Networks and Deploy Application-Aware Defenses**
 - The critical networks and services should be separated and they should be deployed with application-aware network defenses in order to block improperly formed traffic and restrict content, according to policy and legal authorizations.
- ✓ **Integrate Threat Reputation Services**
 - The framework should leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. The reputation services assist in the detection and the prevention of malicious events and allow for rapid global responses to threats, a reduction of exposure from known threats, and provide access to much larger threat analysis. Multi-source reputation and information-sharing services can provide a more timely and effective security posture against dynamic threat actors.
- ✓ **Multi-Factor Authentication services**
 - The framework should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user choices or susceptible to credential theft or even to reuse across multiple systems. The system should prioritize protection for accounts with elevated privileges, remote access, and/or used on high-value assets. Also, physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs.

This Appendix described strategies for mitigating cybersecurity risk. All, the described schemes are built upon the NIST Cybersecurity Framework and ENISA IoT guidelines in order to manage mitigate cybersecurity risk and promote a defense-in-depth security posture, when they are used for Supply Chain systems.