



Horizon 2020 Program

ICT-02-2020

Building blocks for resilience in evolving ICT systems



Certifying the Security and Resilience
of Supply Chain Services

Project Report 2

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

Table of Contents

List of Tables	4
List of Figures	5
List of Acronyms	6
Executive Summary.....	8
1. CYRENE proposed SCS certification scheme.....	9
1.1 Introduction.....	9
2. Subject Matter and Scope	13
3. Purpose of the CYRENE SCS scheme	13
4. Use of Standards	20
5. Assurance Levels	22
6. Self-Assessment.....	30
7. Specific Requirements Applicable to a CAB.....	32
8. Evaluation Methods and Criteria	34
9. Necessary Information for Certification	37
10. Marks and Labels.....	39
11. Compliance Monitoring	41
12. Certificate Management.....	43
13. Non-Compliance	48
14. New Vulnerabilities	52
14.1 Vulnerability handling.....	52
14.2 Vulnerability disclosure.....	53
15. Record Retention	54
16. Related Schemes	55
17. Certificate Format	56
18. Availability of Information	56
19. Certificate Validity.....	57
20. Disclosure Policy	58

21. SCS Mutual Recognition Agreement (MRA).....	60
22. Peer Assessment.....	62
23. Supplementary Information	65
24. Additional Topics.....	66
25. Further Recommendations	70
26. Conclusions.....	72
References.....	74
Appendices.....	76
Appendix A - Security Objectives and Requirements for SCSs	76
Appendix B - Meta-Approach for the Conformity Assessment of SCSs.....	149
Appendix C – Conformity Assessment for Level Basic	159
Appendix D – Conformity Assessment for Levels Substantial and High.....	169
Appendix E - Competence Requirements for Assessors.....	169
Appendix F - Scheme Document Content Requirements	170
Appendix G – Initial Application of SCS scheme	199
Appendix H – Glossary.....	204

List of Tables

Table 1: EAL based on SCS:	14
Table 2: Stakeholders involved in the production of the proposed CYRENE EUSCS certificates.....	16
Table 3: Evaluation Assurance Levels	23
Table 4: Coverage of Article 51 by requirement categories.....	34
Table 5: Nominal decisions associated with the maintenance of certificates.....	47
Table 6: Example of review results report.....	165
Table 7: Example Review Report from Assessor	200
Table 7: Draft Assurance report.....	203
Table 8 – Extracted from Supply Chain and Business Concepts CYRENE online glossary	204
Table 10 – Certification and Security Concepts of the updated CYRENE online glossary	209

List of Figures

Figure 1: Self-conformity assessment based SCS scheme 18

Figure 2: Conformity assessment based SCS scheme 19

Figure 3: Demo label for the proposed CYRENE EUSCS scheme in case of approval by ENISA 41

Figure 4: Processes related to the issuance and maintenance of a certificate 44

Figure 5: Standard Cargo Manifest sub-process 201

Figure 6: Port call Request 201

Figure 7: Port Authority Asset Description 202

List of Acronyms

Acronym	Description
CAB	Conformity Assessment Body
EU	European Union
EUCC	Cybersecurity Certification Scheme
EUCS	EU scheme proposed for the cloud services
SCS	Supply Chain Service
SCS-P	Supply Chain Service Provider
CSOCs	Complementary subservice organization controls
EUSCS	CYRENE proposed Supply Chain Service scheme
SCS-BP	Supply Chain Business Partners
CA	Conformity Assessment
SC	Supply Chain
SCM	Supply Chain Management
ICT	Information Communication Technologies
EUCSA	European Cybersecurity Act
CC	Common Criteria
MS	Member States
TOE	Target Of Evaluation
SCS-TOE	Supply Chain Service as Target of Evaluation
CAP	Conformity Assessment Process
GA	Grant Agreement
TOC	Table of Contents
ISMS	Information Security Management System
CAB	Conformity Assessment Bodies
AL	Assurance Level

EAL	Evaluation Assurance Level
OES	Operator of Essential Services
OIS	Operator of Important Services
ST	Security Target
SFR	Security Functional Requirements
TSF	TOE Security Function
CS	Communication Security
IAM	Identity Access Management
OPS	Operations
BCM	Business Continuity Management
PS	Physical Security
QR	Quick Response
IAR	Impact Analysis Report
NCCA	National Cybersecurity Certification Authority
MA	Mutual Agreement
TLP	Traffic Light Protocol
CVE	Common Vulnerabilities and Exposures
GDPR	General Data Protection Regulations
MRA	Mutual Recognition Agreement
NAB	National Accreditation Body
CB	Conformity Bodies
ECCG	European Cybersecurity Certification Group
CCC	Complementary Customer Controls

Executive Summary

This report proposes a draft version of the EUSCS candidate scheme (European Cybersecurity Certification Scheme for Supply Chain Services), which looks into the certification of the cybersecurity of supply chain services.

In this document all the elements of European cybersecurity certification schemes as defined in Article 54 of the EUCSA are presented. Eight appendices are also included in the document. The proposed SCS serves as guidelines to the SCS auditors; it specifies the various views of the SCS that can be adopted; the cybersecurity requirements that need to be met -such as standards or technical specifications-, the type of evaluation that is planned to be - done such as self-assessment or third party - and the intended level of assurance that is going to be achieved.

1. CYRENE proposed SCS certification scheme

1.1 Introduction

CYRENE [1] targets services (Supply Chain Services (SCS)) that their provision relies on a supply chain of different business partners (SCS-BPs). This supply chain can vary in length and complexity and most of the time exists in a highly liquid ecosystem, where it is monitored and continuously refined, to be consistent with the trending market needs and legal parameters. The mechanism of overseeing and applying regulations on the Supply Chain, is, according to the ISO 28000 series [2], referred to as Supply Chain Management (SCM) whereas the provider of a supply chain is referred to as supply chain provider. The latter is personalised in the term of the Supply Chain Service Provider (SCS-P) who is responsible for the provision of the SCS.

In many cases, a SCS-P can be a third-party logistics company hired by an organization to handle its SCS. SCS-Ps are responsible for ensuring that the business processes described in the SCS are effective and lead - through their actions - in higher efficiency in production, optimization in shipping, savings in costs, risk management, and improved quality control.

A SCS can be described by adopting any of three different views: the overall business, the holistic technical, and the sector-specific technical view of the SCS:

At first, the SCS overall business view 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, 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.

Next, the SCS holistic-technical view is an asset-based interdependent view 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 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.

Lastly, the SCS sector-specific technical view is individual (snapshot) of the SCS, i.e. the view that an individual business partner adopts. More specifically, it consists of the business partner's processes and assets in the SCS (it is a segment of the SCS).

SCSs are recognised by the European Union (EU) as key enablers for economic growth; thus, the SCS management capability is directly linked with the level of efficiency and effectiveness. SCS business partners outsource a variety of their SCS processes, critical information, and Information Communication Technologies (ICT) services to third parties and highly interdependent dispersed nodes of heterogeneous cyber-physical infrastructures.

The proposal of NIS Directive 2.0 (NIS 2 Directive) [3] contains measures for improving cybersecurity infrastructure and particularly the resilience and incident response capabilities of public and private competent authorities. One of the key elements of the Commission's proposal is to address the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. Cybersecurity certification of the SCS can be considered as a mitigation action against cybersecurity SCS risks.

As the threat landscape is enormously evolving, the Regulation (EU) 2019/881 of the European Parliament and the Council, known as EU Cybersecurity Act (EUCSA) [4] will promote the cybersecurity certification for ICT products (software, hardware, processes, services) and it will scale up the response to cyber-attacks, fostering cyber resilience and trust for consumers within the EU. The EUCSA puts the basis for the creation of the EU certification framework for ICT products; it provides a framework based on standards, namely ISO/IEC 15408 [5], also known as Common Criteria (CC) and ISO/IEC 18045 [6] (see D.2.1) [7].

The EU cybersecurity certification is defined as a comprehensive set of rules, technical requirements, standards, and procedures that are established at the Union level and that apply to the certification or Conformity Assessment (CA) of specific ICT products (software, hardware, systems, services). Each certification scheme shall specify the categories of products and services covered; the cybersecurity requirements that need to be met -such as standards or technical specifications-, the type of evaluation that is planned to be - done such as self-assessment or third party - and the intended level of assurance that is going to be achieved. The certificates will be valid across all Member States (MSs).

The European Cybersecurity Certification Scheme (EUCC) [8] will serve as a template to propose security certification schemes for ICT products.

The EUCC scheme is based upon Article 54 of the EUCSA. The latter presents in detail the key elements that an EU certification scheme shall include.

Using the EUCC, any ICT product can serve as a Target Of Evaluation (TOE) and can be the subject of a security evaluation also known as CA in which it is assessed against security requirements. The CA of the TOE is defined as the procedure that is followed for evaluating whether specified requirements relating to the TOE have been fulfilled. That being said, throughout the CA process, the TOE should be identified and security aspects should be concretely specified.

TOE can be an ICT product (equipment, device, asset, process, or service) as a whole or the elements of the ICT product. The CC leaves the assessor flexible on what to evaluate as it is not necessarily tied to the boundaries of ICT products. Based on the EUCC scheme, the EU cybersecurity certification scheme for Cloud Services (EUCS) [9], has been prepared.

This report proposes a SCS-scheme which investigates the certification of the cybersecurity of a SCS ecosystem and derives inspiration from different domains that are based on the ISO/IEC 17065 [10] standard in terms of applicable requirements to assessors performing certification. Additionally, many standards that are described in an abstract level for certification and procedure methods, are taken into consideration, thus the SCS scheme is mainly based on the ISO27000 [11] ISO28000 series of standards and ISO/IEC 15408.

CYRENE is responsible for producing the CYRENE's conformity/certification scheme that will be the basis for Conformity Assessment Process (CAP) that is described in CYRENE report 3 [12] and its realization will include the following:

- A Security Certification Assessment Scheme for SCS for ensuring resilience and security. This scheme will be focused on business-related aspects of SCS and will build upon the ISO28001 standard [13].

- An ICT Security Certification Assessment Scheme for ICT-based or ICT-interconnected SCS on certification of the supply chain IT infrastructure and will build upon ISO standards 28001, 27001 [14], and 27005 [15].
- An ICT Security Certification Assessment Scheme for SCSs' IoT devices and Systems. This certification scheme focuses on individual devices within the supply chain and differs from existing schemes on individual IoT devices as more stress should be put on data protection and privacy issues.

Keeping those capabilities in mind and considering the fact, that ENISA published the European Cybersecurity Scheme (EUCC) and the European Cybersecurity Scheme for Cloud Services (EUCS), after the CYRENE started, the CYRENE consortium to ensure usability and usefulness of the project's work decided to utilize the EUCC to build the proposed SCS scheme as well as use the EUCS as an example.

CYRENE's EUSCS scheme will define an approach that is compatible with EUCC but will also incorporate the notion of the escalating vulnerability assessment level in bond with the different assurance levels. More specifically, the higher the assurance level will be, the deeper the vulnerability analysis will be performed.

The CYRENE enhanced Risk and Conformity Assessment (RCA) methodology, described in a CYRENE Report 3, has a dual use. It can be utilised as a) an enhanced risk assessment for the SCS-P with the SCS-BPs to assess the SCS-risks, undertake controls and develop the protection profile (PP) of the SCS; and b) a conformity assessment methodology where the assessors assess the conformance of the claims in the SCS-PP to issue a SCS-certificate.

This report is structured as follows: Chapters 2 to 25 follow the same structure. In each chapter we propose content related to one of the points raised in Article 54(1) of the EUCSA.

Every chapter contains the following sections:

- An excerpt from Article 54 defining the topic to be addressed in the chapter.
- A proposed text, which is the proposed content for the scheme. This content defines scheme rules and requirements and makes extensive use of "shall" to express a requirement, and "may" to express an option.
- A rationale, starting when available by relevant excerpts from the EUCSA, and providing additional information, reasons for making the choices in the proposed text, and any other information deemed necessary.

The eight (8) Appendices at the end of the document support the proposed CYRENE scheme and their objectives are:

[Appendix A: Security Objectives and Requirements for SCSs](#)

The SCS-P operates an information security management system (ISMS) with the collaboration of the SCS-BPs. The scope of the ISMS covers the SCS's organisational units, locations and processes for providing the supply chain service and its security.

[Appendix B: Meta-Approach for the Assessment of SCSs](#)

The overall objective is to determine whether or not and to what extent a supply chain service delivered by a group of SCS-BPs is in conformity with the control and security requirements defined in the proposed CYRENE EUSCS scheme.

[Appendix C: Assessment for Level Basic](#)

The overall objective is to provide information on how to conduct a self-assessment.

[Appendix D: Assessment for Levels Substantial and High](#)

The overall objective is to encapsulate the assessors' responsibilities on:

- accepting the conformity assessment engagement;
- developing and executing the audit plan;
- provide the analysis of the conformity process results;
- issuing the assurance report.

Please note that both Appendix C and D follow the same structure to present assessors' responsibilities.

[Appendix E: Competence Requirements for Assessors](#)

Describe the requirements that the Conformity Assessment Bodies (CAB) and assessors have to meet in order to be accredited.

[Appendix F: Scheme Document Content Requirements](#)

The objective of this Appendix is to define guidelines for the redaction of documents. Rather than providing full templates, the Appendix lists requirements for writing the documents, which typically takes three forms:

- Requirements on content that shall be present, without constraints on the format;
- Requirements on text that shall be included as is, for a few important statements; and
- Requirements on the format and content of tables, to ease comparability of results.

[Appendix G: Initial example for application of the SCS scheme](#)

The objective for this appendix is to pinpoint the methodology followed for the application of the EUSCS in the Vehicle Transport SCS.

[Appendix H: Glossary](#)

The objective for this appendix is to present the glossary and terminology used in this report that has been inspired by D2.1 and is also available in the CYRENE website: <https://www.cyrene.eu/glossary/> and by Annex A: Conceptual Approach for Consistency of Terminology of ENISA Report on Methodology for a Sectoral Cybersecurity Assessment. [16]

2. Subject Matter and Scope

This section covers what are the types of SCSs the scheme will cover; what will the use of the schema be (for the types of SCS see D.2.1).

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

The EUSCS shall allow for the cybersecurity certification of SCSs according to the criteria and methods defined in CYRENE Report 3 and Chapter 8 below (Evaluation Methods and Criteria).

The EUSCS scheme may cover any SCS provided by any economic sector provided that it meets the following conditions:

- The perimeter (SCS-P/-BPs, view adopted) is well defined and stable for the provision of the SCS
- It aims at reaching the assurance level (AL) corresponding to one of the three levels ‘basic’, ‘substantial’ and ‘high’
- ALs of SCS are defined according to NIS 2 Directive essential services classification (CYRENE Report 3)

ICT services matching these criteria will from now be referred to as SCS. The EUSCS scheme may apply to all supply chain services, following some principles:

The proposed CYRENE EUSCS scheme also covers additional elements as foreseen by Article 54 of the EUCSA, under the conditions defined by [Chapter 24: Additional Topics](#):

- The definition of Security Profiles;
- The handling of force majeure cases;
- Rules for the protection of information related to cybersecurity certification;

3. Purpose of the CYRENE SCS scheme

In this section according to Article 54, we will describe the purpose of the scheme, selected standards, CYRENE methodology aims, who the users may be, what regulations, services, they may use, the definition of rules and mechanisms that may be combined to allow users to reach specific objectives, etc.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods, and assurance levels correspond to the needs of the intended users of the scheme;

The proposed CYRENE EUSCS scheme aims at improving the Internal Market conditions, and at enhancing the level of security in a wide range of SCSs, 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.

The proposed EUSCS scheme also covers a wide range of security requirements, by offering all three (3) security ALs defined in the EUCSA ('basic', 'substantial' and 'high').

The ALS of the SCS depends on how essential are the SCS if the SCS-P is an operator of essential services according to the NIS 2 Directive:

- Entity “means 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”
- Essential entity “means any entity of a type referred to as an essential entity in Annex I” (
- Important entity “means any entity of a type referred to as an important entity in Annex II”

In particular, the AL (Basic/Substantial/High), depends upon whether the SCS is considered essential or important or it is neither essential nor important according to Annex I of the NIS 2 Directive). In case the SCS is an essential service, namely the SCS-P is an Operator of Essential Services (OES), AL is considered “High”, whereas if the SCS is an Important Service, namely the SCS-P is an Operator of Important Services (OIS), AL is considered “Substantial” and when the SCS is neither essential nor important AL is considered “Low” as displayed in the following table.

Table 1: AL based on SCS:

AL	SCS (according to NIS 2 directive)
High	If SCS-P is an OES and the SCS is an essential service as defined in Annex I of NIS 2 Directive
Substantial	If SCS-P is an OIS and the SCS is an important service (as defined in Annex II of NIS 2 Directive)
Low	If SCS-P is non OES neither OIS and the SCS is neither an essential or important service

Users of the scheme may be:

- SCS-Ps who wish to assess the security of their SCSs through third-party certification;

- SCS business partners who wish to benefit from the evidence provided with certified SCSs to make informed decisions related to the security of these supply chain services;
- Regulatory authorities who wish to include security and assurance requirements on SCSs within their regulations and directives;
- Policymakers that wish to implement the proposed NIS 2 (related to the security of supply chains).

These users may use the proposed CYRENE EUSCS scheme:

- to assess how a SCS meets the requirements of a predefined set of security control objectives and a related set of measures when used according to security recommendations provided by the business partners and agreed by them;
- to provide business partners the information required to make informed choices about the procurement and operation of SCSs (including processes, assets, technologies, and operators involved in the provision of the SCSs), and to allow business partners to use certified SCSs in their development activities, and meet their security compliance requirements;
- to allow regulatory authorities to refer to the scheme in European and national regulations, including criteria based on information defined in the scheme, and to check compliance by verifying the information provided in the certificates stored in the site managed by ENISA.

The proposed CYRENE EUSCS scheme defines rules and mechanisms that may be combined to allow the SCS-P and the SCS-BPs to reach the following objectives:

- three (3) ALs (see [Chapter 5: Assurance Levels](#)) corresponding to levels ‘basic’, ‘substantial’ and ‘high’ defined in the EUCSA, which can cover SCSs corresponding to a wide range of risk profiles;
- the SCS Protection Profile (SCS-PP) which includes a set of security objectives and requirements (see [Chapter 8: Evaluation Methods and Criteria](#)), defining objectives to be met by business partners for all certified SCSs, further decomposed into requirements mapped to the ALs referred to above;
- an assessment meta-approach (see [Appendix B: Meta-approach for the conformity assessment of supply chain services](#)) defining by using any assessment method (e.g. the CYRENE RCA methodology described in CYRENE Report 3) to determine that a SCS fulfils the requirements assigned to a given AL;
- an assessment method (see [Chapter 8: Evaluation Methods and Criteria](#), [Appendix C: Conformity Assessment for Level Basic](#) and [Appendix D: Conformity Assessment for Levels Substantial and High](#)) defining how to determine that a supply chain service fulfils a given set of requirements;
- a set of document templates to be used during the evaluation and review activities ([Appendix F: Scheme Document Content requirements](#)) to ensure that the documents released by the self-assessors or Conformity Assessment Bodies (CABs) or their subcontractors follow the same organization and flow;
- a detailed list of the documents to be made publicly available as part of the certificate package, that may allow scheme users to locate the information they are looking for to make informed decisions;
- a set of rules about the lifecycle of certificates after their issuance, including maintenance and renewal requirements, management of vulnerabilities and complaints, and market surveillance activities, that may allow scheme users to remain informed of the evolution of the security of a given SCS.

In addition to these technical features, all stakeholders interested in the cybersecurity certification of SCSs will benefit from the following characteristics from the EUSCS scheme:

- a scheme aimed to harmonize the SCS security efforts;
- quality guarantees through the use of self-assessment, third-party assessment by accredited bodies, supervision by national authorities, and for the High level, authorization by the national authorities and peer assessment between conformity assessment bodies;
- the flexibility offered by three different ALs covering the entire range of assurance introduced in the EUSCS, with the possibility for a certified SCS to upgrade to a higher level in future evaluation cycles;
- assurance maintained over time, with regular reassessments;
- a maintenance framework for the proposed EUSCS scheme itself, if endorsed by EU institutions and MSs, will provide strong guarantees on continued operation of the scheme;
- integration in the European cybersecurity certification framework, which will facilitate the reuse of the proposed EUSCS;

The mechanisms defined above provide the means allowing the scheme’s intended SCS-Ps to meet their objectives, by providing the conditions required for performing evaluations, issuing and managing certificates, and maintaining the framework and scheme over time.

RATIONALE

Additional input

Recital 74 (excerpt). The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle.

Recital 92 (excerpt). European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended end user.

The scheme’s intended users cover all relevant SCS stakeholders in the life cycle of the certificate (production and consumption) and, due to the nature of the scheme, all relevant stakeholders in the life-cycle of the SCS.

Table 2 below describes the intended users of the certificate, their role and their use case related to the scheme.

Table 2: Stakeholders involved in the production of the proposed CYRENE EUSCS certificates

Stakeholder	Role	Use case
-------------	------	----------

Supply Chain Service Provider (SCS-P) (business partner A)	Originator	This business partner type is the main actor in the supply main (originator) who 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). Example: in the vehicle transport SCS, the automotive industry and all its third parties/sub-contractors belong in this type
SCS Commercial Business Partner (business partner B)	Operations	The commercial business partner participates in the provision of the SCS, undertaking an operational role, related to the operation of the SCS, including ordering, transporting, importing, and other processes. Example: in the vehicle transport SCS, the importers, transport/maritime companies and any third-party commercial partner belong in this category.
SCS Governmental Business Partner (business partner C)	Operations	The governmental business partner participates in the provision of the SCS, undertaking an operational role, related to the operation of the SCS, including ordering, provisioning, storing, and other processes. Example: in the vehicle transport SCS, the Ministry of Transport, Customs and other related authorities belong in this category.
Assessor (business partner D)	Compliance (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 conformity (for SCs with AL Low) -see Use Case I in Figure 1
CAB	Evaluation Review and Certification	For SCS of AL Substantial or High, the Evaluation role is undertaken by a CABs includes all the activities related to the assessment of SCSs and related processes (for SCSs with all ALs). The Review and Certification role for CABs includes all the activities related to the issuance and management of certificates, including in particular the review of the evaluation and of its results.
National Accreditation Body (NAB)	CAB Accreditation	NABs are the ones that select the CABs (ensuring that that they meet the criteria) are not directly involved in the production of certificates, but their role in the

National Certification Supervisory Authority (NCSA)	CAB' supervision	accreditation of CABs is essential in the proper operation of the scheme (for SCS with AL Substantial or High) -see Use Case II in Figure 2
ENISA	Proposal	ENISA is in charge of proposing the certificates issued in the context of the scheme to the European Commission (EC), as well as the events associated with these certificates.
EC	Review/Publicity	EC is responsible for reviewing, approving and publicizing the proposed scheme.

Use Case I: Cybersecurity Certification Scheme for SCS of assurance level Low

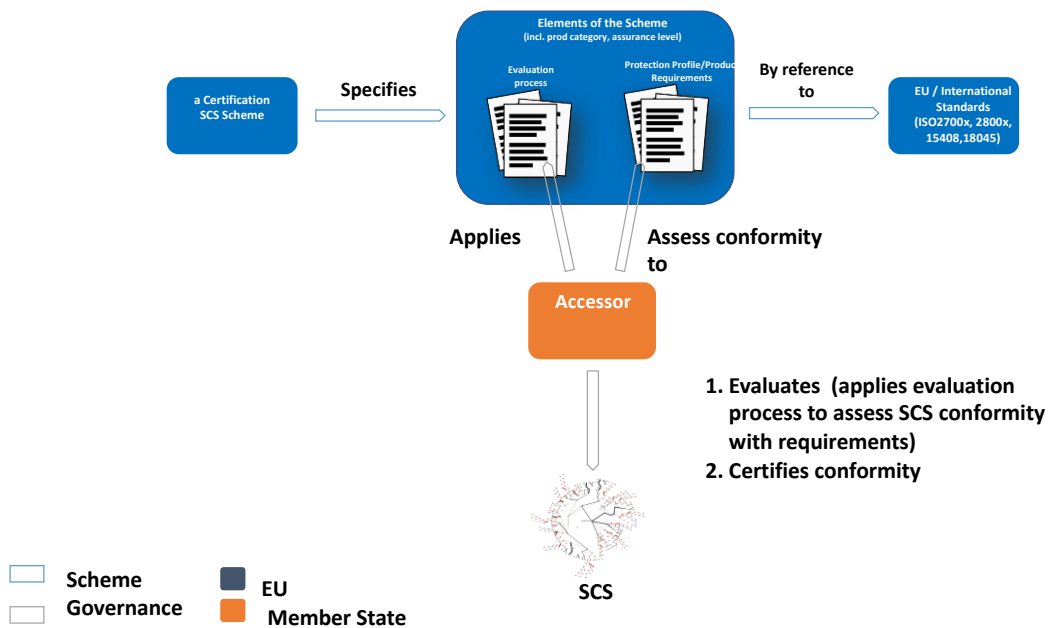


Figure 1: Self-conformity assessment based SCS scheme

Use Case II: Cybersecurity certification scheme of SCS of assurance level Substantial/High

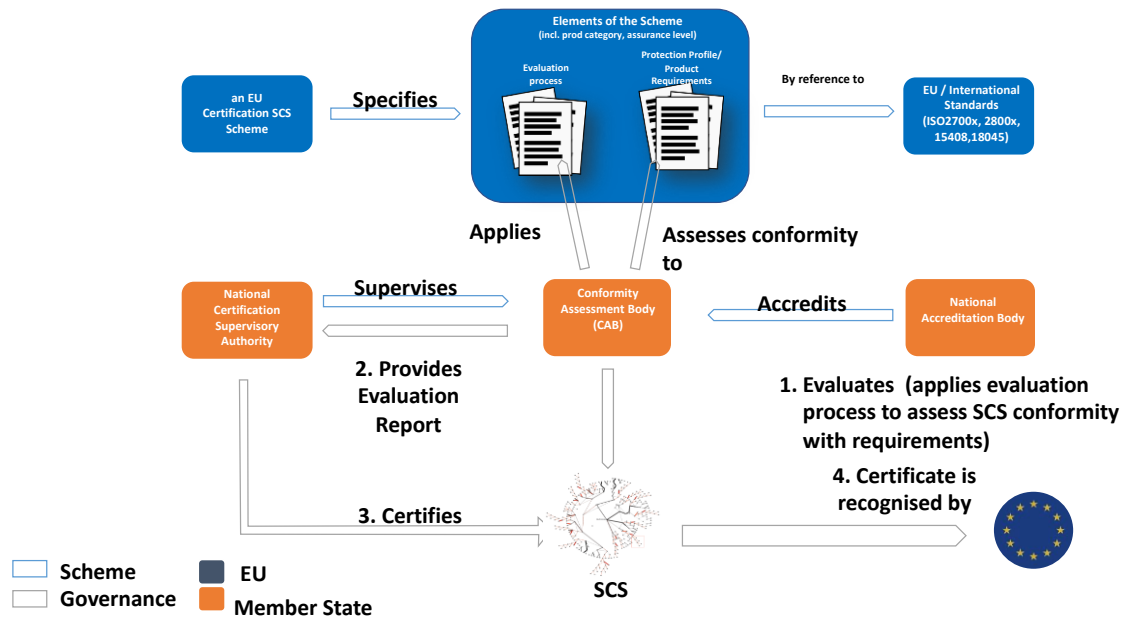


Figure 2: Conformity assessment based SCS scheme

The intended users who need the scheme are all stakeholders mentioned in Table 1 with one distinct objective for each category of users:

- For *SCS-Ps* (Business Partner A) and *SCS Commercial and Governmental Business Partners* (Business Partner B and C): The certification scheme (**Figure 1: Self-conformity assessment based SCS scheme**) shall assess how the SCS that participate meets the requirements of a predefined set of security control objectives and a related set of measures, when used according to security recommendations they have agreed upon. The scheme will allow all business partners to use a certified SCS in their own development activities, and to meet their own security compliance requirements in order to meet the requirements of the SCS. The scheme will also enable any Business partner in the SCS to self-assess (undertake the role of Supply Chain self-assessor-Business Partner D-) the security of the SCS using the scheme.

Finally, the scheme will provide security requirements about the processes, sub-processes, physical and cyber assets used in the provision of the SCS (supply chain assets), location, interrelations of the supply chain processes and assets, and responsibilities of the SCS partners.

- For *Regulatory Authorities*: The EC certification scheme (**Figure 2: Conformity assessment based SCS scheme**) shall allow Regulatory Authorities to refer to the scheme in international, European, and national regulations, including criteria based on information defined in the scheme.

For Regulatory Authorities, the scheme offers:

- a single certification scheme recognised the entire EU;
- three ALs corresponding to different needs from the SCSs and different use cases; and
- requirements mandating transparency about the processes, sub-processes, physical and cyber assets used in the provision of the SCS (supply chain assets), location/ interrelations of the supply chain processes and assets, and responsibilities of the SCS partners.

4. Use of Standards

This section will describe the standards, technical specifications, and security assessment methods that will be used by the CYRENE scheme and are based on Article 54 of the GDPR. This section presents a list of standards beyond the requirements aspect as well as a detailed view of the supply chain ecosystem.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following element (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

The scheme relies on the following standards and technical specifications:

- International standards ISO/IEC 17000 [17], ISO/IEC 9000 [18] and ISO/IEC 27000 [19], are being used as references for the terminology used throughout the scheme, with input from all the schemes listed below when required.
- The security controls used in the scheme, together with the associated security requirements are based on international standards ISO/IEC 28000:2007¹, ISO/IEC 27001:2013, ISO/IEC 27002:2013 [20] and on Annex A.15.1 of ISO 27001:2013.
- The definition of the ALs reuses some concepts defined in the ISO/IEC 9001, ISO/IEC 15408-3 international standard, and ISO 18045.
- The CA methodology defined in the scheme is based on the ISO/IEC 17065 international standard.

The scheme also leverages the following security assessment methods and standards:

- International standards ISO/IEC 17021 [21], ISO/IEC 27006 [22], ISO/IEC Guide 17067:2013 [23], ISO/IEC 17020:2012 [24][24], ISO/IEC 17024 [25][25].
- International auditing standards ISAE3402 [26] and ISAE3000 [27].
- The Integrated Supply Chain Management (ISCM) Guidelines (World Customs Organization, 2018)

Lastly, the security controls and other annexes refer to the following standards:

- The ISO/IEC 29147 [28] and ISO/IEC 30111 [29] standards are referenced about vulnerability handling.
- The ISO/IEC 27005 standard is referred to risk management.

¹ <https://www.iso.org/standard/44641.html>

RATIONALE

Additional input

This is reinforced in the request for the candidate scheme, which indicates that “the candidate scheme (...) should take into account existing and relevant schemes and standards.”

The text mentions regulation (EU) No 1025/2012 (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EU, 2012) it defines the following requirements (this is an outline, further details are available in the regulation itself:

1. Market acceptance, as demonstrated by the existence of compliant implementations from different vendors
2. No conflict with current or foreseen European standard
3. Developed by a non-profit making organization that fulfills some criteria
 - a) Openness of the specification development process
 - b) Consensus-based decision-making process
 - c) Transparency of the development process
4. Requirements on the specification itself
 - a) Sustained maintenance for a long period
 - b) Publicly available for implementation and use on reasonable terms
 - c) IP rights essential to the specification are available on an (F)RAND basis
 - d) Relevant and effective, responding to market needs and regulatory requirements
 - e) Neutral and stable
 - f) Sufficient quality and level of details, with standardised interfaces available as needed

These requirements are classical, and they are based on the World Trade Organization rules, so they are in practice met by many of the technical specifications developed by all kinds of industry groups.

Regarding the elements included in the scheme itself, the following guidance has been provided to the SOGIS (SOGIS, 2010) ad hoc working group:

- The elements that are mandatory for the implementation of the scheme must be included as appendices to the scheme, and they will be included in the regulation.
- The elements that are optional in the implementation of the scheme may be included in other documents, provided by ENISA on the certification framework portal.

Even though the above-mentioned standards are widely used, it has not been possible to solely rely on European standards. More specifically, when it comes to security controls, even though the ISO/IEC

27000 and ISO 28000 series provide a very good basis they could not fully encapsulate the details for the present scheme. Having said that, the proposed scheme will also take into consideration other families of standards such as NIST's SP 2000 [30] which provides more focused controls for Federal supply chains extending the scheme application directives.

The structure of the controls is strongly inspired by these standards taking also into consideration the Integrated Supply Chain Management Guidelines (ISCM) that contains annexes referring to supply chain security assessment, management, and controls. The content has been enriched, in particular by introducing more detailed requirements that have been mapped to assurance levels.

The requirements introduced in the EUSCS, have been designed by drawing inspiration from current practices in Europe, and in particular from the documents issued by the Member States who operated National Schemes for SCS. More specifically, when it comes to the assessment methods, the scheme will incorporate the two most widely used assessment method families, i.e., the ISO/IEC 28000 and ISAE3000 family. However, there has been a need to add a more targeted and simplified assessment method for the 'Basic' assurance level, which is defined in the scheme itself on Appendix C and will be described in detail in CYRNE Report 3.

Both ISO families have been composed in a way that could allow them to be considered as a basis for the establishment of new standards.

5. Assurance Levels

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(d) where applicable, one or more assurance levels;

The EUSCS Assurance Levels will be based on the Common Criteria (CC)². In general, CC assures that the process of specification, implementation, and evaluation of a computer security product has been conducted. To obtain assurance in CC, the analysis and the gathering of operational evidence phases need to be realised. The former includes:

- Traceability/coverage analysis
 - Between TOE design elements
 - Between TOE design elements and Security Functional Requirements (SFRs)
- Analysis of functional tests coverage and results
- Analysis of vulnerabilities
- Verification of proofs

whereas the latter, includes:

- Independent functional testing

² <https://www.commoncriteriaportal.org/>

- Penetration testing
- Checking that procedures have been applied

Evaluation Assurance Level (EAL) refers to a ranking category assigned to an IT product or system after the CC evaluation. The levels that will be analyzed, indicate to what extent this product or system was tested. In general, the CC includes seven levels of increased Assurance (described in 3 below) where its scale is based upon the following aspects:

- The level of assurance obtained (low security to high security in very risky contexts)
- The use of analysis and operational evidence techniques of varying formality (informal, structured, semi-formal, formal)
- The varying requirements regarding the level and formality of evidence are provided for evaluation.
- The varying requirements regarding the TOE development process (no conditions, to tool-supported, and to formal and fully accountable development processes)

Table 3: Evaluation Assurance Levels

EAL of increased assurance		
EAL (Name)	When to use	What does involve
EAL1. Functionally tested	<ul style="list-style-type: none"> ● Correct Security Target (ST) operation BUT some confidence is required. ● No serious threats to security ● Independent evaluation to support existing confidence 	<ul style="list-style-type: none"> ● Limited ST (work directly with of Security Functional Requirements(SFRs) without full threat analysis, assumptions, policies) analysis of SFRs using a functional and interface specification and guidance documentation for TOE ● No assistance from TOE developer ● Search for potential vulnerabilities in the public domain ● Some independent testing (functional and penetration) of TOE Security Function (TSF)
EAL2. Structurally tested	<ul style="list-style-type: none"> ● Independently assured security of low to moderate level ● Incomplete TOE development record ● Typical for legacy systems, or when access to TOE developer is limited. 	<ul style="list-style-type: none"> ● Analysis of SFRs using a functional and interface specification, guidance documentation and basic architecture of TOE (more complete ST) ● Developer testing based on functional specification & selective independent confirmation of developer test results ● Vulnerability analysis against basic penetration attacks ● Use of configuration management and evidence of secure delivery ● Independent testing (functional and penetration) of TSF

<p>EAL3. Methodically tested and checked</p>	<ul style="list-style-type: none"> ● Independently assured security of moderate level ● Thorough investigation of TOE and its development record ● Security engineering during TOE development but no substantial reengineering of TOE 	<ul style="list-style-type: none"> ● Analysis of SFRs using a functional and interface specification, guidance documentation and basic architecture of TOE (more complete ST) ● Developer testing based on functional specification and TOE design & selective independent confirmation of developer test results ● Vulnerability analysis against basic penetration attacks ● Use of configuration management & evidence of secure delivery ● Use of development environment controls ● More complete independent testing (functional and penetration) of TSF including mechanisms preventing tampering of TOE
<p>EAL4. Methodically designed, tested & reviewed</p>	<ul style="list-style-type: none"> ● Independently assured security of moderate to high level ● Thorough investigation of TOE and its development record ● More extensive security engineering during TOE development 	<ul style="list-style-type: none"> ● Analysis of SFRs using a complete functional and interface specification, guidance documentation and basic TOE modular design and a subset of TOE implementation (to understand security) ● Developer testing based on functional specification and TOE design & selective independent confirmation of developer test results ● Vulnerability analysis against enhanced basic attacks based on TOE implementation ● Use of configuration management & evidence of secure delivery ● Use of development environment controls, including automations ● More complete independent testing (functional and penetration) of TSF including mechanisms preventing tampering of TOE
<p>EAL5. Semi formally designed and tested</p>	<ul style="list-style-type: none"> ● Independently assured security of high level ● Thorough investigation of TOE and its development record ● Rigorous security engineering during TOE development 	<ul style="list-style-type: none"> ● Analysis of SFRs using a complete functional and interface specification, guidance documentation, semiformal modular TOE and TSF design, and a subset of TOE implementation ● Developer testing based on functional specification and TOE design & selective independent confirmation of developer test results

		<ul style="list-style-type: none"> ● Independent vulnerability analysis against moderate attacks ● Use of comprehensive configuration management & evidence of secure delivery ● Use of development environment controls, including automations ● More complete independent testing (functional and penetration) of TSF including mechanisms preventing tampering of TOE
EAL6. Semi formally verified design & tested	<ul style="list-style-type: none"> ● Independently assured security in high risk situations ● Rigorous TOE development environment 	<ul style="list-style-type: none"> ● Analysis SFRs using a complete functional and interface specification, guidance documentation, semiformal modular TOE and TSF design, a subset of TOE implementation; and a formal security policies and semiformal TOE functional specification ● Developer testing based on functional specification and TOE design & selective independent confirmation of developer test results ● Independent vulnerability analysis against high attacks ● Comprehensive configuration management & secure delivery ● Use of structured development process & environment controls, including complete automations ● Comprehensive independent testing (functional and penetration) of TSF including mechanisms preventing tampering of TOE
EAL7. Formally verified designed & tested	<ul style="list-style-type: none"> ● Independently assured security in extremely high risk situations ● Limited to TOEs with very focused SFRs, amenable to extensive formal analysis 	<ul style="list-style-type: none"> ● Analysis of SFRs using a complete functional and interface specification, guidance documentation, semiformal modular TOE and TSF design, complete TOE implementation; and a formal security policies and semiformal TOE functional specification ● Developer testing based on functional specification and TOE design & complete independent confirmation of developer test results ● Independent vulnerability analysis against high attacks

		<ul style="list-style-type: none"> ● Comprehensive configuration management & secure delivery ● Use of structured development process & environment controls, including complete automations ● Comprehensive independent testing of TSF
--	--	--

Taking those ways of Assurance into consideration, ALs (see Table 3) are described furtherly, from seven levels of increased assurance. This scale is based upon the following aspects:

- The Level of assurance obtained (low security to high security in very risky contexts)
- The use of analysis and operational evidence techniques of varying formality (informal, structured, semi-formal, formal)
- The varying requirements regarding the level and formality of evidence provided for evaluation
- The varying requirements regarding the TOE development process (no conditions, to tool supported, and to formal and fully accountable development processes)

The scheme defines three assurance levels, with assurance level Basic corresponding to the ‘basic’ assurance level of the EUCSA, assurance level Substantial corresponding to the ‘substantial’ assurance level of the EUCSA, and assurance level High corresponding to the ‘high’ assurance level of the EUCSA.

The assurance level of the EUSCS, will be considered “high”, if it is an essential service in the critical sectors of transport, energy, finance, health, government (as defined by NIS). Otherwise, the assurance level is Substantial (if the EUSCS belongs in a critical sector but it is not essential) and Basic (for all other EUSCS).

As specified in the EUCSA’s Article 52(5), assurance level Basic is “intended to minimise the known basic risks of incidents and cyberattacks” and can be further defined as follows:

- AL Basic should provide limited assurance that the supply chain is built and operated with procedures and mechanisms to meet the corresponding security requirements at a level intended to minimise the known basic risks of incidents and cyberattacks.
- AL Basic should be suitable for supply chain components that are designed to meet typical security requirements on services for non-critical data and systems.
- The typical attacker profile for AL Basic should be a single person with limited skills repeating a known attack with limited resources, not including the ability to perform social engineering attacks.
- The evaluation scope for AL Basic shall be defined by the description of the SCS and by the security objectives and requirements pertaining to assurance level Basic, as defined in [Appendix A: Security Objectives and requirements for SCSs](#), including processes and the software (understood as result of a development process) underlying the service.
- The evaluation depth for AL Basic shall consist solely of inspection activities, based on a check for completeness and coherence of the provided documentation on processes and design intended to confirm the fulfilment of technical and organizational measures, including requirements for fully

automated testing of basic known vulnerabilities and automated compliance checks by the SCS. A report following defined procedures shall be generated by the assessor. Self-gathered evidence shall be regularly submitted to the CAB to justify the continued development and operation of the service.

- The evaluation depth for AL Basic shall be driven by a predefined audit plan.
- As specified in the EUCSA Article 52(6), AL Substantial is “intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources” and can be further defined as follows:
 - AL Substantial should provide reasonable assurance through evaluation by an assessor that the SCS is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The assessor shall determine that the SCS-P has assessed those risks and implemented suitable controls that, if operating effectively, minimise those risks and meet the corresponding security requirements throughout a specified period.
 - AL Substantial should be suitable for supply chains that are designed to meet typical security requirements on services for business-critical data and systems.
 - The typical attacker profile for AL Substantial should be a small team of persons with hacking abilities and access to a wide range of known hacking techniques such as penetration testing, including social engineering, but with limited resources, in particular to launch wide attacks or to discover previously unknown vulnerabilities.
 - The evaluation scope for AL Substantial shall be defined by the description of the supply chain and by the security objectives and requirements pertaining to assurance level Substantial, as defined in [Appendix A: Security Objectives and Requirements for SCSs](#), including processes and the software (understood as result of a development process) underlying the service. The effective operation of the relevant security controls shall also be demonstrated throughout a specified period.
 - The evaluation scope for AL Substantial shall include, in addition to the requirements for assurance level Basic, on-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design, including the validation of the functional tests performed on that implementation. The security controls for assurance level Substantial shall include a limited pen testing using known attacks.

As specified in the EUCSA Article 52(7), AL High is “intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources” and can be further defined as follows:

- AL High should provide reasonable assurance through evaluation by an assessor that the SCS is built and operated with procedures and mechanisms to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The assessor shall determine that the SCS-P has assessed those risks and implemented suitable controls that operated effectively

to minimise those risks and meet the corresponding security requirements throughout a specified period.

- Dedicated requirements are defined in [Appendix A: Security Objectives and Requirements for SCSs](#) to ensure that controls shall be automatically monitored for continuous operation in accordance with their design, and that the controls shall be regularly reviewed and pen tested to validate their actual ability to prevent or detect security breaches.
- Assurance level High should be suitable for SCS that are designed to meet specific (exceeding level ‘substantial’) security requirements for mission-critical data and systems.
- The typical attacker profile for assurance level High should be a team of highly skilled persons with access to significant resources to design and perform attacks, get insider access, discover or buy access to previously unknown vulnerabilities.
- The evaluation scope for assurance level High shall be defined by the description of the SCS and by the security objectives and requirements pertaining to assurance level High, as defined in [Appendix A: Security Objectives and Requirements for SCSs](#), including processes and the software (understood as result of a development process) underlying the service. The effective operation of the relevant security controls shall also be demonstrated throughout a specified period.
- The evaluation depth for assurance level High shall be based on the depth for AL Substantial, to which requirements on depth of inspection or testing shall be added to verify that the controls implemented by the SCS-P actually meet their objective. In particular, these requirements concern the automated monitoring of controls and the review and penetration testing of security controls. Such activities shall be planned over multiple years, and they shall be performed by personnel with appropriate competences, in particular when thorough analysis of penetration testing or in-depth technical reviews are required.
- The evaluation depth for assurance level High shall be driven by a full justification of the coverage for all mappings, including for processes. It may also include higher expectations for some processes and their implementation, as defined in the security controls pertaining to AL High.

RATIONALE

Additional input Article 52 provides details about the assurance levels, and in particular:

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.

3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigor and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.

5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or

that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

6. A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

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

(65) The assurance level of a European certification scheme is a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure the consistency of the European cybersecurity certification framework, a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each European cybersecurity certificate might refer to one of the assurance levels: ‘basic’, ‘substantial’ or ‘high’, while the EU statement of conformity might only refer to the assurance level ‘basic’. The assurance levels would provide the corresponding rigor and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.

(66) A European cybersecurity certification scheme might specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Evaluation levels should correspond to one of the levels and should be associated with an appropriate combination of assurance components. For all assurance levels, the ICT product, ICT service or ICT process should contain a number of secure functions, as specified by the scheme, which may include: a secure out-of-the-box configuration, a signed code, secure

update and exploit mitigations and full stack or heap memory protections. Those functions should have been developed, and be maintained, using security-focused development approaches and associated tools to ensure that effective software and hardware mechanisms are reliably incorporated.

(67) For assurance level ‘basic’, the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service or ICT process by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review. Where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes has carried out a self-assessment of the compliance of the ICT product, ICT service or ICT process with the certification scheme.

(68) For assurance level ‘substantial’, the evaluation, in addition to the requirements for assurance level ‘basic’, should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

(69) For assurance level ‘high’, the evaluation, in addition to the requirements for assurance level ‘substantial’, should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.

All ALs defined in the EUSCS scheme satisfy all requirements that are applicable to all EUCSA ALs, following the notion of the higher the AL the deeper the vulnerability assessment that is going to be performed. ALs of EUSCS to define the level of vulnerability assessment that must be undertaken in each AL it considers both EUCSAALs and CC ALs (AVA assurance class) (presented in CYRENE Report 3) to meet the requirements not only on EU level but also on international level as SCS may be international services supporting global supply chains, including business partners from non EU Member States

6. Self-Assessment

This section describes the circumstances under which the CYRENE conformity self-assessment methodology, that is provided in CYRENE Report 3 in the context of the proposed enhanced Risk and Conformity Assessment (CYRENE RCA) methodology, is permitted under the CYRENE SCS scheme. Figure 1: Self-conformity assessment based SCS scheme above described the steps for self-assessment.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(e) an indication of whether conformity self-assessment is permitted under the scheme.

EU statements of conformity will be issued by SCS-P under the EUSCS scheme if the AL of the SCS is Basic.

RATIONALE

Additional input

In addition, Article 53, provides further information on conformity self-assessment, and in particular:

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.
2. The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

Recitals also provide additional information:

(78) European cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all of the checks to ensure that the ICT products, ICT services or ICT processes conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms. Moreover, conformity self-assessment should be permitted for ICT products, ICT services or ICT processes only where they correspond to assurance level 'basic'.

(79) European cybersecurity certification schemes could allow for both conformity self-assessments and certifications of ICT products, ICT services or ICT processes. In such a case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between ICT products, ICT services or ICT processes with regard to which the manufacturer or provider of ICT products, ICT services or ICT processes is responsible for the assessment, and ICT products, ICT services or ICT processes that are certified by a third party.

Self-assessment is permitted to be performed by the SCS-P or any SCS business partner (with the collaboration of the SCS-P) under the proposed scheme however EU conformity statements can be issued only by the SCS-P. The issuance of EU statements of conformity by SCS-Ps could only have been allowed for all SCSs of AL Basic that present a low risk (Article 53(1)), *i.e.*, to a subset of the SCS that could be certified at level Basic.

Self-assessment is suitable for SCSs, even at level Basic and even on a strictly defined subset of services. In addition, there are many elements in the scheme, including the definition of the security objectives and requirements that are entirely new. The scheme allows the SCS-P with the consensus of all SCS business partners to interpret security requirements. The processes in this case are described in Figure 1: Self-conformity assessment based SCS scheme.

For SCS of higher ALs (“Substantial”, “High”) only accredited CABs can use the proposed CYRENE scheme. The processes in this case are described in Figure 2: Conformity assessment based SCS scheme.

CYRENE conformity assessment methodology that is presented in CYRENE Report 3 could be used not only for the ‘Basic’ AL but also for ‘Substantial’ and ‘High’ ALs.

7. Specific Requirements Applicable to a CAB

In case the SCS has AL High then it needs to be assessed by CABs (self-assessment will not be permitted). In this case according to “Art. 54 (f). CABs need to guarantee their technical competence and here we will propose the competencies that will be required by the CABs.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

All CABs performing assessments in the context of the CYRENE proposed EUSCS scheme will need to be accredited for ISO17065, complemented by the requirements defined for the proposed EUSCS scheme (see [Appendix E: Competence Requirements for Assessors](#)). The requirements will define several profiles corresponding to the various roles in the conformity assessments, in order to allow CABs that only perform a subset of the conformity assessment activities, in particular those that only perform evaluation activities. Since the SCSs can be described with three (3) different views (process, technical, sector-specific technical) they will be the options to assess the SCSs using any of the three different conformity assessment profiles.

The technical competence requirements associated to accreditation are sufficient to perform conformity assessments at levels Basic and Substantial. However, advanced competences are required in order to perform a conformity assessment at level High. As a consequence, conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out in the context of an evaluation at level High conformity assessment tasks related to highly technical topics including:

Penetration testing, encompassing the design and performance of penetration tests and a deep analysis of penetration testing activities of the SCS components (processes, technical assets); a thorough exploration of the SCS security resistance to attacks ensuring tolerance to intrusions requiring an advanced level of attack potential, analysis of development activities, and in particular the review of the design and implementation of security measures in the SCS processes and/or assets. Penetration testing is included in

all ALs based on AVA_VAN security assurance class of CC!! So what changes, as we go to an upper AL, is that the analysis while performing a penetration test is deeper and the SCS should ensure a higher level of resistance to an attack to surpass corresponding levels of attack potential as defined in CYRENE Report 3.

Further details are provided in Appendix E: Competence Requirements for Assessors.

RATIONALE

Additional information from the EUCSA

Article 60 covers Conformity assessment bodies:

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008 [31]. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.
3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

Article 58, about National Cybersecurity Certification Authorities, also covers that topic:

7. National cybersecurity certification authorities shall:

- (c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;
- (e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation;

The Annex to the Cybersecurity Act (Requirements to be met by Conformity Assessment Bodies) provides detailed information on the conditions to be met by all CABs. However, it does not include any reference to point (f) of Article 54 (1), so we don't reproduce it here.

The competence required for CABs are rather generic, since most of the controls are related to the processes and assets used in the provision of the SCS under assessment. Nevertheless, some controls require competences (business, technical and legal), in particular at the highest levels of assurance.

Pen testing and business analysis of development activities are provided as examples, since those activities do require specific competencies, but the “including” formulation does not preclude the addition of further activities.

8. Evaluation Methods and Criteria

This section aims to demonstrate the evaluation methods and criteria referred to Article 51, that will be used in the EUSCS proposed scheme.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

The EUSCS scheme uses a set of evaluation criteria defined in [Appendix A: Security Objectives and requirements for SCSs](#). The EUSCS assessment methodology, based on the ISO17065 standard, is defined in [Appendix B: Meta-approach for the Conformity Assessment of SCSs](#). This methodology defines two assessment approaches that may be used by assessors:

- An assessment approach that may be used for ALs Substantial and High. This approach is defined in [Appendix C: Conformity Assessment for Level Basic](#)) and draws inspiration from both the ISO17021 (ISO/CASCO, 2015) standard and the ISAE family of standards IAASB Handbook [32];
- An assessment approach, defined in [Appendix D: Conformity Assessment for Levels Substantial and High](#) that may be used solely for assurance level Basic.

In the SCS proposed scheme, each assessment level is interconnected with the depth level of vulnerability assessment. The higher the AL that the SCS-P wishes to obtain, the more in-depth vulnerability analysis will be conducted. To achieve a high level of interoperability between the assessment methods, the EUSCS assessment methodology defines strict guidelines and requirements on the assessment process, which shall be followed independently of the assessment method used in a specific evaluation.

Following the methodologies, the objectives of the Article 51 are covered by the security objectives requirements defined in

Table 4: Coverage of Article 51 by requirement categories. The table below provides a high-level vision based of the coverage of Article 51 requirements by security categories from [Appendix A: Security Objectives and Requirements for SCSs](#).

Table 4: Coverage of Article 51 by requirement categories

Security objectives from Article 51	Categories from Appendix A:
(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;	This is covered in many categories of the scheme, including in particular the CKM category (covering cryptography and the Communication Security (CS) category (covering the security of communications

<p>(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;</p>	<p>This is covered in many categories of the scheme, including in particular the CKM category (covering cryptography) and the CS category (covering the security of communications)</p>
<p>(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;</p>	<p>This is mostly covered by the Identity Access Management (IAM) category (covering identity management, authentication, and access control)</p>
<p>(d) to identify and document known dependencies and vulnerabilities;</p>	<p>This is mostly covered by the PM category (defining relationships with suppliers) and the OPS category (defining vulnerability handling)</p>
<p>(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;</p>	<p>This is mostly covered by the OPS category (defining logging)</p>
<p>(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;</p>	<p>This is mostly covered by the OPS category (defining logging)</p>
<p>(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;</p>	<p>This is mostly covered by the OPS category (defining general pen testing measures) and by the DEV category (defining vulnerability testing in the development context)</p>
<p>(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;</p>	<p>This is mostly covered by the Business Continuity Management (BCM) category (defining business continuity) and the Physical Security (PS) category (defining physical security measures)</p>
<p>(i) that ICT products, ICT services and ICT processes are secure by default and by design;</p>	<p>This is mostly covered in the DEV category (defining methodology), with complements in many other categories</p>
<p>(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.</p>	<p>This is mostly covered by the OPS category (vulnerability handling), in the CCM category (for change management) and in the DEV category (for development methodologies)</p>

RATIONALE

Article 51. Security objectives of European cybersecurity certification schemes A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

- (a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process inside the supply chain ecosystem;
- (b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process and with all the means of the Supply Chain as a whole;
- (c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (d) to identify and document known dependencies and vulnerabilities;
- (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) to verify that ICT products, ICT services and ICT processes within the Supply Chain do not contain known vulnerabilities;
- (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- (i) that ICT products, ICT services and ICT processes are secure by default and by design;
- (j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Recital (74) provide a rational for Article 51:

(74) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT processes should then be further specified

in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications if no appropriate standards are available.

The covering of all the categories defined in information security standards such as the ISO 27001 and other conformity assessment schemes are also drawing the ground for the requirements that are defined in this proposed EUSCS scheme. The structure of the requirements is inspired by the C5 criteria [33]. Also, the ISCM Guidelines [34] were taken into consideration for fine-tuning due to its' abstract annexes that revolve around the management of the SCS ecosystem.

Regarding assessment methods, a key objective from the scheme has been to minimise the disruption of existing practices regarding certification and assurance for SCS-Ps. To this end, the scheme utilises a hybrid methodology, based on both the ISO17021 that is used for ISO27001 certifications and on the ISAE3402 used by many companies to obtain assurance for the security of their information systems. As a result, the scheme has the advantage to (a) propose assurance levels with increasing requirements that correspond to the levels defined in EUCSA and (b) allow the combination of the assessments defined in ISO17021 and ISAE3402 allowing SCS-Ps to contain the investment on compliance.

9. Necessary Information for Certification

In this section we will propose the documented information or records that need to be provided to the assessor.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;

When a SCS-P wishes to get a SCS certificate or to maintain the certification of an already certified SCS, the SCS-P shall apply document, following the template defined in [Appendix F: Scheme Document Content Requirements](#) completed with all required information, which depends in part on the reason that triggered the conformity assessment.

During the evaluation, the SCS shall submit all the information needed to demonstrate that the implementation of their SCS meets the security requirements defined in [Appendix A: Security Objectives and Requirements for SCSs](#) for the targeted assurance level, including but not limited to:

- policies and procedures that apply to the design and operation of the SCSs under evaluation;
- documentation related to the SCSs under evaluation, including the view adopted and elements of the view (e.g. in process view then the processes and business partners along with the Mutual Agreement needs to be provided);
- if required, records that can be used as evidence that the abovementioned policies and procedures are being followed e.g. the individual security policies, the documentation of all controls of the SCS-assets;
- if third party organizations/subcontractors are used, the business partners need to provide assurance for their security levels;

- where explicitly stated, specific documents and records required by the assessor to assess the fulfilment of requirements pertaining to specific security controls.

The information to be provided also depends on the assurance level required for the certification, as defined in [Chapter 5: Assurance Levels](#)). The information shall be provided following the assessment processes defined in [Appendix B: Meta-approach for the assessment of SCSs](#), [Appendix C: Conformity Assessment for Level Basic](#) and [Appendix D: Conformity Assessment for Levels Substantial and High](#).

In the context of the conformity assessment, the supply chain shall grant the CAB:

- access to all information, such as records and documentation, including service level agreements, of which management is aware that is relevant to the SCS;
- access to additional information that the CAB may request from management for the purpose of the evaluation;
- unrestricted access to personnel within the Service Organization from whom the CAB determines it may be necessary to obtain evidence relevant to the evaluation.

All records and documentation supporting the Conformity Assessment shall be appropriately archived by the SCS-P and/or the CAB, as defined in [Chapter 15: Record Retention](#) and [Chapter 18: Availability of Information](#).

As part of a new certification, it shall be possible to reuse evaluation results from another ICT certification or assessment. The applicant may therefore make available to the CAB previous evaluation results to be re-used as evidence. The CAB shall reuse such results for its tasks only when the provided evidence conforms to the requirements for such evidence, the evidence has been evaluated following a methodology recognised by the scheme, and the authenticity of the evidence can be confirmed.

In addition, the SCS-P shall submit to the CAB the link to the supplementary cybersecurity information required by Article 55 of the EUCSA, in accordance to the rules defined in [Chapter 23: Supplementary Information](#).

Security requirements are defined in [Appendix A: Security Objectives and Requirements for SCSs](#) related to the availability and content of this supplementary information, to be fulfilled by certified SCSs at all ALs.

Additional information may be required when the Conformity Assessment is performed as a consequence of the vulnerability management process defined in [Chapter 14: New Vulnerabilities](#), or of the nonconformity management process defined in [Chapter 13: Non-Compliance](#), to ensure that the vulnerability or nonconformity has been properly handled.

An important part of the information provided by the SCS-P is the description of its SCSs, which shall follow the principles below:

- The description shall provide the information that is likely to be relevant from the assessor's perspective to understand the SCS and associated controls to meet the applicable EUSCS requirements as defined in [Appendix A: Security Objectives and Requirements for SCSs](#). Other aspects of the SCS do not need to be covered in the provided information.
- If the SCS-P uses subservice organizations in the provision of the SCS, the description shall indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the SCS-P's own controls, to meet certain of the SCS scheme requirements. The information shall include a presentation of applicable EUSCS requirements, with the SCS-P's controls, the types of complementary subservice organization controls assumed in the design of the SCS-P's controls, and pointers to assurance documentation where evidence can be found that the subservice organization satisfies these complementary

subservice organization controls with an level assurance suitable for the targeted level of assurance. The assurance documentation referred to in that presentation shall be included in the information provided to the assessor.

- The description shall indicate that Complementary Customer Controls that are suitably designed and are operating effectively are necessary, along with the SCS-P's controls, to meet some of the applicable EUSCS requirements. The description shall present the applicable EUSCS requirements, the SCS-P's controls and the Complementary Customer Controls assumed in the design of the SCS-P's controls.

General rules regarding the protection of the information provided by an applicant shall comply with the requirements established under [Chapter 24: Additional Topics](#).

RATIONALE

Additional information from the EUCSA

The information to be provided by the SCS-P is mostly guided by the requirements defined in the security controls in [Appendix A: Security Objectives and Requirements for SCSs](#). The present chapter only defines the main principles, which grants the CAB both necessary and limited access to:

- all pertinent documents, including policies and procedures, as well as records, logs, and other documents that can attest that the procedures and policies are being applied appropriately;
- interactions with employees, including individual interviews and group meetings, to gather information on the application of procedures, or to provide explanations pertaining to the definition and implementation of security controls;
- interactions with the SCS-P's systems, in particular to verify that technical security controls are properly implemented, which may either be performed directly by an auditor, or performed by a SCS-P employee in front of an auditor.

There may be some restrictions in the availability of the information, in particular related to the confidential nature of the information, so some information may only be available to the CAB for a limited time, and only on the premises of the SCS-P. Such limitations should be considered in the contractual agreement between the CAB and the SCS-P, to ensure that they are acceptable to the CAB and that possible additional costs are covered by the SCS-P.

In addition to the information related to the requirements, the SCS-P needs to provide other information to the CAB for evaluation:

- the supplementary cybersecurity information required by Article 55 of the EUCSA;
- any relevant information pertaining to a vulnerability or nonconformity that has triggered the conformity assessment.

This provision has been added in the case where the CAB would need specific information related to an issue or to the supplementary cybersecurity information that has not been explicitly planned in the security controls' requirements.

10. Marks and Labels

The aim of this section is to propose a logo for the CYRENE SCS scheme and explain the conditions that need to be fulfilled in order to use this logo.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used.

The CYRENE EUSCS may provide for a label and associated mark.

When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each SCS and related documentation. The labels used on the supply chain service and related documentation shall contain exactly the same information as the label included on the certificate, and follow all the guidelines provided with the label and associated mark defined for the CYRENE EUSCS.

A label and associated mark shall only be used when the certificate is awarded and until its expiration, and in association with the certified SCS: the non-respect of this condition shall be considered as an irregularity, as defined by Chapter 11 (Compliance Monitoring).

Without prejudice to the rules for monitoring compliance as described under Chapter 11 (Compliance Monitoring), depending on the circumstances, the nature and impact of the non-respect, wrong use, misuse, abuse of the mark and or label may have other legal implications in the field of IP right protection, possible criminal allegations (e.g. fraud, deceit), market surveillance regulations related to consumer protection (e.g. misleading and or unlawful comparative advertising of SCS). These legal implications are outside the scope of this CYRENE EUSCS scheme.

RATIONALE

A label and associated mark, established for the CYRENE EUSCS and specifically implemented for this scheme, will allow to:

- highlight that the SCS has been certified in the European Union and to provide immediate information regarding the certificate by referring to the framework (ECCF), the evaluation scheme and the assurance level;
- make the certification easily recognizable as both the label and the associated mark may be used in the SCS's web site and printed on technical documents and on leaflets used for marketing purposes;
- upon approval of the candidacy by ENISA, a direct link (in the form of a QR code) to the ENISA website (as per Article 50) will be provided - where all the information regarding the certificate are disclosed, including the current status of the certificate.




			
Certified in the European Union		EUSCS ENISA website	
EUCSA – Assurance Level (basic / substantial / high)		EUSCS - specific Assurance Level Name	

Figure 3: Demo label for the proposed CYRENE EUSCS scheme in case of approval by ENISA

The “demo label”, shows the basic information that the label associated with the scheme may contain:

- logo of the CYRENE EUSCS (to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework);
- QR code pointing to the web portal of ENISA - as per the Article 50 of the EUCSA – and to the page where the effective status of the certificate of the SCS and the information regarding its lifecycle can be retrieved;
- EUCSA assurance level (with the introduction of a specific colour identifying each level);
- specific EUSCS AL;
- the sentence “Certified in the European Union”, together with the flag of the EU (in case of final approval).

The introduction of the QR code will imply, as defined by [Chapter 20: Disclosure Policy](#), a procedure for the release of the QR code.

The demo label only contains summary information. In particular, it does not contain any reference to a date or to an issuing assessor. The use of the label therefore needs to be strictly controlled to ensure that:

- The label is only used in direct relationship with a certified SCS;
- The label is only used when the corresponding certificate is valid (i.e. after issuance, before withdrawal or expiration);
- The assurance levels and logos mentioned on the label are the appropriate ones for the particular SCS; and
- The label is only used with the QR-code obtained through the procedure defined in Chapter 20, which will point to ENISA’s Web site (upon approval by ENISA and the EC).

Compliance monitoring is in charge of ensuring that SCS-Ps comply to these requirements.

11. Compliance Monitoring

This section describes the rules for monitoring compliance of SCSs security requirements with the ones described by the proposed CYRENE EUSCS proposed scheme.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(j) rules for monitoring compliance of ICT products, ICT services, and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements.

The rules presented herein, include the continuous monitoring of the SCS processes and assets as a means to validate their compliance according to specific European cybersecurity certificates or EU statements of conformity. The requirements met in these rules tend to prevent a set of non-compliant applications and conditions, including but not limited to, the satisfaction of obligations in the context of the SCS certificate, the identification of major security incidents that could potentially lead to a data breach or leak of sensitive information, and the identification of existing or new vulnerabilities with adverse impact upon the SCS security mechanisms. The National Cybersecurity Certification Authority (NCCA) is usually in charge of issuing certificates and overseeing the certification framework of EU member states in cooperation with other surveillance authorities. A generic rule-of-thumb for compliance monitoring involves the regular sampling of services in terms of the provided capabilities and its assurance levels (No & Vasarhelyi, 2017). The assessment of the SCS service will be done either by an independent assessor or by a CAB (according to the assurance level of the SCS).

The detailed monitoring methodology is described in CYRENE Report 3.

The overall financial cost of the compliance monitoring must be covered by the SCS-P (shared by the business partners involved in a way that has been specified by the Mutual Recognition Agreement-MRA), and not by the auditors or the certification authority. The most prominent deviations or irregularities that could be considered as non-compliant elements during the provision of a SCS include:

- Information mismatch between the supplied version of the certificate to the assessor and the version which has been established in the currently running environment.
- Deviation in the requirements met within a certificate content and the supplementary information required for that certification in terms of its format, documentation, and management aspects.
- Irregularities regarding the certification validity requirements including the inability to proceed with maintenance activities, enforce the supplied terms and conditions of the certificate, or deviate from the certified development and operating services.

The monitoring of SCSs security requirements and services require the transmission of the appropriate information to a reliable assessor to both avoid the certification of a service in case the evaluation is still undergoing, and declare it as certified only for the scope specified within the certificate. Furthermore, the available dispositive of a SCS-P should be used to track any significant changes compared to the previous set of obligations, identifying in this way the established market surveillance activities that measure the quality of service and handle any possible complaints. Such complaints, as well as an assessment of the gravity of irregularities, could be potentially resolved with a periodic dialog between the issuers of the certificate and the SCS certificate owner. Failure to meet obligations regarding complaints towards maintaining the certificate validity and deviations from evaluation requirements are considered as serious non-compliant commitments. At this point, it is worth noticing that for the case of assessor evaluation (not-self assessment) the NCCA could be also informed about the results of the aforementioned activities to proceed to a formal check and feedback about the stated certificate obligations. On the other hand, identified

non-compliant conditions which do not fall under the scope of the certificate have to be still recorded and reported to the permitted audits as a medium of the quality monitoring process.

The SCS-P must present a set of procedures (as agreed by all business partners in the MRA) regarding the critical security requirements referenced at the start of this compliance monitoring section. Among them, the obligation to inform the conformity authority about major security incidents, changes in the certified service, or within the SCS- Information Security Management System (ISMS) where all security information (e.g., SCS-threats, vulnerabilities, controls, SCS-risk documentation, SCS-security policy, individual security policies of all partners) of all SCS elements (processes, assets, business partners) are maintained, is the most crucial one. All security compliance monitoring activities can be assessed using the incident management policies defined in the SCS beneath. In case serious non-compliant security issues are found, then a series of evaluation tasks must be performed to confirm the impact of non-conformity in cooperation with the assessor.

RATIONALE

Additional information from the EUCSA

Article 58, on NCCAs, includes:

7. National cybersecurity certification authorities shall:

(a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities.

Article 59, on Peer reviews, includes:

3. Peer review shall assess: (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates pursuant to point (a) of Article 58(7)

12. Certificate Management

In this section we will propose the conditions for issuing, maintaining, continuing the CYRENE certificates, as well as the conditions under which the extension or reduction of the certification's scope will be revalued.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification; Article 56 on Cybersecurity Certification also covers this issue: 9. A European cybersecurity certificate

shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.

In Figure 3 below, the process describing the issue and maintaining of a certificate is described.

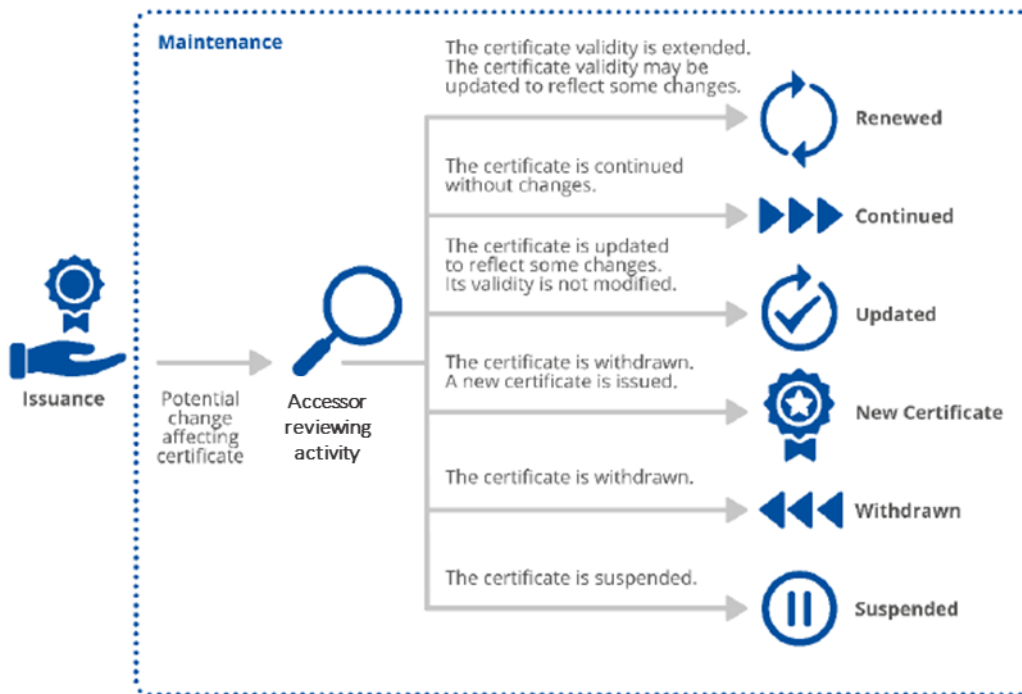


Figure 4: Processes related to the issuance and maintenance of a certificate

The reference standard for these activities is ISO/IEC 17065³ and in particular, its Clause 7.10, where ‘changes affecting a certificate’ are discussed.

Conditions for issuing a certificate

An assessor shall only issue a certificate when:

- the applicant has committed to all obligations that need to be fulfilled under this scheme to obtain the certificate;
- the evaluation of the SCS is successful and in line with the evaluation requirements set in this scheme in *Appendix D – Conformity Assessment for Level Substantial and High*, and *Appendix C – Conformity Assessment for Level Basic* or the requested assurance level and in *Appendix B - Meta-Approach for the Conformity Assessment of Supply Chain Services*) ; and

³ <https://www.iso.org/standard/46568.html>

- the review of the evaluation results is successful and in line with the requirements of ISO/IEC 17065 and with the requirements set in [Appendix B: Meta-Approach for the Conformity Assessment of SCSs](#).

The review shall be performed independently of the evaluation, and it shall cover all reports provided during the evaluation to ensure that the conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied.

The certificate shall be related to the version of the supplementary cybersecurity information produced by the vendor as specified in Article 55 of the EUCSA.

The assessor shall establish a period of validity for the certificate that shall not exceed the maximum period defined in [Chapter 19: Certificate Validity](#).

Conditions for maintaining a certificate

During the validity period of the certificate, periodic reassessments are required to ensure that the SCS-P continues to fulfil the requirements set in this scheme. Such periodic re-assessments shall not be separated by more than one year. This period may be reduced by the assessor if there are specific attention points that require an earlier reassessment.

Maintenance activities shall be initiated upon the following conditions:

- when the SCS has been selected through the sampling rule installed for the general monitoring of certified SCS, as defined by [Chapter 11: Compliance Monitoring](#)
- following a confirmed nonconformity with security requirements, under the conditions defined in [Chapter 13: Non-Compliance](#) ;
- following an identified non-compliance with the accreditation requirements of the assessor, the EUCSA provisions, or the scheme requirements, that affects the certification.

Maintenance activities may be initiated on the request of the owner of the certificate upon one of the following conditions:

- a periodic reassessment is due to be performed;
- a renewal assessment is required to extend the validity period of the certificate;
- a change of the certified SCS requires an update of the content of the certificate of the information published in compliance to Article 55(1);
- a significant change occurs in the certified SCS or in the design and implementation of the security measures that fulfil the requirements of this scheme.

Depending on the nature of the previous conditions, and in accordance with the requirements established in Chapters, [Chapter 11: Compliance Monitoring](#), [Chapter 13. Non-Compliance](#), and [Chapter 14: New Vulnerabilities](#) and the maintenance activities shall be triggered at the discretion of the SCS-P, the assessor, or the NCCA. The National Accreditation Body may also trigger maintenance activities where a complaint has been issued.

When the maintenance activities are initiated by the SCS-P, the request to the assessor shall be accompanied with an Impact Analysis Report (IAR).

In all other cases when the maintenance activities are initiated by any other party (assessor, NCCA, and any stakeholder acting as a sponsor of the associated maintenance activities), the request shall be supported by a maintenance rationale containing a description of the potential or actual non-conformity or the identified non-compliance stated and its potential impact on the certificate.

Based on the IAR or the maintenance rationale and on the requirements defined in this scheme for re-assessment or renewal, the assessor shall validate whether some evaluation tasks are deemed necessary before its review and decision and validate accordingly the scope of and the workload associated to these tasks. The assessor shall also validate the result of the necessary evaluation tasks once completed.

Typical conformity assessment activities are defined as:

- Periodic conformity assessment, including a partial re-assessment of the SCS, to be performed at regular intervals, during the validity period of the certificate, as defined in [Chapter 19: Certificate Validity](#).
- Renewal conformity assessment, including a full re-assessment of the SCS, to be performed before the expiration date of the certificate.
- Restoration conformity assessment, following a request from a SCS-P to consider changes in the certified SCS, or following a request from an assessor or from the NCCA related to a nonconformity (13. Non-Compliance) or to a new vulnerability (14. New Vulnerabilities).

The SCS-P shall support the assessor for the conformity assessment activities deemed necessary, unless otherwise specified in [Chapter 13: Non-Compliance](#)

Upon review and decision of the assessor, the maintenance activities shall result in one the following decisions:

- continuing the certificate, corresponding to keeping the existing certificate alive, without change;
- updating the certificate to reflect some changes in the certified SCS, including an extension of its scope;
- renewing the certificate with a new validity period and optionally some updates, corresponding to re-issuing the same certificate with a new validity period;
- withdrawing the certificate, and issuing a certificate with either a reduced assurance level, or a reduced scope of the certificate to still meet the current assurance level, potentially with a new validity period;
- suspending the certificate pending remedial action by the SCS-P;
- withdrawing the certificate.

Decisions shall be accompanied with a Maintenance Report issued by the assessor, in accordance with and uniquely linked to the certificate; it shall motivate the decision and, where applicable, indicate any necessary change to the initial certificate.

In the case no maintenance has been requested for a certificate that has reached its expiration date, in the case no maintenance has been requested when a periodic assessment is due, or more generally in the case a maintenance shall be initiated and no action was taken by any of the responsible parties in due time the certificate shall be suspended and the SCS-P notified of the non-compliance. If the SCS-P does not perform the maintenance in due time (as defined in [Chapter 13. Non-Compliance](#)), then the certificate shall be withdrawn.

All withdrawn certificates shall be subject to archiving. Archiving shall consist of still providing access to the certificate and associated information, with the clear indication of its withdrawal, for instance that its expiration date has passed.

The following table shall be considered by the assessor to support the appropriate decision on most frequent possible cases.

Table 5: Nominal decisions associated with the maintenance of certificates

Cases	Nominal decisions
The maintenance evaluation activities have been performed and reviewed, and have determined that the SCS still fulfils the requirements without significant changes in the service	Continue the certificate until the next periodic assessment or until its expiration date
The maintenance evaluation activities have been performed and reviewed, and have determined that the SCS still fulfils the requirements, and the changes impact the security of users without any reduction in the scope of certification or AL	Update the certificate with the new information and continue the certificate until the next periodic assessment or until its expiration date
A renewal conformity assessment has been performed and reviewed, and have determined that the SCS still fulfils the requirements, possibly with changes that impact the security of users without any reduction in the scope of certification or AL	Renew the certificate with a new expiration date and if required with the new information
The maintenance evaluation activities have been performed and reviewed, and have determined that the SCS only fulfils the requirements after reducing the scope of certification or reducing the assurance level	Withdraw the certificate and issue a new certificate with the reduced scope or assurance level, possibly with a different expiration date
The maintenance evaluation activities have been performed and reviewed, have determined that the SCS does not fulfil the requirements anymore, and action from the SCS-P is possible to maintain the certificate at the same assurance level and scope, though not immediately, or improper use of the certificate is not solved by suitable retractions and appropriate corrective actions by the SCS-P.	Suspend the certificate pending remedial action from the SCS-P
The maintenance evaluation activities have been performed and reviewed, and have determined that the SCS does not fulfil the requirements anymore	Withdraw the certificate

The periodic assessment has not been performed in due time	Suspend the certificate pending remedial action from the SCS-P.
Remediation action has not been performed in due time after suspension	Withdraw the certificate

A certificate shall only remain in the ‘suspended’ status for a maximum duration of three months that may only be extended with the explicit and motivated approval of the NCCA. In case no action is taken by the vendor in due time the status of certificate shall be changed into ‘withdrawn’ by the assessor.

Any change of the status of a certificate shall be disclosed without undue delay according to the requirements of [Chapter 20: Disclosure Policy](#).

RATIONALE

Requirements have been established considering the requirements associated with ISO/IEC 17065, and ISO/IEC 17067, Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes.

The full life cycle of a certificate, starting from its issuance with a defined validity period till its due or potential expiration (by validity period or preliminary to this due to a selection under the sampling rules for the general monitoring of certificates, a potential or actual non-conformity with security requirements, or an identified non-compliance with the accreditation requirements of the assessor, the EUCSA provisions, or the scheme requirements) has been considered.

One fundamental condition for issuing a certificate for the SCS is successful evaluation, based on the present scheme. Other conditions stem from relevant provisions of the ESA, such as necessary authorizations for assessor based on Article 60.3 of the EUCSA which are external to the certification in its technical meaning, and may, if not fulfilled after certification, be considered as non-conformance cases.

All other certification activities are related to the phase after the certificate is issued, where ‘a change affecting certification’ occurs as mentioned in ISO/IEC 17065. These activities are described as ‘maintenance’. In that case, the assessor is obliged to act in response to a given trigger.

Wording from ISO/IEC 17065 describing all relevant activities related to the certificate which has been issued applies (see Clause 7.10).

13. Non-Compliance

We need to propose here according to Art. 54 (1) rules concerning the consequences for SCSs that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the CYRENE proposed EUSCS scheme.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(1) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

[Chapter 11: Compliance Monitoring](#) defines several categories of non-compliance instances that may be uncovered through monitoring activities. When such non-compliance instances are uncovered, the consequences for the various stakeholders, including the SCS-P, the assessor and its subcontractors, and the NCCA, are as follows.

For confirmed deviations or irregularities associated to non-compliance by a SCS-P to the requirements related to a certificate issued on their SCS, the following consequences shall occur in the general case:

- the assessor who has issued the certificate shall request the SCS-P for assertions and amendments to restore compliance, to be provided within the time frame of 14 days for certificates at the assurance level ‘high’, or 30 days for certificates at the ALs ‘basic’ or ‘substantial’;
- continued non-compliance past the allowed time frame shall trigger a suspension of the certificate for the SCS, a suspension of all certification activities by the assessor on behalf of the SCS-P for other services, with information about the suspension by the assessor to the NCCA.

In the particular case of a confirmed deviation from the requirements of the certificate holder’s obligations towards maintaining the certificate validity, or towards informing the appropriate authorities or bodies of any subsequently detected vulnerabilities, as requested by Article 56.8 of the EUCSA, the following consequences shall occur:

- an immediate suspension of the certificate, with information about the suspension by the assessor to the NCCA.

For a SCS certified at assurance level High, in the case of a confirmed deviation from the requirements of the certificate holder’s obligation of informing the appropriate authorities or bodies of any subsequently detected major non

-conformity to the requirements of the scheme through continuous monitoring, the following consequences shall occur:

- an immediate suspension of the certificate, with information about the suspension by the assessor to the NCCA.

The notification of the owner of a certificate of the suspension of the certificate shall mark the beginning of a suspension period of 14 days for certificates at the AL High, or 30 days for certificates at the assurance levels Basic or Substantial. During this period:

- the impact of the non-compliance on the certified SCS shall be estimated with the necessary support (where necessary, support shall imply financial support to described activities) of the SCS-P;
- when the non-compliance is verified to impact a certificate, this shall be treated as a non-conformity of the certified SCS, the assessor who has issued the certificate shall request the SCS-P for assertions and amendments to restore compliance;
- the SCS-P shall accept or refuse the handling of the verified nonconformity and the associated maintenance activities, as defined in Chapter 12 (Conditions for issuing, maintaining, continuing and renewing certificates);
- when the handling is refused, the certificate shall be withdrawn;
- when the handling is accepted, the SCS-P shall proceed to the necessary changes to the SCS;

- when the defined period is not sufficient for the above described task, the issuer of the certificate, upon receiving a duly justified request, may extend the grace period, no more than three times the above described duration;
- when necessary (e.g. lack of availability of the assessor), the assessor may decide to further extend the suspension period up to a maximum of 90 days;
- if at the end of the suspension period, the handling of the verified non-conformity and the associate maintenance activities have not been completed, then the certificate shall be withdrawn.

ENISA shall be informed for publication on its website, and provided with all the information to be published:

- at the suspension of the certificate;
- at any extension of the suspension period;
- at the end of the suspension of the certificate;
- at the withdrawal of the certificate.

In the case of a suspension or of the extension of a suspension, the information provided to be published to ENISA shall include at least the end date of the suspension period, the reason for the suspension, and recommendations for the users of the certificates.

The NCCA shall be informed at any extension of a suspension period.

For a confirmed non-compliance in the conditions under which the certification takes place and that are not related to the individual SCS, the concerned assessor shall proceed, under the control of the NCCA, to the following:

- the identification, with the support of relevant teams and subcontractors, of potentially impacted certified SCS;
- where deemed necessary by the assessor, or at the discretion of the NCCA, the request for a series of conformity assessment activities to be performed on one or more SCS by either the assessor or subcontractor who performed the audit or any other CAB or subcontractor that would be in a better technical position to perform these activities, leading to updated assurance reports;
- the review by the assessor of the updated assurance reports, and where necessary, the re-issuance of certificates in accordance with the requirements of Chapter 12 (Conditions for issuing, maintaining, continuing and renewing certificates), or the notification to the SCS providers of the impacts of the non-compliance on their certificates.

These activities shall occur within the maximum period of 14 days for certificates at assurance level High or 30 days for certificates at ALs Basic and Substantial, which may only be extended after approval by the NCCA.

When an assessor or the NCCA mandates new evaluation activities to be performed, these activities and the related review and issuance activities shall be supported (where necessary, support shall imply financial support to described activities) by the assessor that proved to be non-compliant (or by a subcontractor of the assessor if that subcontractor proved to be non-compliant in breach of its contractual obligations).

Where impacts are confirmed to affect a certificate, they shall be treated as a nonconformity of the certified SCS, following the above-defined rules.

RATIONALE

Additional information from the EUCSA

Recitals provide additional information: (65) National cybersecurity certification authorities should in particular monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes established in its respective territory in relation to the EU statement of conformity, should assist the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies by providing them with expertise and relevant information, should authorise conformity assessment bodies to carry out their tasks where such bodies meet additional requirements set out in a European cybersecurity certification scheme, and should monitor relevant developments in the field of cybersecurity certification. National cybersecurity certification authorities should also handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by those authorities or in relation to European cybersecurity certificates issued by conformity assessment bodies, where such certificates indicate assurance level ‘high’, should investigate, to the extent appropriate, the subject matter of the complaint and should inform the complainant of the progress and the outcome of the investigation within a reasonable period. Moreover, national cybersecurity certification authorities should cooperate with other national cybersecurity certification authorities or other public authorities, including the sharing of information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with specific European cybersecurity certification schemes. The Commission should facilitate that sharing of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the Rapid Alert System for dangerous non-food products (RAPEX), already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.

This is a rather simple set of rules:

- The main ruleset is about non-conformity in the SCS (and its operation). The way in which it is discovered is not mentioned here, most likely through monitoring or complaints.
 - In that ruleset, the SCS-P has an opportunity to fix the issue without any visible consequence (no suspension, no withdrawal).
 - If they fail to do this timely, then a suspension occurs.
 - There is one exception, when a SCS-P fails in its continued assurance and maintenance duties; then, the suspension occurs directly. This is intended to highlight the responsibility of the SCS-P to continue working on security after the issuance of the certificate; also, it highlights the fact that, at that stage, the assessor only gets involved (with an opportunity to perform evaluation activities) if the SCS-P reports issues as planned.
- The second ruleset is about what happens when a suspension occurs (directly or after failure to act swiftly when a non-conformity is discovered).
 - Another delay starts running, this time with notification of the NCCA, and with publicity through ENISA’s Web site (including automated notification of customers who have registered for updates on the certificate with ENISA).
 - If need be, the delay can be extended, when duly justified. The NCCA is notified of extensions, and my signal at some point that “enough is enough”.
 - When the delay expires, withdrawal occurs; withdrawal may also occur if the SCS-P refuses to implement corrective actions.
- The third ruleset is about what happens when an assessor fails to do their work properly.
 - All certificates issued by that assessor have to be reviewed. That review may involve some work.

- If that review shows that certificates are impacted, then some evaluation work may need to be redone, as well as the corresponding review work, and if needed, the modification of the certificate.
- SCS-Ps are notified when their certificates are impacted, but they are no held directly responsible for the work that needs to be redone. However, if a non-conformity is identified in their SCS during that review, then this non-conformity needs to be handled following the first ruleset (and the second if needed).

In all cases, the entity responsible for the non-conformity is responsible for supporting the additional work, including, but not limited to, additional costs.

14. New Vulnerabilities

In this section, we will propose the rules regarding the way that the previously undetected cybersecurity vulnerabilities in SCSs shall be reported and handled.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

14.1 Vulnerability handling

SCS-Ps shall make use of the provisions of ISO/IEC 30111 for a reference of the steps involved for the handling of vulnerabilities. Such steps include the following main phases: preparation, receipt, verification, remediation development, release, post release. In the rest of this section, such steps shall be adjusted to the application rules and domain-specific context of the current scheme.

Preparation

SCS-Ps in collaboration with their respective business partners shall develop methods and establish communication channels for receiving and publishing vulnerability information. For example, as usually established via a Mutual Recognition Agreement (MRA), all partners have agreed to continuously inform the online SCS-ISM hosted and supported by the SCS-P. Information sharing is a main obligation as described in the MA.

Receipt

New vulnerability information can become available in a variety of ways. The most common ways of receiving information about new vulnerabilities include:

- the SCS-P of the certified SCS receives vulnerability information according to Article 55.1.(c) of the EUCSA;
- there is a new publicly disclosed vulnerability on the referenced online repositories according to Article 55.1.(d) of the EUCSA;
- the SCS-P finds out a related vulnerability to its certified SCS in any other way,

In any of the above cases, the SCS-P shall begin implementing certain policies and procedures for handling the vulnerability. Such policies and procedures have been previously established and agreed-upon by all parties involved SCS-P(s), business partners) and have been captured in an MA. In case that the potential risk introduced by the vulnerability towards the SCS is evaluated as major, then the SCS-P shall report without delay to the assessor that issued the certificate a description of the vulnerability, together with a description of its impact.

The time between the SCS-P becomes aware of a new vulnerability and the notification of the assessor shall not exceed five (5) working days. Failure to notify the assessor of a vulnerability with major impact or notification after five (5) working days shall be considered as a non-compliance to the rules of the scheme, as defined in Chapter 13 (Non-Compliance).

The notification of the assessor by the SCS-P of a new vulnerability may occur before the vulnerability analysis is finalised. To avoid potential delays in the notification process, a maximum of ninety (90) days after the identification of a new vulnerability is allowed before the SCS-P delivers the full vulnerability analysis to the assessor.

The vulnerability analysis shall include information about the possible exploit(s) of the vulnerability. To help quantify such exploits and ensure appropriate levels of protection, a classification scheme shall be followed. The Traffic Light Protocol (TLP) classification⁴ is a commonly used scheme for such purposes but any alternative classification and mechanisms previously agreed between the SCS-P and the assessor shall be also accepted.

Verification and Remediation Development

In addition to the security controls defined in [Appendix A: Security Objectives and Requirements for SCSs](#), the SCS provider's processes shall include the following steps:

- In its analysis of the vulnerability with major impact, the SCS-P shall propose (1) whether the certificate should be suspended until a remediation is released, and (2) whether a restoration conformity assessment should be performed on the supply chain service after remediation. The assessor shall agree on the proposed actions or make alternative proposals within five (5) working days.
- If a maintenance conformity assessment has been deemed necessary, it shall be performed before lifting a potential suspension of the certificate.

Release and Post-Release

There are no specific rules related to these phases.

14.2 Vulnerability disclosure

SCS-Ps may use the ISO/IEC 29147 standard as a reference for the general rules related to vulnerability disclosure.

For the duration of the vulnerability analysis process, the SCS-P may apply an embargo period, meaning that the possible vulnerability is not further disclosed for a period no longer than ninety (90) days. The NCCA may choose to extend or reduce the duration of this embargo period in order to facilitate the needs of other SCS-Ps or SCS customers.

⁴ <https://www.first.org/tlp/>

Once a remediation strategy has been defined by the SCS-P and approved by the assessor, information related to the confirmed vulnerability shall be disclosed to the NCCA, in accordance with the reporting standards established by the NCA. This reporting shall contain all necessary information which will allow the NCAA to understand the potential impact of the vulnerability, the necessary corrective steps taken for its mitigation and how these affect the SCS itself, and the potential for the vulnerability to affect other SCSs. Finally, the reported information shall avoid describing details about the possible exploitation of the vulnerability.

The NCCA shall make the reported information available to other NCCAs which may also decide to further investigate the vulnerability. As part of such investigation an NCAA can choose to further analyze the information internally or, after informing the SCS-Ps about the information exchange, ask the related assessors to analyze whether further SCSs can be affected. In any case, all information exchanges related to the investigation of a new vulnerability shall adhere to the principles of confidentiality by making use of encrypted communication channels and need-to-know access to the information.

The final step of the disclosure process of a new vulnerability occurs when a correction has been brought to the SCS to mitigate the risk introduced by such vulnerability. Once this has been established, the SCS-P shall create or update the necessary CVE entry, supported by the NCCA and, if necessary, the national CSIRT. The CVE shall then be published on the relevant list and ENISA shall be informed. NCAAs are expected to coordinate the new vulnerability disclosure process, as defined in ISO/IEC 29147, or choose to transfer the coordination role to their national CSIRT. In that case, the CSIRT shall be provided with all necessary access to all information related to the vulnerability and the affected SCSs.

15. Record Retention

We need to propose here according to Art. 54 (n) rules concerning the retention of records by conformity assessment bodies (CABs).

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(n) where applicable, rules concerning the retention of records by conformity assessment bodies;;

Each CAB shall maintain a records system in accordance with the requirements of the accreditation standard ISO/IEC 17065 (or to the applicable accreditation standard for its internal or external evaluation facilities, e.g. ISO/IEC17021-3).

The records system shall include all records and other documents produced in connection with each conformity assessment, as well as documents and evidence provided by the SCS-Ps about the implementation of security controls; the record system shall also include a list of all the documents and evidence made available temporarily by the SCS-P during the conformity assessment. It shall be sufficiently complete to enable the course of each certification to be traced.

All records shall be securely and accessibly stored for a period of at least seven (7) years after the expiration or withdrawal of the certificate.

If the certification scheme involves complete re-evaluation of the product(s), processes and/or services within a determined cycle, records shall be retained at least for the current and the previous cycle. Otherwise, records shall be retained for a period defined by the certification assessment body.

In case a later expiration date of the certificate is attributed in accordance with the conditions of Chapter 12 (Certificate Management), it shall be taken into account for the new calculation of the retention period of the records, with the same rule as previously stated. New or revised information related to the activities described under Chapter 12 (Certificate Management) shall be added to the previous records for the certificate.

For legal and practical reasons records shall be stored securely until minimum retention periods have expired, but no longer than required to support the business needs of the SCS-P.

In defining retention times, legal circumstances and recognition arrangements shall be considered.

RATIONALE

The proposal is to require records to be kept for seven (7) years after the expiration of the certificate, or until legal actions related to the certificate are completed.

If the certificate is renewed, then the records are kept for seven (7) years after the new date, with a full history of the certificate, including records related to all conformity assessments.

Also, there is a split responsibility between the CAB and the SCS-P regarding the documents and evidence that the SCS-P made available in a restricted manner to the CAB: It is the SCS-P's responsibility to keep these records, while the CAB only maintains a list of the documents.

16. Related Schemes

This section includes the identification of national or international cybersecurity certification relevant schemes (if any) covering the SCS security requirements, evaluation criteria and methods, and assurance levels, based on Art. 54 (o).

According to "Art. 54 (o)", a valid European cybersecurity certification scheme has to include a set of elements that successfully cover the same type of categories of ICT products, services, and processes, as well as the security requirements, evaluation criteria, methods, and assurance levels that fall into them (ENISA, 2020). Today, several cybersecurity certification schemes apply on a national level and tend to cover similar categories of services. Inspired by the ISO-27001, which meets high-security standards, highlights the risks in data sharing in the context of any supply chain ecosystem, and proposes a series of prevention and mitigation measures.

The Federal Office for Information Security (BSI)⁵ promoted its cybersecurity certification scheme for the federal government of Germany. It targets audiences and people from the areas of compliance and

⁵ https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

information security who desire to control and monitor their confidential data under the criteria and audit methodologies described within the C5 scheme (BSI, 2017). Doing so, they can assess the information security and deduct detailed reports about the security posture of their organization, taking into consideration several variables including but not limited to policies, personnel, asset management, physical devices, operations, cryptography, communication, etc. At this point, it is worth mentioning however that this scheme provides partial only coverage of the requirements that should be met in a supply chain environment. Therefore, the design and provision of a novel and EU-compliant cybersecurity certification scheme must be transformed into a certificate under the SCS scheme and validate that its security requirements follow the guidance issued by the (ENISA, 2020) or any other collaborated member capable of issuing a declaration of conformity (Mitrakas, 2018). In case the differences between the related schemes are too great to bridge, then methodologies like reuse of evidence and evaluation of results could still lead to the definition of a novel SCS scheme by clarifying its documentation, certificates, and reports, allowing in this way its adoption by smaller vendors and supply chain infrastructures. The European Cyber Security Organization supports several Working Groups which aim to increase industrial competitiveness in Europe, including the WG1: Standardization, Certification, and Supply Chain Management (ECSO, 2017). The latter contributes to defining the necessary activities for the pre-standardization, standardization, development, and use of trusted European certified solutions across supply chain sectors.

17. Certificate Format

In this section according to Art. 54 (p) we need to propose the content and the format of the CYRENE cybersecurity certificates and the statements of conformity to be issued;”

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

RATIONALE

A proposal for the Certification Report format is included in Appendix E: (Scheme Document Content Requirements). A proposed format for the certificate itself will be added later after the approval of the proposed scheme.

18. Availability of Information

We propose here according to Art. 54 (q). the period of the availability of the CYRENE statement of conformity, technical documentation, and all other relevant information to be made available by the SCS business partners.

The cybersecurity certification scheme provided to SCS business partners in the context of the CYRENE project has to explicitly state and clarify its availability of information. This availability of information includes the period of the availability of the EU statement of conformity, the technical documentation of the scheme, as well as any other type of information deemed appropriate by the provider of the ICT product, service, or process. This is feasible by maintaining and continuously updating a publication system that includes all information that could be made publicly available without compromising the security of the system beneath. Such information should remain available for a period of at least seven (7) years after the expiration of the withdrawal of the SCS certificate. In cases where the expiration date of a certificate extends later, then it must comply with the activities described within the Certificate Management chapter of this report. Furthermore, any updates or revision of information upon the documentation that affect the same set of activities must also take into consideration the same management procedures of the certificate.

Records of information that were used to formulate the conformity assessment process of the SCS certificate, must always remain both accessible and stored in a secured manner. This kind of information should become evident only to the appropriate personnel (e.g., the Conformance Assessment Body) and keep intact following the duration defined in the Record Retention chapter of this report as well. It is a common practice in the industry to keep records of information up to five (5) years after the expiration of the certification. Typical pieces of information included in these records involve the documentation and all evidence used during the conformity assessment -even the ones which were initially characterised as restricted- for a limited only time or on the premises of the service provider. The service provider however may extend the information retention and availability period up to ten (10) years in case he desires to satisfy stricter documentation criteria that could be potentially met in SCS domain.

Furthermore, the validity of a certificate shall require the partial update of its information over the years, something which immediately marks the replaced information as deprecated or even worst obsolete. On these occasions, the deprecated and obsolete information must be also archived and comply with the seven (7) years policy of the availability of information. The period of documentation retention of the service provider cannot be shorter than the retention of records of the CAB after the end of the validity period of the certificate. This requirement finds application especially on confidential information shared between these two parties and aims at ensuring that the service provider has all the necessary documentation available in his repository, rather than the publicly available one which is usually stored in the premises of the CAB. Finally, the retention policy of documentation should of course comply with the obligations defined by the national strategies of the relative SCS, as well as the directives and the General Data Protection Regulations that should be met on a corporate EU level (Markopoulou, et al., 2019).

19. Certificate Validity

According to Art. 54 (r) we propose here the maximum period of validity of the cybersecurity certificates issued under the CYRENE SCS-scheme;”

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(r) maximum period of validity of European cybersecurity certificates issued under the scheme;

The maximum period of validity of the certificates shall be three (3) years. To maintain the validity of the certificate for its full period of validity, the SCS-P shall follow the processes defined in [Chapter 12: Certificate Management](#), and the certified SCS shall be subject to a periodic conformity assessment or to a renewal conformity assessment at most one (1) year after the previous initial, periodic, or renewal conformity assessment.

Under certain conditions, and following the processes defined in [Chapter 12: Certificate Management](#), an assessor may continue a certificate with an extended validity period beyond the initial three (3) years.

RATIONALE

According to the large variety of SCS that can be certified under this scheme, to their and evolution (often with frequent updates), to the various levels of assurance that can be achieved and the associated effort to generate assurance that the scheme's requirements are fulfilled, an average maximum of three (3) years was selected for the general case.

Since this is a maximum, it remains possible to issue a certificate for a shorter period of time, in particular if the assessor believes that issuing a certificate for three (3) years would lead to potential risks.

The chapter also defines the 1-year limit between periodic assessments. This limit applies to all levels, but the nature of the activities to be performed depends on the level.

20. Disclosure Policy

According to Art. 54, (s) a disclosure policy (when, how, by whom) is proposed for European cybersecurity certificates issued, amended or withdrawn under the CYRENE scheme;”

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme.

The certificates shall be disclosed by ENISA (in case the CYRENE scheme has been adopted), with the related certification report and any relevant information as requested by other chapters of this document, in a dedicated website on European cybersecurity certification schemes, in accordance with Article 50.1 of the EUCSA.

The certificates shall be disclosed with their applicable status, as decided through the application of the requirements established by [Chapter 12: Certificate Management](#) and [Chapter 13: Non-Compliance](#).

The certificates may also be disclosed by the NCCAs and the issuing assessor on their websites in case of SCS of AL higher than basic. Any change to the status of a certificate shall be reported to the NCCA and to ENISA.

Amendments and withdrawals of certificates resulting from maintenance activities shall as well be published, in a way that users of certificates can identify which versions of a certified SCS are certified (where applicable) and which relevant information shall apply (such as guidance).

Information about the European cybersecurity certification schemes and their updates will be made available on the ENISA website. It shall be available at least for the entire period of validity of the certificate.

The certificates may be complemented with additional information, such as a QR-code providing a direct link to the corresponding certificate and related information, as to offer a better user experience and to publicise the certificates. ENISA may therefore establish a procedure for the generation of a QR-code: such procedure may imply that assessors, ahead of the release of a certificate, request from ENISA the generation of the QR-code to be applied on the certificate and provided to the SCS-Ps for their commercial and technical documents.

SCS-Ps may use certificates published on ENISA's website for commercial purposes, but they shall not modify the certificate, and in particular, they shall always include a link to the original certificate on ENISA's website to allow customers to check the current status of the certificate. Only SCSs with a valid certificate shall be promoted as certified SCSs by their relevant SCS-P, or users of these services.

If a certificate is suspended, the information published on ENISA's website shall include the date of the end of the suspension period, a reason for the suspension, as well as recommendations for the users of the certificate.

Once a certificate has expired or has been withdrawn, ENISA shall move it to a dedicated archive part of the website, where it shall remain available for at least (5) years. SCS-Ps shall not refer to such expired or withdrawn certificates in their commercial information, and any access to the expired or withdrawn certificate through its initial URL or QR-code shall lead to the prominent display of the current status of the certificate.

RATIONALE

ENISA will publish the certificates with appropriate relevant information attached. To manage accurate and up to date data flows, ENISA will establish conditions and/or guidance for the delivery and publication of information.

In accordance with Chapter 17 (Certificate Format), both certificates and associated certification reports, as well as relevant information for the secure configuration and usage of the certified SCS (guidance) shall be made available to the users (and potential users) of certificates. Amendments to certificate will also need to contain the same type of information as the issuance of certificates, including guidance, and users shall be given an easy access to the status of the certificates when using ENISA dedicated Website.

As to offer an easy access to the Supplementary cybersecurity information defined by Article 55, a validated link to that information will be made available into the certificate.

ENISA shall be informed without undue delay of the evolution of the certificates, be it an amendment or a withdrawal, in line with the requirements of relevant Chapters of this scheme and Recital 93 of the EUCSA.

As to offer the necessary flexibility and enforcing character of the conditions for presentation of the information to ENISA, and for its publication, ENISA will establish generic conditions and/or guidance.

The generic conditions and/or guidance should make sure information is accurate and up to date as the information provided by ENISA could act as a single point of reference. It should define what information is to be transmitted to ENISA and within what reasonable timeframe. According to principles of transparency and openness, the outlines of these conditions/guidance should be made public on the ENISA Website.

As to promote valid certificates, certificates that have expired will be archived and made available on a different webpage than the valid ones.

In case of self-assessment, the assessor will provide proposals to the SCS-P, and the SCS-P (with the agreement of the business partners) will issue a “non-official certificate”

21. SCS Mutual Recognition Agreement (MRA)

In this section we propose the conditions for the mutual recognition of certification schemes with third countries, which information shall include the business agreement.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(t) conditions for the mutual recognition of certification schemes with third countries;

The mutual recognition of certification schemes with third countries shall be supported by the establishment of a SCS Mutual Recognition Agreement (MRA) between the SCS business partners (EU and non-EU partners).

This SCS MRA may include the following information:

- participants to the SCS MRA;
- purpose and spirit of the Agreement;
- membership;
- scope;
- exceptions;

- definitions;
- conditions for recognition of certificates;
- peer assessments;
- publications;
- sharing of Information;
- acceptance of new participants and compliant authorities or bodies;
- administration of this Agreement;
- disagreements;
- costs of this Agreement;
- revision;
- duration;
- voluntary termination of participation;
- commencement and continuation;
- effect of this Agreement.

Conditions for recognition of certificates by participants to such an Agreement shall include at a minimum the following conditions:

- the participants shall commit themselves to recognise applicable conformant certificates by any accepted Participant;
- acceptance of participants shall confirm that the evaluation and certification processes have been carried out in a duly professional manner:
 - on the basis of commonly accepted ICT security evaluation criteria;
 - using commonly accepted ICT security evaluation methods;
 - in the context of an evaluation and certification scheme managed by a compliant certification body in the accepted participant's country;
 - the conformant certificates and certification reports issued satisfy the objectives of this Agreement;
- certificates which meet all these conditions shall be termed as conformant certificates for the purposes of this Agreement;
- ICT security evaluation criteria are to be those laid down in [Chapter 8: Evaluation Methods and Criteria](#) of this document;
- the scheme of the participants or to which the participants adhere shall be organised with a proper National Authority and CABs, in accordance with the following requirements:
 - the National Authority supervises the certification activities, notifies and authorises where applicable CABs, and reports any vulnerability of certified to the NCCAs of the EU participants;
 - the CAB has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO/IEC 17065 and has been authorised where necessary by the National Authority;
 - the CAB is accepted as compliant by the Participants through a peer assessment mechanism installed for the SCS MRA;

- o the CAB has been where necessary subject to an assessment by the National Authority in order to confirm its competence to perform evaluations, in accordance with Chapter 7 (Specific requirements applicable to a CAB) of this document;
- in order to assist the consistent application of the criteria and methods between evaluation and certification schemes, the participants plan to work towards a uniform interpretation of the currently applicable criteria and methods and commit to accept the supporting documents that results from this work. In pursuit of this goal, the participants also plan to conduct regular exchanges of information on interpretations and discussions necessary to resolve differences of interpretation;
- in further aid to the goal of consistent, credible and competent application of the criteria and methods, the certification bodies shall undertake the responsibility for the monitoring of all evaluations in progress within the SCS MRA at an appropriate level, and carrying out other procedures to ensure that all CABs:
 - o perform evaluations impartially;
 - o apply the criteria and methods correctly and consistently;
 - o have and maintain the required business and technical competencies;
 - o adequately protect the confidentiality of sensitive or protected information.

The SCS MRA may include a limitation of the assurance level of the certificates subject to recognition.

CAB(s) of the participants of such an Agreement that issue(s) certificates at the equivalent assurance level 'high' of the EUCSA shall be subject to peer assessments in line with the procedure set up in this scheme ([Appendix D: Conformity Assessment for Levels Substantial and High](#)).

The procedure may be adapted and simplified for the CABs that issue certificates at the equivalent assurance levels 'basic' or 'substantial' of the EUCSA as to benefit from the international Accreditation system, and shall at least consist of the following activities by the peer assessment team regarding review of the:

- documentation associated to 2 certification projects of the 'substantial' assurance level; procedures associated to the security of information.

RATIONALE

Additional input from the EUCSA

The context for mutual recognition is provided in the EUCSA recitals:

(104) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries.

The text is here strongly inspired from the EUCC scheme, around which some SCS MRAs already exist. In the context of the EUSCS scheme, a number of parameters, including the evaluation criteria and methods, are specific to the scheme; mutual recognition is therefore likely to be possible only with third countries that will operate a scheme locally that use the criteria and methods defined in the EUSCS scheme.

22. Peer Assessment

We need to propose here according to Art. 54 (u) how the assessors (self-assessor or CABs) can be audited

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level “high” pursuant to Article 56(s). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

The EUSCS scheme requires that each authority or body issuing certificates at the ALI High undergo a peer assessment at periodic intervals.

While every authority or body issuing certificates for AL ‘high’ pursuant to Article 56.6 of the EUCSA, including their subcontractors, shall operate under its own responsibility, a peer assessment shall be established for those issuing EUSCS certificates at level High to:

- assess that they work in a harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composite service certification, as offered by Chapter 3 (Purpose of the CYRENE SCS scheme), including the reuse of a certified supply service evaluation results when used as base component in a composite service;
- identify any potential strength that result out of their daily work and that may benefit to others;
- identify any potential weakness that result out of their daily work and that shall be considered for improvement by the peer assessed CAB;
- find a harmonised way to handle non-conformities and vulnerabilities and exchange best practices regarding the handling of complaints.

Note: The peer assessment is not intended to interfere with or make judgement to the activities performed by the NCCA, as this is the subject of the peer review process as required by Article 59 of EUCSA. Nor shall it interfere with or make judgement to the activities performed by the National Accreditation Body (NAB).

In order to allow timely feedback with respect to questions of the national aspects of the scheme that are handled by the NCCA, a representative of the NCCA of the assessed CAB shall participate to the peer assessment.

The peer assessment of each CAB issuing certificates of AL ‘high’ shall take place on a regular basis, with a periodic interval that shall not exceed five (5) years.

The ECCG shall establish and maintain a planning of peer assessments ensuring that this periodicity is respected, and take into consideration the level of priority that may be given to the peer assessment of a CAB issuing certificates at the assurance level ‘high’ in case of alleged non-compliance of this CAB, and in case of CBs with recent activity engaged in certifications for the first time or after a long lasting break (more than two years).

In the case of Article 56.6.(a) of the EUCSA, both the CAB issuing the certificates and the NCCA proceeding to the prior approval for each individual certificate shall be subject to the peer assessment. This shall include the procedure established by of the NCCA for prior approval for each individual certificate.

In the case of Article 56.6.(b) of the EUCSA, both the CAB issuing the certificates and the NCCA shall be subject to the peer assessment. This shall include the general delegation requirements defined by the NCCA. Peer assessments shall be performed on site for the peer assessed CAB and, where applicable, for a selected set of its subcontractors.

The peer assessment team may decide to reuse results of previous peer assessments of the assessed authority or body covering part of the scope, under the following conditions:

- such results shall be not older than five (5) years;
- where previous peer assessments of the peer assessed CAB were performed under a different scheme, these shall be provided with the description of the peer assessment procedures in place for that different scheme;
- the peer assessment report shall clearly indicate which parts were reused without further assessment, and which parts were reused with additional assessment;

The peer assessment team shall report their findings to the ECCG in a peer assessment report, with an indication of the severity of any shortcomings. The peer assessment report shall include where necessary guidelines or recommendations on actions or measures to be taken by the peer assessed CAB, as well as the measures proposed by the peer assessed CAB to handle the findings.

When establishing measures to handle the findings, the peer assessed CAB may ask for the support of the peer assessment team. These measures shall be transmitted to the ECCG, indicating how they intend to correct the findings, within the peer assessment report. Where necessary, the ECCG may inform the relevant:

- NCCA of the peer assessed CAB for its consideration of the potential impact of the remaining findings on the certificates issued by the peer assessed CAB, or any authorisation or notification related to the peer assessed CAB and associated subcontractors;
- National Accreditation Body (NAB) of the peer assessed CAB for its consideration of the potential impact of the remaining findings on the accreditation of the peer assessed CAB and associated subcontractors; and may ask for their conclusions.

The peer assessed CAB and related NCCA shall have the opportunity to address with the ECCG any shortcomings and recommendations identified in the report, before the results of the peer assessment are published by ENISA. Also, the NAB shall have the opportunity to address any shortcomings and recommendations in case any have been brought up to the NAB before the results are published.

ENISA may participate in the peer assessments.

CABs shall inform applicants to certification at the assurance level High of the EUSCS scheme that their certification projects may be subject to the peer assessment installed by this scheme.

RATIONALE

Additional input from the EUCSA

Additional information about peer assessment is provided in the EUCSA recitals

(100) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the European cybersecurity certification framework, certain European cybersecurity certification schemes may include a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services and ICT processes with an assurance level ‘high’ under such schemes. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way, and may include appeal mechanisms. The results of the peer assessments should be made publicly available. The bodies concerned may adopt appropriate measures to adapt their practices and expertise accordingly.

In addition to the peer review between NCCAs, introduced in Article 59 of the EUCSA, which is outside of the scope of this scheme, a peer assessment may be defined for each scheme, with scheme specific objectives defined here for the EUCC scheme in the first part of this Chapter, and requirements.

This approach guarantees the high quality of evaluation activities as required for a ‘high’ level of security assurance and the harmonisation of the evaluation methods between different CAB, therefore allowing more objective results and to proceed to composite SCS certifications within different CABs.

It is essential that a planning is established for such activities, including reassessments, and necessary priorities associated to newcomers to certification, or those facing issues with certification.

The results of the peer assessment will be made publicly available on the ENISA website dedicated to cybersecurity certification, as recommended by Recital 100 of the EUCSA.

It is considered of importance that where applicable, the assessed body or authority presents the effective measures to adapt their practices and expertise accordingly to the ECCG, in order to reinsure other participants to the scheme of the quality of the certificate it issues.

In cases where the quality of the certificates is considered by the ECCG not in line with the requirements of this scheme, the ECCG may inform and consult the NCCA and the National Accreditation Body of the assessed body or authority for their conclusions on the impacts on its authorisation and accreditation.

23. Supplementary Information

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

All supplementary cybersecurity information defined in Article 55 of the EUCSA shall be provided during conformity assessment by SCS-Ps to the assessor in the course of the conformity assessment.

In particular, in accordance with the requirements of [Chapter 17: Certificate Format](#), a link to the website and relevant pages where that information is made available shall be provided to be integrated into the certificate. Once all other requirements for certification have been fulfilled, the issuing body shall request the SCS Provider to provide the URL (link) so that this can be processed before the certificate can be uploaded to the ENISA Website for certification.

SCS-Ps shall make Supplementary cybersecurity information in accordance with Article 55 of the EUCSA publicly available on their websites.

The information shall be available in electronic form and in English language and shall remain available at least until the expiration or withdrawal of the corresponding European cybersecurity certificate. It shall be updated in accordance with the requirements of [Chapter 12: Certificate Management](#).

In addition, “guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the supply chain services”, as defined by Article 55.1. (a), shall be updated as required to reflect the evolution of the supply chain service, in accordance with the requirements of [Chapter 12: Certificate Management](#).

RATIONALE

In addition to the public availability of the information, as requested by Article 55, the need for having access to all or part of it during certification may be requested, such as to test that the information complies with the requirements of the scheme. The SCS-P should have the URL up and running before the certificate is issued or updated, and provisioned with the information provided for the conformity assessment. This specific need to review part of Supplementary cybersecurity information during the conformity assessment phase shall however only occur where the relevant Chapters of this scheme establish a requirement to do so.

For an easy and harmonised access of users of certificates to the webpages where the information will be accessible on the Websites of SCS-Ps, the associated link will have to be provided in the certificate.

The conditions to deliver the Supplementary cybersecurity information should be part of a more detailed disclosure policy that ENISA will establish in accordance with the requirements of [Chapter 20: Disclosure Policy](#).

24. Additional Topics

This chapter will introduce topics that are not addressed in Article 54, but may still be relevant for the present scheme.

24.1 SECURITY PROFILES

PROPOSAL

All related certification schemes need to be considered. For example, a SCS is likely to be offered via a cloud provider. In this case the proposed SCS certification scheme (EUSCS) needs to be considered. Furthermore, a SCS (technical profile) may include IoTs among its supply chain assets then the IoT certification scheme also needs to be considered.

The applicable certification schemes may have specific requirements, related to an industry and need to be considered.

In order to simplify the use of certificates issued in the proposed EUSCS scheme in other schemes, it is therefore important to support the definition of such specific vertical requirements, and to allow supply chain services to take these requirements into consideration in their certification.

Such specific requirements shall be defined in a Security Profile, following some principles:

A security profile shall not remove or weaken any requirement defined in the EUSCS scheme.

A security profile shall not modify the assessment methodology or the assessment methods defined in the EUSCS scheme.

A security profile shall follow the processes defined in the scheme, and shall produce the same deliverables.

A security profile shall specify the EUSCS AL that it targets.

A security profile may define new security controls, or may add new requirements to an existing security control, as long as these requirements do not weaken existing EUSCS requirements.

A security profile may mandate a higher frequency of periodic assessments.

A security profile may define a dedicated section in the document templates defined in the EUSCS scheme.

A SCS-P may choose to claim conformity to the requirements of one or several security profiles in addition to the core requirements of the scheme. If this claim is confirmed by the conformity assessment, then the SCS-P may list the security profile(s) in the certificate documentation.

24.2 FORCE MAJEURE

PROPOSAL

In case of force majeure, a NCCA may take temporary measures to ensure the continuity of certification, by extending the timelines related to the periodic and renewal assessments, by relaxing requirements on

the execution of conformity assessment activities, and if necessary, by extending the validity of certificates.

The NCCA shall inform ENISA about the extension and provide transparency on reasons and the duration of extension, and ENISA shall make the information available on their website.

24.3 SECURITY OF INFORMATION

PROBLEM STATEMENT

Annex to the EUCSA, item 16: The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or MS law to which such persons are subject, and except in relation to the competent authorities of the MSs in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

RECOMMENDATION

Unless otherwise provided for in this scheme and without prejudice to existing national provisions and practices in the MSs on confidentiality, all parties^[1] involved in the application of this Scheme shall maintain confidentiality and observe professional secrecy with regard to all information and data obtained in carrying out their tasks in order to protect the following:

personal data, in accordance with GDPR [35];

commercially sensitive and confidential information and trade secrets of a natural or legal person, including intellectual property rights, during the certification lifecycle of the SCS and up to the end of the indicated retention time for all certification information, unless disclosure is necessary in the public interest, or subject to court orders;

exchange of information necessary for the effective implementation of this scheme, in particular for the purpose of peer reviews, peer assessments or audits, effective collaboration between the involved SCS business partners and their third parties, authorities and bodies, the handling of publicly unknown and subsequently detected vulnerabilities in the process of, or after certification, and the handling of complaints.

Without prejudice to previous paragraph, information exchanged on a confidential basis between the SCS business partners, the competent authorities and between competent authorities and the Commission shall not be disclosed to the public without the prior agreement of the originating authority.

All information received from the CABs or their subcontractors or the SCS-P shall only be used for the purpose of the certification and deemed confidential by the NCCAs – unless a different agreement is reached between the parties or unless an information flow is required by a specific regulation of the scheme.

All parties involved in the application of this Scheme shall implement security measures in order to ensure the confidentiality of the information provided during the certification process.

RATIONALE

Security of information is key in cybersecurity related activities. All cybersecurity certification related activities fall into the latter.

Information provided by the applicant to the CAB for certification might be sensitive, especially as, the higher the evaluation level, the deeper the evaluator shall go into the analysis of the SCS and related life-cycle, based on information details that may comprise commercially confidential information and trade secrets, including intellectual property rights.

Information developed by cybersecurity certification activities, such as Assurance Reports, which are associated to vulnerabilities assessment, handling and release, will also contain information sensitive parts that, when poorly protected, may obviously endanger the users of associated SCSs, even when these SCSs are certified.

Therefore, the obligations of the different actors of the scheme to insure the security of information shall be established and take into consideration the requirements for SCS-Ps and developers to comply with Article 55 of the EUCSA, and the necessary respect of Freedom of Information policies and legal frameworks, Access to Information Acts, and/or any other similar national, European and international policies and regulations by any individuals or entities.

24.4 COMPOSITION

PROBLEM STATEMENT

The composition of certificates is not mentioned explicitly in the EUCSA, but it is a common way of building complex services (e.g., supply chain services) by leveraging previously certified services. In the context of the EUSCS scheme, the objective is to:

Reduce the costs of certifying a supply chain service that relies on previously certified services (e.g., SCS or cloud services) by allowing the reuse of evidence and of audit results.

The use of composition leads to specific issues related to the evaluation of composed supply chain services, and also to the maintenance of the certification for composed SCSs, relatively to the maintenance of the certification of their components.

RECOMMENDATION

SCSs are layered systems, in which infrastructure and platform capabilities from a service are often used as a basis for other services. There may also be some dependencies between an application capability and another service. These services used by a SCS-P in the provision of its own supply chain service are referred to as sub-services, supplied by sub-service providers or organizations. The general rules for the consideration of such sub-service providers in the assessment of a supply chain service is covered extensively in [Appendix B: Meta-approach for the assessment of SCSs](#). In addition, SCS-Ps need to fulfil

specific requirements related to their service providers and suppliers that are defined in [Appendix A: Security Objectives and Requirements for SCSs](#).

Composition is a particular case, in which the sub-service (then called a base service) is itself a SCS that has been certified in the EUSCS scheme. In such a case the SCS (or dependent service) relying on the base service can expect the assessment of the requirements related to the base service to be greatly simplified, because they use the same security framework, and because the rules of the scheme (and in particular those related to the CABs) are trusted.

In order to be eligible for composition, the base supply chain service shall satisfy some specific requirements, defined in [Appendix A: Security Objectives and Requirements for SCSs](#), which will allow the assessment of dependent supply chain services to be further simplified. These specific requirements consist in defining precisely, in terms of specific EUSCS security objectives and requirements, how security responsibilities are split between the base service and the dependent service:

The base SCS shall provide a description of their contribution to the EUSCS requirement fulfilment of their dependent services, properly justified through references to their own controls; and

1. The base service shall provide a list of actionable requirements on Complementary Customer Controls (CCCs, based on the EUSCS objectives and requirements) that define the requirements to be fulfilled by the dependent supply chain service in order for the base service to fulfil the requirements for EUSCS certification at the chosen assurance level.

These two conditions are defined as requirements for base services in [Appendix A: Security Objectives and Requirements for SCSs](#). Therefore, they are in the scope of the conformity assessment for the base service.

This information can then be used by the SCS-P of the dependent service in several ways:

2. During the design phase, the SCS-P can use the information about the base service to drive design decisions for its dependent service;
3. When building documentation for its certification, the description of the base service's contribution and of its CCCs can be used directly by the SCS-P of the dependent service, who will simply need to document its implementation of the CCCs; and
4. The CAB only needs to verify that this information has not been modified and if necessary that a subset has been properly selected, and will focus on verifying that the CCCs are fulfilled by the dependent service.

In addition, there are a few simple rules that must be followed:

5. In order to apply composition, the base service shall be certified at a level equal or greater than the level targeted by the dependent service;
6. In order to apply composition fully, the base service shall claim compliance to the security profiles that the dependent service claims compliance to. If the dependent service claims compliance to a security profile that is not claimed by the base service, then this security profile is excluded from the composition, and a classical process shall be used if necessary to demonstrate that the base service satisfies as a subservice the expectations of the dependent service relative to that security profile;
7. The dependent service shall add to the requirements to be fulfilled the requirements from the base service's CCCs.

8. In its description of its contribution of the base service to the fulfilment of the scheme's requirements, the dependent service shall indicate when the description is the one provided by the base service in its documentation.

25. Further Recommendations

The recommendations provided in this section are not intended to be included in the CYRENE EUSCS scheme. They will be related to the lifecycle of the scheme, specifically measures to be considered between the formal adoption of the scheme and the emission of the first certificates, and measures related to the maintenance of the scheme.

They nevertheless represent important topics that will need to be addressed in order for the CYRENE EUSCS scheme to be successful. The scheme adoption topic, in particular, will be of paramount importance for this new scheme, and requires our full attention.

25.1 SCHEME ADOPTION

25.1.1 Problem statement

EUCSA Reference

Article 57 1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.

Additional information

The transition period is here considered as the period between the date of adoption of the implementing act adopted pursuant to Article 49(7), and the date established into this implementing act when national schemes shall cease to produce effect.

25.1.2 Recommendation

The CYRENE EUSCS scheme is the first scheme for SCSs at an international level. It will complement some existing EU schemes (e.g. EUCS, EUIoT) and national schemes, but it is mostly a new scheme that needs to be set up gradually across the EU.

Prerequisites for scheme adoption

In order for relevant auditors in a MS to start issuing certificates at the Basic level the following should happen:

- All SCS-Ps have identified their business partners, have conducted a SCS risk assessment and they have agreed upon the Protection Profile (PP) (security requirements, security objectives, risks, controls,) of the SCS
- Assessors in the MSs have been qualified to access the SCS-TOE based upon relevant standards

In order for relevant auditors in a MS to start issuing certificates at Substantial levels, the following should happen:

- existing and new assessors get accredited to ISO/IEC 17065, and their internal and external evaluation facilities get accredited to relevant standards;
- the NCCA notifies accredited assessors to the EC;
- assessors need to work with the NCCA to set up monitoring activities; and
- the NCCA sets up the market surveillance process.

In order for the relevant auditors in a MS to start issuing certificates at level High, the following should also happen:

- the NCCA establishes how High certificates will be issued and take the relevant action (get its assessor-NCCA accredited, and/or designate an assessor for general delegation, and/or organise a prior approval process of certificates); and
- existing and new assessors, including their internal or external evaluation facilities get authorised by the NCCA before notification to the EC;

In addition, before relevant auditors in any MS can start issuing certificates, the following should happen at European level:

- a maintenance organization is put in place for the CYRENE EUSCS scheme, to further develop the scheme and to support any interpretation and harmonisation question related to the adoption of the new scheme.
- CYRENE recommends an adoption period of one (1) year between the adoption of the scheme (upon its approval by ENISA) and the issuance of the first certificate as being technically acceptable.

25.2 SCHEME MAINTENANCE

25.2.1 Problem statement

EUCSA Reference

Article 62.4 – The ECCG shall have the following tasks:

e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

25.2.2 Recommendation

The ECCG should mandate groups of experts involving NCCAs, assessors and associated auditors, SCS Providers and Supply Chain Commercial Business Partners to:

- improve the security controls and associated requirements;
- improve the assessment methodology and associated documents;
- provide guidance to SCS-Ps and Supply Chain Commercial Business Partners about the prerequisites and operation of the scheme.

The expert groups should focus on methodology harmonization of evaluation activities, analysis of new technologies and vulnerability classes, and propose new or revised supporting documents.

As an alternative, some of the appendices to the scheme, and in particular Appendix A: Security Objectives and Requirements for SCSs, may be considered for submission to a European Standards Developing

Organization (SDO) as a basis for a future European standard, to be referenced in future versions of the CYRENE proposed EUSCS scheme.

26. Conclusions

In this report we propose a cybersecurity certification scheme that tackles the challenges identified towards the certification of Supply Chain Services (SCS), such as a diverse set of relevant SCS stakeholders involved in the life cycle of the certificate as well as in the life-cycle of the SCS, complex systems and a constantly evolving threat landscape of supply chain services, as well as the existence of different schemes in Member States by calling for cybersecurity best practices across three levels of assurance and by allowing for a transition from current national schemes in the EU. This scheme is based on the EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) and it looks into the certification of SCS based on the ISO2800x, ISO2700x, Common Criteria, ISO/IEC 15408 and the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 18045. The proposed scheme can be used by a self-assessor or by a CAB depending upon the assurance level of the SCS.

References

- [1] CYRENE EU H2020 project. Online available: <https://www.cyrene.eu>, accessed on May 14, 2021.
- [2] ISO 28000:2007 international standard, “Specification for security management systems for the supply chain”, 1st Edition 2007-09, accessed on April 20, 2021.
- [3] *The Directive on security of network and information systems (NIS Directive)*. (2020, December 16). An official website of the European Union. Retrieved July 18, 2021, from <https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive>
- [4] 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.
- [5] ISO/IEC 15408-1/2/3:2008-09, international standard, “Information technology-Security techniques-Evaluation criteria for IT security”.
- [6] ISO/IEC 18045:2008 international standard, “Information technology-Security techniques-Methodology for IT security evaluation”, accessed on April 29, 2021
- [7] CYRENE EU H2020 project. Report 1 - Supply Chain Analysis and Requirements, 2021.
- [8] 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.
- [9] ENISA, "EUCS – Cloud Service Scheme: a candidate cybersecurity certification scheme for cloud services". Online available: <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>, accessed on April 29, 2021.
- [10] ISO/IEC 17065:2012. Conformity assessment — Requirements for bodies certifying products, processes and services
- [11] ISO/IEC 27000-series on Information Security, accessed on April 29, 2021.
- [12] CYRENE EU H2020 project. Report 3 - Conformity Evaluation Process & Multi Level Evidence Driven Supply Chain Risk Assessment, 2021.
- [13] 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, accessed on April 20 2021.
- [14] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
- [15] ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management
- [16] ENISA, Methodology for a Sectoral Cybersecurity Assessment, Online available: <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>, accessed on September 14, 2021
- [17] ISO/IEC 17000:2020, Conformity assessment – Vocabulary and general principles.
- [18] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- [19] ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary.

- [20] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls
- [21] ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- [22] ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- [23] ISO/IEC 17067:2013, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
- [24] ISO/IEC 17020:2012, Conformity Assessment - Requirements For The Operation Of Various Types Of Bodies Performing Inspection
- [25] ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons
- [26] International Standard on Assurance Engagements (ISAE) 3402 Assurance reports on controls at a service organization, in [IAASB Handbook], Vol. 2, pp. 217-264]
- [27] International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance engagements other than audits or reviews of historical financial information, 2013. In [IAASB Handbook] Vol. 2, pp. 123-206
- [28] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure
- [29] ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes
- [30] NIST Special Publication 2000-02, Conformity Assessment Considerations for Federal Agencies, online available at: <https://doi.org/10.6028/NIST.SP.2000-02>
- [31] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, 2008/2018
- [32] Handbook of international quality control, auditing, review, other assurance, and related service announcements, 2018. ISBN 978-1-60815-389-3. Available from <https://www.iaasb.org/publications/2018-handbook-international-quality-control-auditing-review-other-assurance-and-related-services-26>
- [33] Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloud Computing Compliance Criteria Catalogue (C5), 2020. Available from: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html
- [34] World Customs Organization, Integrated Supply Chain Management Guidelines (ISCM), 2018, Available from: http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/_media/d81b2807c64a4b669942f88d51d5fcf6.ashx
- [35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

Appendices

Appendix A - Security Objectives and Requirements for SCSs

Assurance levels

The requirements defined in the present Appendix are labelled Basic, Substantial or High:

- Requirements labelled Basic apply to all assurance levels.
- Requirements labelled Substantial apply to levels Substantial and High, and they will in most cases be considered as guidance for level Basic (i.e., the reference method to achieve the Basic requirements, which are often less detailed).
- Requirements labelled High only apply to level High.

Typically, the requirements corresponding to an objective are organised as follows:

- Basic requirements define a baseline, often with limited details or constraints
- Substantial requirements add to that baseline further details and constraints. Sometimes, there are a few specific Substantial requirements.
- High requirements add further constraints. Some are also related to continuous monitoring, or to additional testing and review requirements, contributing to an increase in the depth of the audit.

A.1 ORGANISATION OF INFORMATION SECURITY

Plan, implement, maintain and continuously improve the information security framework of the SCS in collaboration of the SCS-P and the SCS-BPs

OIS-01 Supply Chain Service Information Security Management System (SCS-ISMS)

The SCS-P operates an information security management system (ISMS). The scope of the SCS-ISMS is to provide all updated information related to the SCS and its security.

Requirements

Ref	Description	Assurance Level
OIS-01.1	The SCS-P with the collaboration of the SCS-BPs shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least SCS-process models, SCS-BPs information, security reports (SCS-risk	Basic

	management reports, BCPs, DRPs), documentation of SCS-assets and SCS implemented controls, SCS- asset models revealing the interrelated processes, SCS-BPS and interconnected SCS-assets and mutual agreements (e.g. regarding responsibilities for mitigation actions, information sharing)	
OIS-01.2	The SCS-ISMS shall be in accordance to ISO/IEC 27001	Substantial
OIS-01.3	The SCS-ISMS shall have a valid certification according to ISO/IEC 27001 or to national schemes based on ISO 27001	High
OSI-01.4	The SCS-P with the collaboration of the SCS-BPs shall document the measures for documenting, implementing, maintaining and continuously updating and improving the ISMS	Basic
OIS-01.5	<p>The documentation shall include at least:</p> <ul style="list-style-type: none"> • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3 of ISO/IEC 27001); • Results of the last SCS-risk management review (Section 9.3) • Inventory of information related to the SCS-BPs, models (SCS-processes/assets), graphs (e.g. attack paths), documentation of SCS-assets, and implemented controls (including testing outcomes of controls) • Mutual Agreements at least regarding mitigation responsibilities and information sharing 	Substantial

OIS-02 SEGREGATION OF DUTIES

Objective

Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of SCS data processed, stored or transmitted by SCS.

Requirements

Ref	Description	Assurance Level
OIS-02.1	The SCS-P with the collaboration of the SCS-BPs shall perform a risk assessment (using the CYRENE extended risk assessment methodology in CYRENE Report 3) as defined in RM-01 about the accumulation of responsibilities or tasks on	Basic

	roles or business partners or third parties or individuals, regarding the provision of the SCS	
OIS-02.2	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the SCS and are in the area of responsibility of the SCS-P.	Basic
OIS-02.3	The SCS business partners under the supervision/approval of the SCS-P shall implement additional mitigating measures (as agreed in the Mutual Agreement) defined in the risk assessment.	Basic
OIS-02.4	The SCS-P shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.	High

OIS-03 CONTACT WITH AUTHORITIES AND INTEREST GROUPS

Objective

The SCS-P with the collaboration of the SCS-BPs stay informed about current threats and vulnerabilities by monitoring all public vulnerability data basis (e.g. NIST), commercial inventories, Dark Web and by maintaining the cooperation and information sharing with relevant authorities (ENISA, Europol, CSIRTs, CERTs) and special interest groups (e.g. ISACs). The information flows into the procedures for handling risks (cf. RM-01) and vulnerabilities (cf. OPS-17).

Requirements Ref	Description	Assurance Level
OIS-03.1	The SCS-P in collaboration with the SCS partners shall stay informed about current threats and vulnerabilities of all SCS assets. All SCS partners need to share with the SCS-P any threat/ vulnerability/incident of any SCS asset they host.	Basic
OIS-03.2	The SCS-P shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities	Substantial
OIS-03.3	SCS-P and SCS-BPs continuously monitor all public vulnerability data basis (e.g. NIST), commercial inventories, Dark Web, maintain cooperation and share information with relevant authorities (ENISA, Europol, CSIRTs, CERTs) and special interest groups (e.g. ISACs); maintain regular contact with CABs and NCCA. The information flows into the procedures for handling risks (cf. RM-01) and vulnerabilities (cf. OPS-17).	High

OIS-04 INFORMATION SECURITY IN PROJECT MANAGEMENT

Objective

Information security is considered in project management, regardless of the nature of the project.

Requirements

Requirements Ref	Description	Assurance Level
OIS-04.1	The SCS-P and the SCS partners shall include information security in the project management of all projects that may affect the SCS, regardless of the nature of the project	Basic
OIS-04.2	The SCS-P in collaboration with the SCS partners shall perform a risk assessment according to RM-01 to assess and treat the risks on any project that may affect the provision of the SCS, regardless of the nature of the project	Substantial/ High

A.2 INFORMATION SECURITY POLICIES

Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements.

ISP-01 SCS- INFORMATION SECURITY POLICY

Objective

The SCS-P in collaboration with the SCS partners have agreed to operate the SCS under a common security policy and implement specific security procedures. The top management of the SCS-P and the SCS-BPs have adopted a common information SCS-security policy, implemented by all as well by all their internal and external employees as well as SCS customers and third parties.

Requirements

Requirements Ref	Description	Assurance Level
------------------	-------------	-----------------

ISP-01.1	<p>The SCS-P in collaboration with the SCS partners shall document a global information security policy covering at least the following aspects:</p> <ul style="list-style-type: none"> ● the importance of information security, based on the requirements of SCS customers in relation to information security, as well as on the need to ensure the security of the SCS assets hosted by the SCS partners, information processed and stored by the SCS provider /partners and the SCS assets that support the services provided ● the security objectives and the desired security level, based on the business goals and tasks of the SCS-P. ● the commitment of the SCS-P and of the SCS-BPs to implement the security measures required to achieve the established security objectives. ● the most important aspects of the security strategy to achieve the security objectives set; and ● the organisational structure for information security in the SCS-ISMS application area. 	Basic
ISP-01.2	The SCS-P's and business partners' top management shall approve and endorse the global SCS information security policy	Basic
ISP-01.3	The SCS-P shall review the SCS- security policy at least following any significant SCS change or any change in the SCS business partners' susceptible to affect the principles defined in the policy, including the approval and endorsement by top management	Substantial
ISP-01.4	The SCS-P shall review the global information security policy at least annually	High
ISP-01.5	The SCS-P shall communicate and make available in the online SCS-ISMS the SCS- security policy to internal and external employees, to SCS _BPs and all SCS stakeholders	Basic

ISP-02 SECURITY POLICIES AND PROCEDURES

Objective

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all SCS partners, stakeholders, internal and external employees of the SCS-Provider/ partners in an appropriate manner.

Requirements

Requirements Ref	Description	Assurance Level
ISP-02.1	<p>The SCS-P in collaboration with the SCS partners shall derive policies and procedures from the SCS- security policy for all relevant subject matters, documented according to a uniform structure, including at least the following aspects:</p> <ul style="list-style-type: none"> ● Objectives; ● Scope; ● Roles, responsibilities and individual security policies of all SCS BPs; ● Roles and dependencies on other ● Steps for the execution of the security strategy; and ● Applicable legal and regulatory requirements. 	Basic
ISP-02.2	The policies and procedures shall include staff qualification requirements and the establishment of substitution rules in their description of roles and responsibilities within the organizations of the SCS provider/partners	Substantial
ISP-02.3	The SCS-P shall communicate and make available the policies and procedures to all SCS partners/stakeholders/internal and external employees	Basic
ISP-02.4	The SCS-P's and SCS business partners' top management shall approve the security policies and procedures or delegate this responsibility to authorised bodies	Basic

ISP-02.5	In case of a delegation, the authorised bodies shall report at least annually to the top management on the security policies and their implementation	High
ISP-02.6	The SCS-P's subject matter experts shall review the policies and procedures for adequacy at least annually, when the SCS-security policy is updated, and when major changes may affect the security of the SCS	Basic
ISP-02.7	After an update of procedures and policies, they shall be approved by the SCS-P and all SCS-BPs before they become effective, and then communicated and made available to the SCS partners/stakeholders/ internal and external employees	Basic

ISP-03 EXCEPTIONS

Objective

Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.

Requirements

Requirements Ref	Description	Assurance Level
ISP-03.1	The SCS-P in collaboration with the SCS partners shall maintain (and reported in the Mutual Agreement) a list of exceptions to the security policies and procedures, including associated controls.	Basic
ISP-03.2	The exceptions are limited in time	Basic
ISP-03.3	The exceptions shall be subjected to the RM-01 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners	Substantial
ISP-03.4	The exceptions to a security policy or procedure shall be approved by the top	High

	management or authorised body who approved the security policy or procedure	
ISP-03.5	The list of exceptions shall be reviewed at least annually	Basic
ISP-03.6	The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated	Substantial
ISP-03.7	The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date	High

A.3 RISK MANAGEMENT

Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the SCS-P.

RM-01 RISK MANAGEMENT POLICY

Objective

Risk management policies and procedures are documented and communicated to all SCS partners/ stakeholders

Reference: [ISO27005], [ISO2800], [ISO15408]

Requirements

Ref	Description	Assurance Level
RM-01.1	<p>The SCS-P shall document policies and procedures in accordance with ISP-02 for the following aspects:</p> <ul style="list-style-type: none"> • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners of all SCS assets; • Analysis of the probability and impact of occurrence and determination of the level of risk; 	Basic

	<ul style="list-style-type: none"> • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of handling (as agreed by all SCS partners); • Handling of risks through measures, including approval of authorization and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results across all SCS partners. 	
RM-01.2	The SCS-P shall use a documented risk analysis method (e.g. CYRENE methodology described in CYRENE Report 3) that guarantees reproducibility and comparability of the approach	Substantial

Guidance elements	
RM-01.2	The notion of “documented method” is close to “standardised method”, but the idea is to allow methods using in a national, vertical or other specific context. CYRENE has developed its own method based on ISO27001, ISO27005,

RM-02 RISK ASSESSMENT IMPLEMENTATION

Objective

Risk assessment-related policies and procedures are implemented on the entire perimeter of the SCS.

Requirements

Requirements Ref	Description	Assurance Level
RM-02.1	The SCS-P (with the agreement and responsibility of the SCS partners) shall implement the policies and procedures covering risk assessment on the entire perimeter of the supply chain service.	Basic
RM-02.2	The SCS-P shall make the results of the risk assessment available to all SCS partners and relevant stakeholders (using the SCS-ISMS)	Basic

RM-02.3	The SCS-P shall review and revise the risk assessment at least annually, and after each major change that may affect the security of the SCS.	Basic
RM-02.4	The SCS-P shall monitor the evolution of the risk factors and revise the risk assessment results accordingly informing all SCS partners and relevant stakeholders for the outcomes and possible advanced controls that they may need to implement.	High

Guidance elements		
RM-02.1	<p>The scope of risk identification should include the aspects below, insofar as they are applicable to the SCS provided and are within the area of responsibility of the SCS-P and the SCS partners:</p> <ul style="list-style-type: none"> ● Processing, storage or transmission of data of all SCS partners and relevant stakeholders with different protection needs; ● Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; ● Occurrence of weak points and malfunctions in the integration at system level of technical protective measures; ● Attacks via access points, including interfaces accessible from public networks (in particular administrative interfaces); ● Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and ● Dependencies on subservice organisations. 	
RM-02.1	For higher assurance levels, specific technical risks should be considered.	

RM-03 RISK TREATMENT IMPLEMENTATION

Objective

Identified risks are prioritised according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.

Requirements

Requirements Ref	Description	Assurance Level
------------------	-------------	-----------------

RM-03.1	The SCS-P (with the consensus of all SCS-BPs partners and relevant stakeholders) shall prioritise risks according to their criticality	Basic
RM-03.2	The SCS-P shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them (The Mutual Agreement imposes the SCS-partners.	Basic
RM-03.3	The risk treatment plan shall reduce the risk level to a threshold that the SCS-P, all SCS partners and relevant stakeholders deem acceptable (Residual Risk).	Basic
RM-03.4	The risk owners shall formally approve the treatment plan and in particular accept the residual risk	Substantial
RM-03.5	The SCS-P shall make the risk treatment plan available to all SCS partners and relevant stakeholders	Basic
RM-03.6	If the SCS-P shares risks with the SCS partners and customers, the shared risks shall be associated to Complementary Customer Controls (CCCs) and described in the user documentation	Basic
RM-03.7	The SCS-P shall revise the risk treatment plan every time the risk assessment is revised informing all SCS partners and relevant stakeholders.	Basic
RM-03.8	The risk owners (SCS partners) shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.	Substantial

Guidance elements	
RM-03.6	Sharing risks with SCS provider/partners should always be explicit, and associated with clear expectations, included in the documentation.

A.4 HUMAN RESOURCES

Ensure that SCS partners and stakeholders understand their responsibilities, are aware of their responsibilities with regard to information security, and that the SCS assets are protected in the event of changes in responsibilities or termination.

HR-01 HUMAN RESOURCE POLICIES

Objective

The policies applicable to the all SCS provider/partners and relevant SCS stakeholders, internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.

Requirements

Ref	Description	Assurance Level
HR-01.1	The SCS-P shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the supply chain service in the production environment, and all positions with access to supply chain service, all SCS partners and relevant stakeholders, data or system components.	Basic
HR-01.2	The SCS-P shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement from all SCS partners and relevant stakeholders, internal and external employees to act ethically in their professional duties.	Basic
HR-01.3	The SCS-P shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: <ul style="list-style-type: none"> ● Verifying whether a violation has occurred, to which SCS partner/asset; and ● Consideration of the nature and severity of the violation and its impact to the SCS operation, provision and performance 	Basic
HR-01.4	If disciplinary measures are defined in the policy mentioned in HR-01.3, then all SCS partners and relevant stakeholders, internal and external employees of the SCS-P shall be informed about	Basic

	possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.	
--	--	--

Guidance elements	
HR-01.2	<p>The agreement (Mutal Agreement) should at least stipulate that for any matter related to the security of the supply chain service:</p> <ul style="list-style-type: none"> ● professional duties are performed with loyalty, discretion and impartiality; and ● all SCS partners and relevant stakeholders, Internal and external employees use only those methods, tools and techniques that have been approved by the SCS-P.
HR-01.2	<p>The Code of Ethics should also consider the following provisions, especially at higher levels; the SCS-P, all SCS partners, relevant stakeholders and employees:</p> <ul style="list-style-type: none"> ● pledge to not disclose information to a third party, even if anonymised and decontextualised, which has been obtained or generated as part of the service, unless the SCS Customer has given formal written authorisation. ● pledge to alert the SCS-P to all clearly illegal content discovered during the provision of the service; ● pledge to comply with the legislation and regulations in force and with best practices related to their activities; ● share information with the SCS-P related to a security incident; the SCS-P needs to share such information with CSIRTS, local CERTs, relevant ISAC, national authorities

HR-02 VERIFICATION OF QUALIFICATION AND TRUSTWORTHINESS

Objective

The competency and integrity of all SCS partners, SCS relevant stakeholders, internal and external employees in a position classified in objective HR-01 are verified prior to commencement of employment in accordance with EU, national and local legislation and regulation by the SCS-P.

Requirements

Requirements Ref	Description	Assurance Level
HR-02.1	The competency and integrity of all SCS partners, SCS relevant stakeholders, internal and external employees of the SCS provider/business partner with access to SCS assets under the SCS-P's responsibility, or who are responsible to provide the supply chain service in the production environment shall be reviewed before commencement of employment in a position classified in objective HR-01. The extent of the review shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks.	Basic
HR-02.3	The competency and integrity of all SCS partners, SCS relevant stakeholders, internal and external employees of the SCS-P shall be reviewed before commencement of employment in a position with a higher risk classification than their previous position	Substantial
HR-02.4	The competency and integrity of all SCS partners, SCS relevant stakeholders, internal and external employees shall be reviewed annually for the employees in positions with the highest levels of risk classification, starting at a level to be defined in the human resource policy	High

Guidance elements	
HR-02.1:	<p>The agreement should at least stipulate that for any matter related to the security of the SCS:</p> <ul style="list-style-type: none"> ● professional duties are performed with loyalty, discretion and impartiality; and ● all SCS partners, SCS relevant stakeholders, internal and external employees use only those methods, tools and techniques that have been approved by the SCS-P. <p>For higher levels, the following areas should also be included:</p> <ul style="list-style-type: none"> ● Request of a police clearance certificate for applicants; and ● Evaluation of the risk to be blackmailed.

HR-03 EMPLOYEE TERMS AND CONDITIONS

Objective

The SCS provider's /partners' internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the SCS-P's code of ethics, before being granted access to any data or system components under the responsibility of the SCS-P used to provide the SCS in the production environment.

Requirements

Requirements Ref	Description	Assurance Level
HR-03.1	The SCS provider/partners/stakeholders shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures	Basic
HR-03.2	The SCS provider/partners/stakeholders shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the supply chain service, even if anonymised and decontextualised.	Basic
HR-03.3	The SCS-P shall give a presentation of all applicable information security policies and procedures to all SCS partners/stakeholders, internal and external employees before granting them any access to any SCS asset	Basic
HR-03.4	All SCS provider/partners/stakeholders, internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof	Substantial
HR-03.5	The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to SCS provider/partners/stakeholders, employees.	High

HR-04 SECURITY AWARENESS AND TRAINING

Objective

The SCS-P operates a target group-oriented security awareness and training program, which is completed by all SCS provider/partners/stakeholders, internal and external employees of the SCS-P on a regular basis.

Requirements

Requirements Ref	Description	Assurance Level
HR-04.1	<p>The SCS-P shall define a security awareness and training program that covers the following aspects:</p> <ul style="list-style-type: none"> ● Handling system components used to provide the SCS in the production environment in accordance with the SCS applicable policies and procedures; ● Handling SCS assets in accordance with applicable policies and instructions and applicable legal and regulatory requirements; ● Information about the current threat situation; and ● Correct behaviour in the event of security incidents. 	Basic
HR-04.2	The SCS-P shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification, business and technical duty of each SCS partner.	Substantial
HR-04.3	The SCS provider/partner shall review their security awareness and training program based on changes to policies and instructions and the current threat situation	Basic
HR-04.4	The SCS-P shall update their security awareness and training program at least annually	Substantial
HR-04.5	The SCS-P shall ensure that all SCS partners/stakeholders/employees complete the security awareness and training program defined for them	Basic

HR-04.6	The SCS-P shall ensure that all SCS partners/stakeholders, employees complete the security awareness and training program on a regular basis, and when changing target group	Substantial
HR-04.7	The SCS-P shall automatically monitor the completion of the security awareness and training program	High
HR-04.8	The SCS-P shall measure and evaluate the learning outcomes achieved through the awareness and training programme	Substantial
HR-04.9	The SCS-P shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme.	High
HR-04.10	The SCS-P shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks	Substantial

HR-05 TERMINATION OR CHANGE IN EMPLOYMENT

Objective

SCS partners/stakeholders, Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.

Requirements

Requirements Ref	Description	Assurance Level
HR-05.1	The SCS-P shall communicate to the SCS partners/stakeholders, internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed.	Basic
HR-05.2	The SCS-P shall apply a specific procedure to revoke the access rights and process appropriately	Basic

	the accounts and assets of the SCS partners/stakeholder, internal and external employees when their employment is terminated or changed	
HR-05.3	The procedure mentioned in HR-05.2 shall define specific roles and responsibilities and include a documented checklist of all required steps	Substantial
HR-05.4	The SCS-P shall automatically monitor the application of the procedure mentioned in HR-05.2	High

HR-06 CONFIDENTIALITY AGREEMENTS

Objective

Non-disclosure or confidentiality agreements are in place with the SCS- partners/stakeholders (called Mutual Recognition Agreement) internal employees, external service providers and suppliers of the SCS-P to protect the confidentiality of the information exchanged between them.

Requirements

Requirements Ref	Description	Assurance Level
HR-06.1	The SCS-P shall ensure that non-disclosure or confidentiality agreements are agreed with the SCS partners/stakeholders, internal employees, external service providers and suppliers	Basic
HR-06.2	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the SCS-P (with the agreement of all SCS partners/stakeholders) for the protection of confidential information and operational details	Substantial
HR-06.3	The agreements shall be accepted by the SCS partners/stakeholders external service providers and suppliers when the contract is agreed	Substantial
HR-06.4	The agreements shall be accepted by the SCS partners/stakeholders, internal employees of the SCS-P before authorisation of the access to the SCS resources.	Substantial
HR-06.5	The requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review	Substantial

	shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly.	
HR-06.6	The SCS-P shall inform its SCS partners/stakeholders internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.	Substantial
HR-06.7	The SCS-P shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by the SCS partners/stakeholders, internal employees, external service providers and suppliers	High

A.5 ASSET MANAGEMENT

Identify the SCS- assets and ensure an appropriate level of protection throughout their lifecycle

AM-01 ASSET INVENTORY

Objective

The SCS-P has established procedures for inventorying SCS assets, including SCS processes, SCS-asset models revealing the inter dependencies, all IT to ensure complete, accurate, valid and consistent inventory throughout the SCS asset lifecycle. The SCS-asset inventory is embedded in the online SCS-ISMS where all SCS-BPs update and the SCS-P maintains an ensures its security.

Requirements

Ref	Description	Ass. Level
AM-01.1	The SCS-P shall document and implement policies and procedures for maintaining an inventory of SCS-assets in the online SCS-ISMS.	Basic
AM-01.2	The inventory shall be performed automatically and/or by the SCS partners/stakeholders, the people or teams responsible for the SCS-assets to ensure complete, accurate, valid and consistent inventory throughout the SCS asset life cycle	Substantial
AM-01.3	The SCS-P shall record for each SCS asset the information needed to apply the risk management procedure defined in RM-01	Basic

AM-01.4	The information recorded with assets shall include the measures taken to manage the risks associated to the asset through its life cycle	Substantial
AM-01.5	The information about assets shall be considered by monitoring applications to identify the impact on SCSs and functions in case of events that could lead to a breach of protection objectives, and to support information provided to the operation of the SCS, affected SCS partners/stakeholders, customers in accordance with contractual agreements	High
AM-01.6	The SCS-P shall automatically monitor (with the collaboration of the SCS partners that host the SCS assets) the inventory of SCS assets to guarantee it is up-to-date	High

Guidance elements		
AM-01.1	The SCS assets include the processes, physical, digital, and virtual objects required for the information security of the SCS during the creation, processing, storage, transmission, deletion or destruction of information in the SCS-P's area of responsibility	
AM-01.2	<p>The information recorded should include:</p> <ul style="list-style-type: none"> ● the information for identifying the SCS asset ● the function of the asset; ● the model and version of the asset; ● the location of the asset; ● the interdependency and interactions of the asset with other SCS-assets (developed asset-models); ● implementation documentation of the asset; ● controls and documentation implemented in the asset 	
AM-01.3	The SCS-P shall log at least all changes to the information related to risk management on each SCS asset	

AM-02 ACCEPTABLE USE AND SAFE HANDLING OF ASSETS POLICY

Objective

Policies and procedures for acceptable use and safe handling of SCS assets are documented, communicated and provided in accordance with SP-01.

Requirements

Requirements Ref	Description	Assurance Level
AM-02.1	The SCS-P (with the collaboration and agreements of the SCS partners /stakeholders) shall document, communicate and implement policies and procedures for acceptable use and safe handling of the SCS assets	Basic
AM-02.2	The policies and procedures for acceptable use and safe handling of assets shall address at least the following aspects of the asset lifecycle as applicable to the asset	Substantial
AM-02.3	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use	High

Guidance elements	
AM-02.1	<p>The policies and procedures for acceptable use and safe handling of SCS assets shall address at least the following aspects of the asset lifecycle as applicable to the asset:</p> <ul style="list-style-type: none"> ● Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components; ● Inventory; ● Classification and labelling based on the need for protection of the information and measures for the level of protection identified; ● Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation; ● Requirements for versions of software and images as well as application of patches; ● Handling of software for which support, and security patches are not available anymore; ● Restriction of software installations or use of services; ● Protection against malware;

	<ul style="list-style-type: none"> ● Remote deactivation, deletion or blocking; ● Physical delivery and transport; ● Dealing with incidents and vulnerabilities; and ● Complete and irrevocable deletion of the data upon decommissioning.
--	--

AM-03 COMMISSIONING AND DECOMMISSIONING OF HARDWARE

Objective

The SCS-P has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the SCS in the production environment, depending on its intended use and based on the applicable policies and procedures.

Requirements

Ref	Description	Assurance Level
AM-03.1	The SCS-P (with the collaboration and agreements of the SCS partners /stakeholders) shall document, communicate and implement a procedure for the commissioning of hardware that is used to provide the SCS in the production environment, based on applicable policies and procedures	Basic
AM-03.2	The procedure mentioned in AM-03.1 shall ensure that the risks arising from the commissioning are identified, analysed and mitigated.	Substantial
AM-03.3	The procedure mentioned in AM-03.1 shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies, before authorization to commission the SCS asset can be granted.	Substantial
AM-03.4	The SCS-P (with the collaboration and agreements of the SCS partners /stakeholders) shall document, communicate and implement a procedure for the decommissioning of hardware that is used to provide the supply chain service in the production environment, requiring approval based on applicable policies.	Basic
AM-03.5	The procedure mentioned in AM.03-4 shall include the complete and permanent deletion of the data or the proper destruction of the media.	Basic

AM-03.6	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.	High
---------	--	------

AM-04 ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS

Objective

The SCS-P's, SCS partners, stakeholders, internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of SCS assets before they can be used if the SCS-P has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.

Requirements

Ref	Description	Assurance Level
AM-04.1	The SCS-P shall ensure and document that all SCS partners /stakeholders, internal and external employees are committed to the policies and procedures for acceptable use and safe handling of SCS assets in the situations described in AM-03	Basic
AM-04.2	The procedure mentioned in HR-06.2 shall include steps to ensure that all assets under custody of a SCS business partner, an employee are not used or returned upon termination of collaboration or employment.	Basic
AM-04.3	The SCS-P shall centrally manage the SCS assets under the custody of all the SCS partners, internal and external employees, including at least software, data, and policy distribution, as well as remote deactivation, deletion or locking, as available on the asset.	High
AM-04.4	The verification of the commitment defined in AM-04.1 shall be automatically monitored	High

AM-05 ASSET CLASSIFICATION AND LABELLING

Objective

SCS assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.

Requirements

Ref	Description	Assurance Level
AM-05.1	The SCS-P/ SCS partners /stakeholders shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits	Basic
AM-05.2	The SCS asset classification schema shall provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives	Substantial
AM-05.3	When applicable, the SCS-P with the SCS partners /stakeholders shall label all assets according to their classification in the asset classification schema	Basic
AM-05.4	The need for protection shall be determined by the SCS partners, individuals or groups responsible for the SCS assets	Substantial

Guidance elements	
AM-05.3	Definition of a label: “The means used to associate a set of security attributes with an asset”. Note that labelling is not necessarily physical.

A.6 PHYSICAL SECURITY

Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations

PS-01 PHYSICAL SECURITY PERIMETERS

Objective

The buildings and premises related to the supply chain service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises.

Requirements

Ref	Description	Assurance Level
PS-01.1	The SCS-P, SCS-BPs, partners /stakeholders shall define security perimeters in the buildings and premises related to the SCS provided	Basic
PS-01.2	The SCS-P, SCS partners /stakeholders shall define at least two security areas, with one covering all buildings and premises and one covering sensitive activities such as	Basic

	the buildings and premises hosting the information system for the production of the SCS	
PS01-3	The SCS-P, SCS partners /stakeholders shall define at least an additional private area that may host development activities and administration, supervision and operation of the critical SCS assets	High
PS-01.4	The SCS provider/partners shall ensure that no direct access exists between a public area and a sensitive area	High
PS-01.5	The SCS provider/partners shall ensure that all delivery, loading areas, and other points through which unauthorised persons can penetrate into the premises without being accompanied are part of the public area	High
PS-01.6	The SCS provider/partners shall define and communicate a set of security requirements for each security area in a policy according to SP-02	Basic

PS-02 PHYSICAL SITE ACCESS CONTROL

Objective

Physical access through the security perimeters is subject to access control measures that match each zone's security requirements and that are supported by an access control system.

Requirements

Ref	Description	Assurance Level
PS-02.1	The SCS provider/SCS partners shall document, communicate and implement policies and procedures related to the physical access control to the security areas matching the requirements defined in PS-01 and based on the principles defined in IAM-01	Basic
PS-02.2	The access control policy shall require at least one authentication factor for accessing any non-public area	Basic
PS-02.3	The access control policy shall require at least two authentication factors are used for access to sensitive areas	Substantial
PS-02.4	The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay	Substantial

PS-02.5	The access control policy shall describe the physical access control derogations in case of emergency	Basic
PS-02.6	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users	High
PS-02.7	The SCS provider/SCS partners shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters	Basic
PS-02.8	The SCS provider/SCS partners shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner so that it does not compromise the information security of the supply chain service	Basic
PS-02.9	The access control policy shall include logging of all accesses to non-public areas that enables the SCS provider/SCS partners to check whether only defined personnel have entered these zones	Substantial
PS-02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9	High

Guidance elements	
PS-02.4	Third-party personnel do not include external employees, who are subject to HR policies and do not have to be supervised
PS-02.8	A mix of prevention and detection measures are possible, and “timely” will be defined in greater details in the guidance for the different ALs and areas

PS-03 WORKING IN NON-PUBLIC AREAS

Objective

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.

Requirements

Requirements Ref	Description	Assurance Level
------------------	-------------	-----------------

PS-03.1	The SCS-P shall document, communicate, and implement policies and procedures concerning work in non-public areas	Basic
PS-03.2	The policies and procedures in PS-02.1 shall include a clear screen policy and a clear desk policy for documents and removable media	Substantial
PS-03.3	The SCS-P /SCS partners shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area	High
PS-03.4	The SCS-P /SCS partners shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area	High

PS-04 EQUIPMENT PROTECTION

Objective

The equipment used in the SCS-P's premises and buildings are protected physically against damage and unauthorised access by specific measures.

Requirements

Requirements Ref	Description	Assurance Level
PS-04.1	<p>The SCS-P/SCS partners shall document, communicate, and implement policies and procedures concerning the protection of equipment and including at least the following aspects:</p> <ul style="list-style-type: none"> ● Protecting power and communications cabling from interception, interference or damage; ● Protecting equipment during maintenance operations; ● Protecting equipment holding customer data during transport. 	Basic
PS-04.2	The procedures defined in PS-04.1 shall include a procedure to check the protection of power and communications cabling, to be performed regularly,	Substantial

	at least every two years, as well as in case of suspected manipulation by qualified personnel	
PS-04.3	The policies and procedures in PS-04.1 shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site	Substantial
PS-04.4	The procedure mentioned in PS-04.3 shall include a formal validation by top management of the SCS-P or by the authorised body that validated this procedure	High
PS-04.4	The SCS-P shall establish a wiring scheme and keep it up-to-date	High
PS-04.5	The SCS-P shall ensure that the maintenance agreements for equipment used in providing services make it possible to have security updates installed timely on this equipment	High
PS-04.6	The policies and procedures in PS-04.1 shall include measures to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) are compatible with the service's availability and security requirements	High
PS-04.7	The SCS-P shall ensure that an equipment containing a media with SCS or customer data can be returned to a third party only if the customer data stored on it is encrypted in accordance with CKM-03 or has been destroyed beforehand using a secure deletion mechanism	High
PS-04.8	The SCS-P /SCS partners shall use encryption on the removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media	Basic

Guidance elements

PS-04.2	<p>The checks to be performed should include at least the following aspects:</p> <ul style="list-style-type: none"> ● Traces of violent attempts to open closed distributors; ● Up-to-datedness of the documentation in the distribution list; ● Conformity of the actual wiring and patching with the documentation; ● The short-circuits and earthing of unneeded cables are intact; and ● Impermissible installations and modifications.
---------	--

PS-05 PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

Objective

The premises from which the supply chain service operated, and in particular its data centres, are protected against external and environmental threats.

Requirements

Requirements Ref	Description	Assurance Level
PS-05.1	<p>The SCS-P/SCS partners shall document and communicate a set of security requirements related to external and environmental threats in a policy according to SP-02, addressing the following risks in accordance with the applicable legal and contractual requirements:</p> <ul style="list-style-type: none"> ● Faults in planning; ● Unauthorised access; ● Insufficient surveillance; ● Insufficient air-conditioning; ● Fire and smoke; ● Water; ● Power failure; and ● Air ventilation and filtration. 	Basic

PS-05.2	The security requirements defined in PS-05.1 for datacentres shall be based on criteria which comply with established rules of technology	Substantial
PS-05.3	The security requirements defined in PS-05.1 for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime	High
PS-05.4	The security requirements defined in PS-05.1 for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually	High
PS-05.5	The SCS-P shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises (cf. BCM-04)	Substantial

A.7 OPERATIONAL SECURITY

Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

OPS-01 CAPACITY MANAGEMENT – PLANNING

Objective

The capacities of critical SCS resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.

Requirements

Ref	Description	Assurance Level
OPS-01.1	The SCS-P /SCS partners shall document and implement procedures to plan for capacities and resources (personnel and IT resources), which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload	Basic
OPS-01.2	The SCS-P /SCS partners shall meet the requirements included in contractual agreements with customers regarding the provision of the service in case of capacity bottlenecks or personnel and IT resources outages	Basic

OPS-01.3	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning	High
----------	---	------

OPS-02 CAPACITY MANAGEMENT – MONITORING

Objective

The capacities of critical resources such as personnel and IT resources are monitored.

Requirements

Ref	Description	Assurance Level
OPS-02.1	The SCS-P /SCS partners shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning of the services to ensure compliance with the service level agreement	Basic
OPS-02.2	The SCS-P /SCS partners shall make available to the customer the relevant information regarding capacity and availability on a self-service portal	High
OPS-02.3	The provisioning and de-provisioning of the services shall be automatically monitored to guarantee fulfilment of OPS-02.1	High

OPS-03 CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES

Objective

The SCS customers have the ability to manage the IT resources allocated to them in order to avoid overcrowding of resources and to achieve sufficient performance.

Requirements

Requirements Ref	Description	Assurance Level
OPS-03.1	The SCS-P/SCS partners shall enable customers to control and monitor the allocation of the system resources assigned to them, if the corresponding service capabilities are exposed to the customers	Basic

OPS-04 PROTECTION AGAINST MALWARE – POLICIES

Objective

Policies are defined that ensure the protection against malware of IT equipment related to the supply chain service.

Requirements

Ref	Description	Assurance Level
OPS-04.1	<p>The SCS-P shall document, communicate and implement policies and procedures according to ISP-02 to protect its systems and its SCS-BPs from malware, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the SCS-P that are used to provide the service in the production environment; and • Operation of protection programs for employees' terminal equipment. 	Basic
OPS-04.2	The SCS provider/partner shall create regular reports on the malware checks performed, which shall be reviewed and analysed by the SCS-P, authorised bodies in the reviews of the policies related to malware	Substantial
OPS-04.3	The policies and instructions related to malware shall include the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces (both the customer's self-service and the SCS-P's administration)	High
OPS-04.4	The SCS-P/SCS partners shall update the anti-malware products at the highest frequency that the vendors actually offer	High

OPS-05 PROTECTION AGAINST MALWARE – IMPLEMENTATION

Objective

Malware protection is deployed and maintained on systems that provide the SCS.

Requirements

Ref	Description	Assurance Level
OPS-05.1	The SCS-P/SCS partners shall deploy malware protection, if technically feasible, on all systems that support delivery	Basic

	of the supply chain service in the production environment, according to policies and procedures	
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial
OPS-05.3	The SCS-P/SCS partners shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1	High
OPS-05.4	The SCS-P shall automatically monitor the antimalware scans to track detected malware or irregularities	High

OPS-06 DATA BACKUP AND RECOVERY – POLICIES

Objective

Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.

Requirements

Requirements Ref	Description	Assurance Level
OPS-06.1	The SCS-P shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery	Basic
06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: <ul style="list-style-type: none"> ● Data is backed up in encrypted, state-of-the-art form; ● Access to the backed-up data and the execution of restores is performed only by authorised persons; and ● Tests of recovery procedures (cf. OPS-08). 	Substantial

OPS-07 DATA BACKUP AND RECOVERY – MONITORING

Objective

The proper execution of data backups is monitored.

Requirements

Requirements Ref	Description	Assurance Level
OPS-07.1	The SCP and SCS-BPs shall document and implement technical and organizational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06	Basic
OPS-07.2	The SCS-P shall make available to the SCS partners/stakeholders/ a self-service portal (on line ISMS) for automatically monitoring the SCS data backup to guarantee fulfilment with OPS-07.1	High
OPS-07.3	The SCS-P shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1	High

OPS-08 DATA BACKUP AND RECOVERY – REGULAR TESTING

Objective

The proper restoration of data backups is regularly tested.

Requirements

Ref	Description	Assurance Level
OPS-08.1	The SCS-P (with the collaboration of the SCS partners) shall test the restore procedures at least annually	Basic
OPS-08.2	The restore tests shall assess if the specifications for the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), the two of the most important parameters of a disaster recovery or data protection plan agreed with the SCS partners.	Substantial
OPS-08.3	Any deviation from the specification during the restore test shall be reported to the SCS-P's responsible person for assessment and remediation	Substantial
OPS-08.4	The SCS-P shall inform the SCS- partners/stakeholders, at their request, of the results of the recovery tests	High
OPS-08.5	Recovery tests shall be included in the SCS-P's and SCS partners (as appropriate) business continuity management	High

OPS-09 DATA BACKUP AND RECOVERY – STORAGE

Objective

Backup data is stored at an appropriately remote location.

Requirements

Requirements Ref	Description	Assurance Level
OPS-09.1	The SCS-P (with the collaboration of the SCS partners) shall transfer backup data to a remote location or transport them on backup media to a remote location	Basic
OPS-09.2	When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art	Basic
OPS-09.3	The SCS-P (with the collaboration of the SCS partners) shall select a remote location to store its backups concerning the distance, recovery times and the impact of disasters of both sites	Substantial
OPS-09.4	The physical and environmental security measures at the remote site shall have the same level as at the main site	Substantial
OPS-09.5	When the backup data is transmitted to a remote location via a network, the SCS-P (with the collaboration of the SCS partners) shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1	High

OPS-10 LOGGING AND MONITORING – POLICIES

Objective

Policies are defined to govern logging and monitoring events on system components under the CSP's responsibility.

Requirements

Requirements Ref	Description	Assurance Level
------------------	-------------	-----------------

OPS-10.1	The SCS-P and the SCS partners shall document, communicate and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under their responsibility	Basic
OPS-10.2	<p>The policies and procedures shall cover at least the following aspects:</p> <ul style="list-style-type: none"> ● Definition of events that the service lead to a violation of the protection goals; ● Specifications for activating, stopping and pausing the various logs; ● Information regarding the purpose and retention period of the logs; ● Define roles and responsibilities for setting up and monitoring logging; ● Time synchronisation of system components; and ● Compliance with legal and regulatory frameworks. 	Substantial

OPS-11 LOGGING AND MONITORING – DERIVED DATA MANAGEMENT

Objective

Policies are defined to govern the management of derived data by the SCS-P.

Requirements

Requirements Ref	Description	Assurance Level
OPS-11.1	The SCS-P and SCS partners shall document, communicate and implement policies and procedures according to ISP-02 that govern the secure handling of derived data	Basic
OPS-11.2	<p>The policies and procedures on derived data shall cover at least the following aspects:</p> <ul style="list-style-type: none"> ● Purpose for the collection and use of derived data beyond the operation of the supply 	Substantial

	<p>chain service, including purposes related to the implementation of security controls;</p> <ul style="list-style-type: none"> ● Anonymisation of the data whenever used in a context that goes beyond a single SCS partner; ● Period of storage reasonably related to the purposes of the collection; ● Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and ● Provision of the derived data to SCS partners/stakeholders according to contractual agreements. 	
OPS-11.3	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.	High

OPS-12 LOGGING AND MONITORING – IDENTIFICATION OF EVENTS

Objective

Logs are monitored to identify events that may lead to security incidents.

Requirements

Ref	Description	Assurance Level
OPS-12.1	The SCS-P and the SCS partners shall monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements	Basic
OPS-12.2	Identified events shall be reported to the appropriate departments for timely assessment and remediation.	Basic
OPS-12.3	The monitoring of events mentioned in OPS-12.1 shall be automated	Substantial
OPS-12.4	The SCS-P and the SCS partners shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1	High

OPS-13 LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION

Objective

The confidentiality, integrity and availability of logging and monitoring data are protected with measures adapted to their specific use.

Requirements

Ref	Description	Assurance Level
OPS-13.1	The SCS-P and the SCS partners shall store all log data in an integrity-protected and aggregated form that allow its centralised evaluation	Basic
OPS-13.2	Log data shall be deleted when it is no longer required for the purpose for which they were collected	Basic
OPS-13.3	The communication between the SCS assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality	Basic
OPS-13.4	The communication between the SCS assets to be logged and the logging servers shall be encrypted using state-of-the-art encryption or shall take place on a dedicated administration network	Substantial
OPS-12.5	The SCS provider shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: <ul style="list-style-type: none"> · Access only to authorised users and systems. · Retention for the specified period; and · Deletion when further retention is no longer necessary for the purpose of collection. 	Substantial
OPS-13.6	The SCS-P shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2	High

OPS-14 LOGGING AND MONITORING – ATTRIBUTION

Objective

Log data can be unambiguously attributed to a customer.

Requirement

Requirements Ref	Description	Assurance Level
OPS-14.1	The log data generated allows an unambiguous identification of user accesses at the SCS-P / and the SCS partners level to support analysis in the event of an incident	Basic
OPS-14.2	The SCS-P shall make available interfaces to conduct forensic analysis and perform backups of SCS partners infrastructure components and the SCS assets they host	Substantial
OPS-14.3	In the context of an investigation of an incident the SCS partner shall have the ability to provide to the SCS-P the logs related to its service	High

OPS-15 LOGGING AND MONITORING – CONFIGURATION

Objective

Access to the logging and monitoring system components and to their configuration is strictly restricted.

Requirements

Requirements Ref	Description	Assurance Level
OPS-15.1	The SCS-P and the SCS partners shall restrict to authorised users only the access to system components used for logging and monitoring under their responsibility	Basic
OPS-15.2	Changes to the logging and monitoring configuration are made in accordance with applicable policies	Basic
OPS-15.3	The access to SCS assets for logging and monitoring shall require strong authentication	Substantial

OPS-16 LOGGING AND MONITORING – AVAILABILITY

Objective

Systems for logging and monitoring are themselves monitored for availability.

Requirements

Requirements Ref	Description	Assurance Level
------------------	-------------	-----------------

OPS-16.1	The SCS-P and the SCS partners shall monitor the system components for logging and monitoring under its responsibility, and shall automatically report failures to the SCS provider for assessment and remediation	Basic
OPS-16.2	The SCS provider/partners shall design the SCS architecture/ system components for logging and monitoring in such a way that the overall functionality is not restricted if individual components fail	High

OPS-17 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES

Objective

Vulnerabilities in the system components used to provide the supply chain service are identified and addressed in a timely manner.

Requirements

Ref	Description	Assurance Level
OPS-17.1	The SCS provider/business partners shall document, communicated and implement in accordance to ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the SCS assets used to provide the supply chain service	Basic
OPS-17.2	<p>The policies and procedures shall describe measures regarding at least the following aspects:</p> <ul style="list-style-type: none"> ● Regular identification of vulnerabilities; ● Assessment of the severity of identified vulnerabilities; ● Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and ● Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities. 	Substantial

OPS-17.3	The SCS-P and the SCS partners shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities	Basic
OPS-17.4	The SCS-P and the SCS partners shall mandate in its policies and procedures the immediate handling of “critical” vulnerabilities and the handling of “high” vulnerabilities within a day, with a follow-up of the vulnerability until it has been remediated	Substantial

OPS-18 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION

Objective

Tests are performed on a regular basis to identify vulnerabilities.

Requirements

Requirements Ref	Description	Assurance Level
OPS-18.1	The SCS-P and the SCS partners shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the SCS, in accordance with policies for handling vulnerabilities	Basic
OPS-18.2	The SCS-P and the SCS partners shall have penetration tests carried out by qualified internal personnel or external service providers, according to a documented test methodology and including in their scope the system components relevant to the provision of the SCS in the area of responsibility of the SCS provider /partner as identified in a risk analysis	Substantial
OPS-18.3	The SCS-P shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures in collaboration with the SCS partners.	Substantial

OPS-20 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS OF PROCEDURES

Objective

The vulnerability and incident handling measures are regularly evaluated and improved.

Requirements

Requirements Ref	Description	Assurance Level
OPS-19.1	The SCS provider /partners shall regularly measure, analyse and assess the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness	Basic
OPS-19.2	The SCS-P shall organise a quarterly review of the results of the assessment defined in OPS-20.1 by accountable departments to initiate continuous improvement actions and verify their effectiveness	Substantial

OPS-21 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING

Objective

System components are hardened to reduce their attack surface and eliminate potential attack vectors.

Requirements

Requirements Ref	Description	Assurance Level
OPS-21.1	The SCS provider/partners shall harden all the SCS-assets under their responsibility that are used to provide the SCS, according to accepted industry standards	Basic
OPS-21.2	The hardening requirements for each SCS assets shall be documented	Basic
OPS-21.3	The SCS-P and the SCS-partners shall automatically monitor the service components under their responsibility for compliance with hardening specifications	High

A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT

Limit access to information and information processing facilities

IAM-01 POLICIES FOR ACCESS CONTROL TO INFORMATION

Objective

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorised.

Requirements

Requirements Ref	Description	Assurance Level
IAM-01.1	<p>The SCS-P (with the collaboration of the SCS partners) shall document, communicate and make available role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on the business and security requirements of the SCS provider, in which at least the following aspects are covered:</p> <ul style="list-style-type: none"> ● Parameters to be considered for making access control decisions ● Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle. ● Use of a role-based mechanism for the assignment of access rights ● Segregation of duties between managing, approving and assigning access rights ● Dedicated rules for users with privileged access ● Requirements for the approval and documentation of the management of access rights 	Basic
IAM-01.2	<p>The SCS-P (with the collaboration of the SCS partners) shall link the access control policy defined in IAM-01.1 with the physical access control policy defined in PS-02.1, to guarantee that the access to the premises where information is located is also controlled.</p>	Basic
IAM-01.3	<p>The SCS-P (with the collaboration of the SCS partners) shall base its access control policy on the use of role-based access control.</p>	Substantial

IAM-02 AUTHENTICATION MECHANISMS

Objective

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.

Requirements

Ref	Description	Assurance Level
IAM-02.1	<p>The SCS-P (with the collaboration of the SCS partners) shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects:</p> <ul style="list-style-type: none"> • The selection of mechanisms suitable for every type of account and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new accounts; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules; 	Basic
IAM-02.2	The access to all SCS environments of the SCS provider and partners shall be authenticated, including non-production environments	Substantial
IAM-02.3	The access to the production SCS environment of the SCS provider and partners shall require strong authentication	High
IAM-02.4	The access to all environments of the SCS provider/partners containing SCS assets shall require strong authentication	High
IAM-02.5	Within an SCS environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security	Substantial
IAM-02.6	For access to non-personal shared accounts, the SCS-P shall implement measures that require the users to be	Substantial

	authenticated with their personal account before being able to access these technical accounts	
IAM-02.7	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts	Basic
IAM-02.8	The SCS-P shall offer strong authentication methods to the SCS partners/stakeholders for use with the accounts under their responsibility	Substantial

IAM-03 PROTECTION AND STRENGTH OF CREDENTIALS

Objective

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.

Requirements

Ref	Description	Assurance Level
IAM-03.1	The SCS-P (with the collaboration of the SCS partners) shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: <ul style="list-style-type: none"> ● Non-reuse of credentials ● Trade-offs between entropy and ability to memorise ● Recommendations for renewal of passwords ● Rules on storage of passwords 	Basic
IAM-03.2	The SCS-P rules and recommendations defined in IAM-03.1 shall address at least the following aspects: <ul style="list-style-type: none"> ● Recommendations on password managers ● Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling 	Substantial
IAM-03.3	The SCS-P shall require users to whom authentication credentials are provided to sign a declaration in which they assure that they treat personal (or shared) authentication confidentially and keep it exclusively for themselves	High

IAM-03.4	Passwords shall be only stored using cryptographically strong hash functions	Basic
IAM-03.5	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	Basic
IAM-03.6	When creating credentials, compliance with specifications is enforced automatically as far as technically possible	Substantial
IAM-03.7	When a credential associated to a personal account is changed or renewed, the person associated to that account shall be notified	Substantial
IAM-03.8	Any password communicated to a user through e-mail, message or similar shall be changed by the user after its first use, and its validity shall not exceed 14 days after communication to the user	Substantial
IAM-03.9	The SCS-P shall make available to the SCS partners/stakeholders the rules and recommendations that shall or may apply to the users under their responsibility, and provide tools to manage and enforce these rules	Substantial

IAM-09 GENERAL ACCESS RESTRICTIONS

Objective

The assets in and around the supply chain service are managed in a way that ensure that access restrictions are enforced between different categories of assets.

Requirements

Ref	Description	Assurance Level
IAM-09.1	The SCS-P and the SCS partners shall implement sufficient partitioning measures between the information system providing the SCS and its other information systems	Basic
IAM-09.2	The SCS-P and the SCS partners shall design, develop, configure and deploy the information system providing the SCS to include a partitioning between the technical infrastructure and the equipment required for the administration of the SCS and the SCS assets that host	Substantial
IAM-09.3	The SCS-P shall separate the administration interfaces made available to the SCS partners from those made available to customers, its internal and external employees	High

IAM-09.4	The SCS-P shall implement suitable measures for partitioning between the SCS partners	Basic
----------	---	-------

A.9 CRYPTOGRAPHY AND KEY MANAGEMENT

Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information

CKM-01 POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT

Objective

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.

Requirements

Ref	Description	Assurance Level
CKM-01.1	<p>The SCS-P and the SCS partners shall document, communicate, make available and implement policies with technical and organizational safeguards for encryption and key management, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> ● Usage of strong encryption procedures and secure network protocols ● Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys ● Consideration of relevant legal and regulatory obligations and requirements 	Basic
CKM-01.2	Cryptography policies and procedures shall include risk-based provisions for the use of encryption aligned with the data classification schemes and considering the	Substantial

	communication channel, type, strength and quality of the encryption	
CKM-01.3	The strong encryption procedures and secure network protocols mentioned in the cryptography policies and procedures shall correspond to the state-of-the-art	Substantial

CKM-02 ENCRYPTION OF DATA IN TRANSIT

Objective

Data communicated over public networks which is related to the SCS stakeholders protected in confidentiality, integrity, and authenticity.

Requirements

Requirements Ref	Description	Assurance Level
CKM-02.1	The SCS-P and the SCS partners shall define and implement strong encryption mechanisms for the transmission of SCS customer data over public networks	Basic
CKM-02.2	The SCS-P and the SCS partners shall define, and implement strong encryption mechanisms for the transmission of all data over public networks	High

CKM-03 ENCRYPTION OF DATA AT REST

Objective

The SCS-P has established procedures and technical safeguards to prevent the disclosure of data during providing of the service.

Requirements

Ref	Description	Assurance Level
CKM-03.1	The SCS-P shall document and implement procedures and technical safeguards to encrypt SCS data	Basic
CKM-03.2	The private and secret keys used for encryption shall be known only to the SCS partners in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions	Substantial

CKM-03.3	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the SCS partners	Substantial
CKM-03.4	The private and secret keys used for encryption shall be known exclusively by the customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements	High

CKM-04 SECURE KEY MANAGEMENT

Objective

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.

Requirements

Ref	Description	Assurance Level
CKM-04.1	<p>Procedures and technical safeguards for secure key management in the area of responsibility of the SCS-P shall include at least the following aspects:</p> <ul style="list-style-type: none"> ● Generation of keys for different cryptographic systems and applications; ● Issuing and obtaining public-key certificates; ● Provisioning and activation of the keys; ● Secure storage of keys including description of how authorised users get access; ● Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; ● Handling of compromised keys; and ● Withdrawal and deletion of keys; 	Basic
CKM-04.2	For the secure storage of keys, the key management system shall be separated from the application and middleware levels	Substantial
CKM-04.3	For the secure storage of keys and other secrets used for the administration tasks, the SCS-P shall use a suitable security container, software or hardware	High

CKM-04.4	If pre-shared keys are used, the specific provisions relating to the secure use of this procedure shall be specified separately.	Substantial
----------	--	-------------

A.10 COMMUNICATION SECURITY

Ensure the protection of information in networks and the corresponding information processing systems

CS-01 TECHNICAL SAFEGUARDS

Objective

The SCS-P has implemented appropriate technical safeguards in order to detect and respond to network-based attacks as well as to ensure the protection of information and information processing systems.

Requirements

Ref	Description	Assurance Level
CS-01.1	The SCS-P and the SCS partners shall document, communicate and implement technical safeguards that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems, in accordance with ISP-02	Basic
CS-01.2	The SCS-P and the SCS partners shall feed into a SIEM (Security Information and Event Management) SCS system, all data from the technical safeguards implemented so that automatic countermeasures regarding correlating events are initiated	Substantial
CS-01.3	The SCS-P and the SCS partners shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network	High
CS-01.4	The SCS-P and the SCS partners shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines	High

CS-02 SECURITY REQUIREMENTS TO CONNECT WITHIN THE SCS NETWORK

Objective

The establishment of connections within the SCS network is subject to specific security requirements.

Requirements

Ref	Description	Assurance Level
CS-02-1	<p>The SCS-P and the SCS partners shall document, communicate, make available and implement specific security requirements to connect within their network, including at least:</p> <ul style="list-style-type: none"> • when the security zones are to be separated and when the assets are to be logically or physically segregated; • what communication relationships and what network and application protocols are permitted in each case; • how the data traffic for administration and monitoring are segregated from each other at the network level; • what internal, cross-location communication is permitted; and • what cross-network communication is allowed. 	Basic

CS-03 MONITORING OF CONNECTIONS WITHIN THE SCS-P'S NETWORK

Objective

The communication flows within the supply chain environment, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.

Requirements

Ref	Description	Assurance Level
CS-03.1	The SCS-P and the SCS partners shall distinguish between trusted and untrusted networks, based on a risk assessment	Basic
CS-03.2	The SCS-P and the SCS partners shall separate trusted and untrusted networks into different security zones for internal and external network areas and demilitarised zone (DMZ) if applicable	Basic
CS-03.2	The SCS-P and the SCS partners shall design and configure both physical and virtualised network environments to restrict and monitor the connection to	Basic

	trusted or untrusted networks according to the defined security requirements	
CS-03.3	The SCS-P and the SCS partners shall review at specified intervals the business justification for using all services, protocols, and ports. This review shall also include the compensatory measures used for protocols that are considered insecure	Basic
CS-03.4	The SCS-P shall review at least annually the design and implementation and configuration undertaken to monitor the connections in a risk-oriented manner, with regard to the defined security requirements	Substantial
CS-03.5	The SCS-P and the SCS partners shall assess the risks of identified vulnerabilities in accordance with the risk management procedure and follow-up measures shall be defined and tracked	Substantial
CS-03.6	The SCS-P shall protect all SIEM logs to avoid tampering	Substantial

A.11 CHANGE AND CONFIGURATION MANAGEMENT

Ensure that changes and configuration actions to information systems guarantee the security of the delivered SCS.

CCM-01 POLICIES FOR CHANGES TO INFORMATION SYSTEMS

Objective

Policies and procedures are defined to control changes to information systems.

Requirements

Ref	Description	Assurance Level
CCM-01.1	The SCS-P (with the collaboration of the SCS partners) shall document, implement, and communicate policies and procedures for change management of the IT systems	Basic

CCM-01.2	<p>The change management policies and procedures shall cover at least the following aspects:</p> <ul style="list-style-type: none"> ● Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals; ● Requirements for the performance and documentation of tests; ● Requirements for segregation of duties during planning, testing, and release of changes; ● Requirements for the documentation of changes in the system, operational and user documentation; and ● Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes. 	Substantial
----------	--	-------------

CCM-02 RISK ASSESSMENT, CATEGORISATION AND PRIORITISATION OF CHANGES

Objective

Responsibilities are assigned inside the SCS provider/partners organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Ref	Description	Assurance Level
CCM-02.1	The SCS-P shall categorise and prioritise changes considering the potential security effects on the system components concerned	Basic
CCM-02.2	The SCS-P shall base the decision on classification and prioritization on a risk assessment performed in accordance with RM-01 with regard to potential effects on the system components concerned	Substantial
CCM-02.3	If the risk associated to a planned change is high, then appropriate mitigation measures shall be taken before	High

	deploying the service (with the collaboration of the SCS partners)	
--	--	--

CCM-06 VERSION CONTROL

Objective

Version control is used to track individual changes and enable restoration of a previous version if required.

Requirements

Ref	Description	Assurance Level
CCM-06.1	The SCS-P / SCS-BPs shall implement version control procedures to track the dependencies of individual changes and to restore affected SCS-assets to their previous state as a result of errors or identified vulnerabilities.	Basic
CCM-06.2	The version control procedures shall provide appropriate safeguards to ensure that the confidentiality, integrity and availability of supply chain service is not compromised when SCS assets are restored back to their previous state	High
CCM-06.3	The SCS-P and SCS partners shall retain a history of the software versions and of the systems that are implemented in order to be able to reconstitute, where applicable in a test environment, a complete environment such as was implemented on a given date; the retention time for this history shall be at least the same as that for backups.	High

A.12 DEVELOPMENT OF INFORMATION SYSTEMS

Ensure information security in the development cycle of information systems

DEV-01 POLICIES FOR THE DEVELOPMENT AND PROCUREMENT OF INFORMATION SYSTEMS

Objective

Policies are defined to define technical and organisational measures for the development of the supply chain service throughout its lifecycle.

Requirements

Ref	Description	Assurance Level
DEV-01.1	The SCS-P (with the collaboration of the SCS partners) shall document, communicate and implement policies and procedures with technical and organisational measures for the secure development of the SCS.	Basic
DEV-01.2	The policies and procedures for secure development shall consider information security from the earliest phases of design	Basic
DEV-01.3	The policies and procedures for secure development shall be based on recognised standards and methods with regard to the following aspects: <ul style="list-style-type: none"> ● Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ● Security in software deployment (including continuous delivery); ● Security in operation (reaction to identified faults and vulnerabilities); and ● Secure coding standards and practices (avoiding the introduction of vulnerabilities in code). 	Substantial
DEV-01.4	The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools	Substantial

DEV-02 DEVELOPMENT SUPPLY CHAIN SECURITY

Objective

The SCS of system components is considered in development security.

Requirements

Ref	Description	Assurance Level
DEV-02.1	The SCS-P/ SCS-BPs shall maintain a list of dependencies to the SCS partners, processes, SCS assets (including hardware and software products) used in the development of its service	Basic

DEV-02.2	The SCS-P/ SCS-BPs shall document and implement policies for the use of third-party and open source software	Substantial
DEV-02.3	The SCS-P/ SCS-BPs make its list of dependencies available to customers upon request	Substantial

DEV-02 SECURE DEVELOPMENT ENVIRONMENT

Objective

The development environment takes information security in consideration.

Requirements

Ref	Description	Assurance Level
DEV-03.1	The SCS-P and the SCS partners shall ensure that the confidentiality and integrity of the SCS-asset is adequately protected at all stages of its development/procurement	Basic
DEV-03.2	The SCS-P and the SCS partners shall use version control to keep a history of the changes in the SCS asset with an attribution of changes to individual developers	Basic
DEV-03.3	The SCS-P and the SCS partners shall implement a secure development and test environments that makes it possible to manage the entire development cycle of the information system of the service	Substantial
DEV-03.4	The SCS-P and the SCS partners shall consider the development and test environments when performing risk assessment	Substantial
DEV-03.5	The SCS-P and the SCS partners shall include development resources as part of the backup policy	Substantial

DEV-04 SEPARATION OF ENVIRONMENTS

Objective

The development SCS-environment takes information security in consideration.

Requirements

Ref	Description	Assurance Level
-----	-------------	-----------------

DEV-04.1	The SCS-P and the SCS partners shall ensure that SCS environments are physically or logically separated from development, test or pre-production environments	Basic
DEV-04.2	Data contained in the SCS-environments shall not be used in development, test or pre-production environments in order not to compromise their confidentiality	Basic
DEV-04.3	When non-production SCS-environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment	High

DEV-05 DEVELOPMENT OF SECURITY FEATURES

Objective

The development environment takes information security in consideration.

Requirements

Ref	Description	Assurance Level
DEV-05.1	The SCS-P and the SCS partners shall document, communicate, make available and implement specific procedures for the development of functions that implement technical mechanisms or safeguards required by the EUSCS scheme, with increased testing requirements.	Basic
DEV-05.2	Design documentation for security features shall include a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature	Substantial
DEV-05.3	The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.	Substantial
DEV-05.4	The documentation of the tests for security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test.	Substantial
DEV-05.5	The documentation of the tests shall include a demonstration of the coverage of the source code, including branch coverage for security-critical code.	High

DEV-07 OUTSOURCING OF THE DEVELOPMENT

Objective

Outsourced developments provide similar security guarantees than in-house developments.

Requirements

Ref	Description	Assurance Level
DEV-07.1	<p>When outsourcing development of the supply chain service or components thereof to a contractor, the SCS provider/partner and the contractor shall contractually agree on specifications regarding at least the following aspects:</p> <ul style="list-style-type: none"> • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; • Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities. 	Basic
DEV-07.2	<p>Before subcontracting the development of the supply chain service or components thereof, the SCS-P shall conduct a risk assessment that considers at least the following aspects</p> <ul style="list-style-type: none"> • Management of source code by the subcontractor; • Human resource procedures implemented by the subcontractor; and • Required access to the SCS-P's development, testing and pre-production environments. 	Substantial
DEV-07.3	<p>The SCS provider/partner shall document and implement a procedure that makes it possible to supervise and control the outsourced development activity, in order to ensure that the outsourced development activity is compliant with the secure development policy of the service provider and makes it possible to achieve a level of security of the external development that is equivalent to that of internal development</p>	High
DEV-07.4	<p>Internal or external employees of the SCS provider/partner shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.</p>	High

A.13 PROCUREMENT MANAGEMENT

Ensure the protection of information that suppliers of the SCS-P can access and monitor the agreed services and security requirements

PM-01 POLICIES AND PROCEDURES FOR CONTROLLING AND MONITORING THIRD PARTIES

Objective

Responsibilities are assigned inside the SCS-P and its SCS partners to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Requirements

Ref	Description	Assurance Level
PM-01.1	The SCS-P (with the collaboration and agreement of the SCS partners) shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the supply chain service	Basic
PM-01.2	<p>The policies and procedures shall cover at least the following aspects:</p> <ul style="list-style-type: none"> ● Requirements for the assessment of risks resulting from the procurement of third-party services; ● Requirements for the classification of third parties based on the risk assessment by the SCS-P; ● Information security requirements for the processing, storage, or transmission of information by third parties based on recognised industry standards; ● Information security awareness and training requirements for staff; ● Applicable legal and regulatory requirements; ● Requirements for dealing with vulnerabilities, security incidents, and malfunctions; ● Specifications for the contractual agreement of these requirements; 	Substantial

	<ul style="list-style-type: none"> • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers, also contribute to the provision of the supply chain service. 	
PM-01.3	The SCS-P shall contractually require its subservice organizations to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system with respect to the EUSCS requirements.	High
PM-01.4	The reports shall include the complementary subservice organisation controls that are required, together with the controls of the SCS-P, to meet the applicable EUSCS requirements with reasonable assurance	High
PM-01.5	In case the supplier organizations are not able to provide an EUSCS compliance report, the SCS-P shall reserve the right to audit them to assess the suitability and effectiveness of the service-related internal and complementary controls by qualified personnel	High

PM-02 RISK ASSESSMENT OF SUPPLIERS

Objective

Suppliers of the SCS-P and of the SCS partners undergo a risk assessment to determine the security needs related to the product or service they provide.

Requirements

Ref	Description	Assurance Level
PM-02.1	The SCS-P and of the SCS partners shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties before they start contributing to the provision of the SCS.	Basic
PM-02.2	The risk assessment shall include the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects:	Substantial

	<ul style="list-style-type: none"> ● Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the third party; ● Impact of a protection breach on the provision of the supply chain service; ● The SCS provider's/partner's dependence on the supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives. 	
--	--	--

PM-03 DIRECTORY OF SUPPLIERS

Objective

A centralised directory of suppliers is available to facilitate their control and monitoring.

Requirements

Ref	Description	Assurance Level
PM-03.1	The SCS-P shall maintain (with the collaboration of the SCS partners) a directory for controlling and monitoring his and his SCS business partners suppliers who contribute to the delivery of the SCS	Basic
PM-03.2	<p>The directory shall contain the following information:</p> <ul style="list-style-type: none"> ● Company name; ● Address; ● Locations of data processing and storage; ● Responsible contact person at the service provider/supplier; ● Responsible contact person at the SCS-P; ● Description of the service; ● Classification based on the risk assessment; ● Beginning of service usage; and ● Proof of compliance with contractually agreed requirements. 	Substantial

PM-04 MONITORING OF COMPLIANCE WITH REQUIREMENTS

Objective

Monitoring mechanisms are in place to ensure that third parties comply with their regulatory and contractual obligations.

Requirements

Ref	Description	Assurance Level
PM-04.1	The SCS-P and the SCS partners shall monitor the compliance of their suppliers with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties	Basic
PM-04.2	Monitoring activities shall include at least a regular review of the following evidence, as provided by suppliers under contractual agreements: <ul style="list-style-type: none"> ● reports on the quality of the service provided; ● certificates of the management systems' compliance with international standards; ● independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and ● Records of the third parties on the handling of vulnerabilities, security incidents, and malfunctions. 	Substantial
PM-04.3	The frequency of the monitoring shall correspond to the classification of the third party based on the risk assessment conducted by the SCS-P and the SCS partners and the results of the monitoring shall be included in the review of the third party's risk assessment.	Basic
PM-04.4	Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf. RM-01)	Basic
PM-04.5	When a change in a third-party contributing to the delivery of the supply chain service affects its level of security, the SCS-P shall inform all the SCS partners and stakeholders without delay	Basic
PM-04.6	The SCS-P (with the collaboration of the SCS partners) shall document and implement a procedure to review and update, at least once a year, non-disclosure or	Substantial

	confidentiality requirements regarding suppliers contributing to the delivery of the service	
PM-04.7	<p>The SCS-P and the SCS partners shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects:</p> <ul style="list-style-type: none"> ● Configuration of SCS assets; ● Performance and availability of SCS assets; ● Response time to malfunctions and security incidents; and ● Recovery time (time until completion of error handling). 	High
PM-04.8	The SCS-P and SCS partners shall automatically monitor identified violations and discrepancies, and these shall be automatically reported to the responsible SCS partner for prompt assessment and action	High

A.14 INCIDENT MANAGEMENT

Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents

IM-01 POLICY FOR SECURITY INCIDENT MANAGEMENT

Objective

A policy is defined to respond to security incidents in a fast, efficient and orderly manner.

Requirements

Ref	Description	Assurance Level
IM-01.1	The SCS-P (with the collaboration of the SCS partners) shall document, communicate and implement policies and procedures containing technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents	Basic
IM-01.2	The policies and procedures shall include guidelines for the classification, prioritization, and escalation of security	Basic

	incidents and creates interfaces for incident management and business continuity management	
IM-01.3	The SCS-P (with the collaboration of the SCS partners) shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents in the SCS.	Basic
IM-01.4	The SCS-P shall inform the SCS partners and stakeholders affected by security incidents in a timely and appropriate manner	Substantial
IM-01.5	The incident management policy shall include procedures as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident	Substantial
IM-01.6	The incident management policy shall include analysis plans for typical security incidents	High
IM-01.7	The incident management policy shall include an evaluation methodology so that the collected information does not lose its evidential value in any subsequent legal assessment	High
IM-01.8	The incident management policy shall include provisions for the regular testing of the incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential deficiencies	High

IM-02 PROCESSING OF SECURITY INCIDENTS

Objective

A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.

Requirements

Ref	Description	Assurance Level
IM-02.1	The SCS-P (with the collaboration of the SCS-Partners) shall classify, prioritise, and perform root-cause analyses for events that could constitute a security incident, using their subject matter experts and external security providers where appropriate	Basic
IM-02.2	The SCS-P shall maintain a catalogue that clearly identifies the security incidents that affect SCS partners/assets and data, and use that catalogue to classify incidents	Substantial

IM-02.3	The incident classification mechanism shall include provisions to correlate events. In addition, these correlated events shall themselves be assessed and classified according to their criticality	Substantial
IM-02.4	The SCS-P shall simulate the identification, analysis, and defence of security incidents and attacks at least once a year through appropriate tests and exercises	High
IM-02.5	The SCS-P shall monitor the processing of incident to verify the application of incident management policies and procedures	High

IM-03 DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS

Objective

Security incidents are documented to and reported in a timely manner to customers.

Requirements

Ref	Description	Assurance Level
IM-03.1	The SCS-P (with the collaboration of the SCS partners) shall document the implemented measures after a security incident has been processed and, following the contractual agreements, the document shall be sent to the affected SCS partners and stakeholders for final acknowledgment or, if applicable, as confirmation.	Basic
IM-03.2	The SCS-P shall make information on security incidents or confirmed security breaches available to all affected SCS stakeholders	Basic
IM-03.3	The SCS-P shall continuously report on security incidents to affected SCS partners until the security incident is closed and a solution is applied and documented, in accordance to the defined Service Level Agreement (SLA) and contractual agreements	Substantial
IM-03.4	The SCS-P shall allow SCS partners to actively approve the solution before automatically approving it after a certain period	High

IM-06 EVALUATION AND LEARNING PROCESS

Objective

Measures are in place to continuously improve the service from experience learned in incidents.

Requirements

Ref	Description	Assurance Level
IM-06.1	The SCS-P (with the collaboration of the SCS partners) shall perform an analysis of security incidents to identify recurrent or significant incidents and to identify the need for further protection, if needed with the support of external bodies	Basic
IM-06.2	The SCS-P and the SCS partners shall only contract supporting external bodies that are qualified incident response service providers or government agencies	Basic
IM-06.3	The SCS-P (with the collaboration of the SCS partners) shall define, implement and maintain a knowledge repository of security incidents and the measures taken to solve them, as well as information related to the assets that these incidents affected, and use that information to enrich the classification catalogue	Substantial
IM-06.4	The intelligence gained from the incident management and gathered in the knowledge repository shall be used to identify recurring incidents or potential significant incidents and to determine the need for advanced safeguards and implement them	Substantial

IM-07 INCIDENT EVIDENCE PRESERVATION

Objective

Measures are in place to preserve information related to security incidents.

Requirements

Ref	Description	Assurance Level
IM-07.1	The SCS-P (with the collaboration of the SCS partners) shall document and implement a procedure to archive all documents and evidence that provide details on security incidents	Basic
IM-07.2	The documents and evidence shall be archived in a way that could be used as evidence in court	Substantial
IM-07.3	When the SCS-P and the SCS partners require additional expertise in order to preserve the evidences and secure the	Substantial

	chain of custody on a security incident, the SCS-P shall contract a qualified incident response service provider only	
IM-07.4	The SCS-P (with the collaboration of the SCS-partners) shall implement security mechanisms and processes for protecting all the information related to security incidents in accordance with criticality levels and legal requirements in effect	Basic
IM-07.5	The service provider shall establish an integrated team of forensic/incident responder personnel specifically trained on evidence preservation and chain of custody management	High

A.15 BUSINESS CONTINUITY

Plan, implement, maintain and test procedures and measures for business continuity and emergency management

BC-01 BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY

Objective

Responsibilities are assigned inside the SCS-P and SCS partners' organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Requirements

Ref	Description	Assurance Level
BC-01.1	The SCS-P (with the collaboration of the SCS partners) shall document, communicate and make available policies and procedures establishing the strategy and guidelines to ensure business continuity and contingency management	Basic
BC-01.2	The SCS-P and the SCS partners shall name (a member of) top management as the process owner of business continuity and emergency management, and responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines, and for ensuring that sufficient resources are made available for an effective process	Substantial
BC-01.3	The business continuity and contingency management process owner shall ensure that sufficient resources are made available for an effective process	Substantial

BC-02 BUSINESS IMPACT ANALYSIS PROCEDURES

Objective

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the SCS or enterprise.

Requirements

Ref	Description	Assurance Level
BC-02.1	The policies and procedures for business continuity and contingency management shall include the need to perform a business impact analysis to determine the impact of any malfunction to the SCS or enterprise.	Basic
BC-02.2	<p>The business impact analysis policies and procedures shall consider at least the following aspects:</p> <ul style="list-style-type: none"> ● Possible scenarios based on a risk analysis; ● Identification of critical processes, partners and assets ● Identification of dependencies, including processes (including resources required), applications, business partners and third parties; ● Identification of threats to critical SCS assets ● Identification of effects resulting from planned and unplanned malfunctions and changes over time; ● Determination of the maximum acceptable duration of malfunctions; ● Identification of restoration priorities; ● Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); ● Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and ● Estimation of the resources needed for resumption. 	Substantial
BC-02.3	The business impact analysis resulting from these policies and procedures shall be reviewed at regular intervals, at least once	Substantial

	a year, or after significant organisational or environment-related changes.	
--	---	--

BC-03 BUSINESS CONTINUITY AND CONTINGENCY PLANNING

Objective

A business continuity framework including a business continuity plan and associated contingency plans is available.

Requirements

Ref	Description	Assurance Level
BC-03.1	The SCS-P (with the collaboration of the SCS partners) shall document and implement a business continuity plan and contingency plans to ensure continuity of the services, taking into account information security constraints and the results of the business impact analysis	Basic
BC-03.2	The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used	Substantial
BC-03.3	<p>The business continuity plan and contingency plans shall cover at least the following aspects:</p> <ul style="list-style-type: none"> ● Defined purpose and scope, including relevant business processes and dependencies; ● Accessibility and comprehensibility of the plans for persons who are to act accordingly; ● Ownership by at least one designated person responsible for review, updating and approval; ● Defined communication channels, roles and responsibilities including notification of the customer; ● Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of supply chain infrastructure components and services and alignment with customers); ● Methods for putting the plans into effect; 	Substantial

	<ul style="list-style-type: none"> • Continuous process improvement; and • Interfaces to Security Incident Management. 	
BC-03.4	The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Substantial

BC-04 BUSINESS CONTINUITY TESTS AND EXERCISES

Objective

The business continuity framework is tested on a regular basis.

Requirements

Ref	Description	Assurance Level
BC-04.1	The business impact analysis, business continuity plan and contingency plans shall be tested at regular intervals (at least once a year) or after an update	Substantial
BC-04.2	The tests shall be documented, and the results considered to update the business continuity plan and to define future operational continuity measures	Substantial
BC-04.3	The tests shall involve SCS partners, stakeholders and relevant third parties, such as external service providers and suppliers	Substantial
BC-04.4	In addition to the tests, exercises shall also be carried out, which are, among other things, based on scenarios resulting from security incidents that have already occurred in the past	High

A.16 COMPLIANCE

Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements

CO-01 IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS

Objective

The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the supply chain service are defined and documented.

Requirements

Ref	Description	Assurance Level
CO-01.1	The SCS-P (with the collaboration of the SCS partners) shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the SCS.	Basic
CO-01.2	The SCS-P (with the collaboration of the SCS partners) shall document and implement procedures for complying to these contractual requirements	Substantial
CO-01.3	The SCS-P (with the collaboration of the SCS partners) shall provide these procedures	High
CO-01.4	The SCS-P (with the collaboration of the SCS partners) shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the SCS	High

CO-02 POLICY FOR PLANNING AND CONDUCTING AUDITS

Objective

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the SCS.

Requirements

Ref	Description	Assurance Level
CO-02.1	<p>The SCS-P (with the collaboration of the SCS partners) shall document, communicate, make available and implement policies and procedures for planning and conducting audits, addressing at least the following aspects:</p> <ul style="list-style-type: none"> ● Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; ● Activities that may result in malfunctions to the SCS or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and ● Logging and monitoring of activities. 	Basic

CO-02.2	The SCS-P (with the collaboration of the SCS partners) shall document and implement an audit programme over three years that defines the scope and the frequency of the audits in accordance with the management of change, policies, and the results of the risk assessment	Substantial

CO-03 INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM

Objective

Subject matter experts regularly check the compliance of the ISMS to relevant and applicable legal, regulatory, self-imposed or contractual requirements.

Requirements

Ref	Description	Assurance Level
CO-03.1	The SCS-P(with the collaboration of the SCS partners) shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control system	Basic
CO-03.2	The internal audit shall check the compliance with the requirements of the scheme	Basic
CO-03.3	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked	Substantial
CO-03.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions	High
CO-03.5	The SCS-P shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate SCS-P's subject matter experts for immediate assessment and action	High

CO-04 INFORMATION ON INTERNAL CONTROL SYSTEM ASSESSMENT

Objective

The top management of the SCS-Pis kept informed of the performance of the internal control system in order to ensure its continued suitability, adequacy and effectiveness

Requirements

Ref	Description	Assurance Level
CO-04.1	The SCS-P and the SCS-BPs shall regular inform its top management about the information security performance within the scope of the internal control system.	Basic
CO-04.2	This information shall be included in the management review of the internal control system that is performed at least once a year	Substantial

A.20 PRODUCT SAFETY AND SECURITY (PSS)

Provide appropriate mechanisms for supply chain customers

PSS-01 ERROR HANDLING AND LOGGING MECHANISMS

Objective

Customers have access to sufficient information about the SCS through error handling and logging mechanisms.

Requirements

Ref	Description	Assurance Level
PSS-01.1	The SCS-P shall offer to their SCS partners error handling and logging mechanisms that allow them to obtain security-related information about the security status of the SCS	Basic
PSS-01.2	<p>The information provided shall be detailed enough to allow SCS partners to check the following aspects, insofar as they are applicable to the supply chain service:</p> <ul style="list-style-type: none"> ● Which data, services or functions available to the user within the SCS, have been accessed by whom and when (Audit Logs); ● Malfunctions during processing of automatic or manual actions; and ● Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. 	Substantial

PSS-01.3	The logged information shall be protected from unauthorised access and modification	Substantial
PSS-01.4	When the SCS partner(s) is responsible for the activation or type and scope of logging, the SCS-P shall provide appropriate logging capabilities	Substantial
PSS-01.5	The SCS-P shall make the information available to customers via documented interfaces that are suitable for further processing this information as part of their Security Information and Event Management (SIEM).	High

Appendix B - Meta-Approach for the Conformity Assessment of SCSs

We make the assumption that the SCS-P with the SCS-BPs have used the CYRENE enhanced risk assessment methodology (CYRENE Report 3) in order to identify and manage the SCS- cybersecurity risks and they have developed the protection profile (SCS-PP).

In the Mutual Agreement between the SCS-P and the SCS-BPs it is assumed that the following are included:

The composition of the supply chain service (in terms of business partners involved, processes, and ICT assets);

A SCS-ISMS has been created where the latest documentations of the SCS-assets and the controls is included in the inventory;

The latest risk assessment and risk treatment plan of the SCS is included in the SCS-ISMS

The security policy and all security reports (e.g. BCP, DRP) of the SCS are uploaded in the SCS-ISMS SCS-Protection Profile (SCS-PP) that describe the security requirements, objectives, etc.

Direction and guidance of assessment/audit procedures;

Acceptance of risk levels' threshold

Based on the above assumptions this appendix describes the overall flow and requirements of the Conformity Assessment of supply chain services where the assessor may use the CYRENE methodology (CYRENE Report 3) in order to assess the claims in the SCS-PP of the submitted SCS for evaluation (SCS-TOE).

The standards that the assessor needs to take into account are:

ISO 17021 - Conformity assessment — Requirements for bodies providing audit and certification of management systems;

ISO 27007/2017 - Information technology - Security techniques - Guidelines for information security management system auditing;

ISO 19011 - Guidelines for auditing management systems;

ISAE 3000 - Assurance engagements other than audits or review of historical financial information;

ISAE 3402 - Assurance reports on controls at a service organization.



The term “audit” is used for all assessment activities leading to an assurance report; this assurance report forms after evaluation by a Certification Body the basis for awarding a certificate.

Objective of the Conformity Assessment

The overall objective is to determine whether or not and to what extend a supply chain service delivered by a group of SCS-BPs is in conformity with the control and security requirements defined in the proposed CYRENE EUSCS scheme.

The SC-BPs prepare the description of the supply chain (“Description”), and the accompanying SC-BPs’ assertion (“Management Assertion”), including the completeness, accuracy and method of presentation of that description and assertion.

The object of conformity assessment (the subject matter) is the management assertion and the underlying documentation and operation as described in the description.

For the basic level, as mentioned in the EUCSA, an approach leading to a limited level of assurance is defined, using the evidence based conformity assessment approach. For the levels substantial and high a full audit approach is defined leading to reasonable assurance.

1.1 Basic Level

The objective is to provide limited assurance through limited evaluation (review) of the control framework of the SCS business partners by an independent auditor/reviewer that the SCS is built and operated with procedures and mechanisms to meet the corresponding control and security requirements at a level intended to minimise the known basic risks of incidents and cyberattacks: the evidence based conformity assessment approach.

1.2 Substantial Level

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent auditor that the supply chain service is built and operated with procedures and mechanisms to meet the corresponding control and security requirements:

The SCS is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.

The SCS business partners have assessed those risks and implemented suitable controls that, if operating effectively, minimise those risks and meet the corresponding security requirements as of a specified date or throughout a specified period.

An independent auditor evaluates the risk assessment approach and the design effectiveness of controls as of a specified date during the initial conformity assessment. In subsequent conformity assessments the controls are tested for operating effectiveness (consistent application) throughout a specified period.

1.3 High Level

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent auditor that the supply chain service is built and operated with procedures and mechanisms to meet the corresponding control and security requirements as defined by the EUSCS.

The SCS is built and operated with procedures and mechanisms to minimise the risk of state-of-the-art cyberattacks carried out by threat actors with significant skills and resources.

The SCS business partners have assessed those risks and implemented suitable controls that operated effectively to minimise those risks and meet the corresponding security requirements throughout a specified period.

Automated controls are monitored for continuous operation in accordance with their design and tested for functional effectiveness to validate their actual ability to prevent or detect security breaches.

Tests for functional effectiveness are performed by the independent auditor or a third party (for example a party with expertise in hacking) engaged by the SCS business partners with the objective to identify vulnerabilities that allow to circumvent, override or breach controls

Before agreeing to accept, or continue, an assessment or certification engagement the assessor shall:

Verify by performing a review of the application to determine whether the request is appropriate i.e. the assessor shall obtain all the necessary information to complete the assessment and certification process in accordance with the relevant certification scheme. This includes at minimum the following information

The description of the supply chain service (SCS TOE) and underlying and supporting processes/assets (depending of the adopted view) (“Description”), and the accompanying protection profile (“Management Assertion”), including the completeness, accuracy and method of presentation of that description and assertion;

the SCS to be certified;

the standards and/or other normative documents

name and the address(es) of the SCS-P and all SCS partners (and their third parties) responsible to the service to be certified, and of all the physical location(s) involved in activities related to the service to be certified, a description of the significant aspects of the process, operations and SCS assets related to the SCS (based on the view(s)) to be certified;

The assessor shall conduct a review of the information obtained for application to ensure that:

- a) the information about the SCS TOE is sufficient for the conduct of the certification process;
- c) the scope, view and perimeter of certification sought is defined;
- d) the means are available to perform all evaluation activities;
- e) the assessor has the competence and capability to perform the certification activity.

Determine whether the assessor has the resources, capabilities and competence to perform the engagement, that have knowledge of the relevant sector of the SCS, an understanding of SCS business, technological and information technology and SCS systems and experience in evaluating risks as they relate to the suitable design of controls, and experience in the design and execution of tests of controls and the evaluation of the results.

The assessor starts the assessment by executing audit (or assessment) procedures in 4 major categories

1 Planning the risk assessment;

2 Execution of assessment procedures;

3 Evaluation of results;

4 Issue of an assurance report

Planning the risk assessment

The assessor shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the engagement, and determining the nature, timing and extent of planned assessment procedures that are required to be carried out in order to achieve the objective of the conformity assessment. This activity shall result in an audit plan as described in ISO 19011 and 27007.

For each activity mentioned below: the auditor need to document the procedures executed, the information and documentation used, the evidence gained, and the conclusion reached.

In this phase the assessor is:

- Obtaining an understanding of the supply chain service by reading provided documentation and inquiries of SCS partners involved. The auditor shall identify the boundaries of the SCS TOE
 - Assessing the applicability of the criteria as set in the CYRENE EUSCS scheme
 - Determine which assessment approach is appropriate (CYRENE methodology -CYRENE Report 3-may be an option)
 - Determining audit activities: nature, timing and extent of audit procedures to be executed: writing the detailed audit plan to be executed. The nature (what kind of audit procedure), the extent (how many or how often to execute the procedure) and the timing (at what point in time or over what

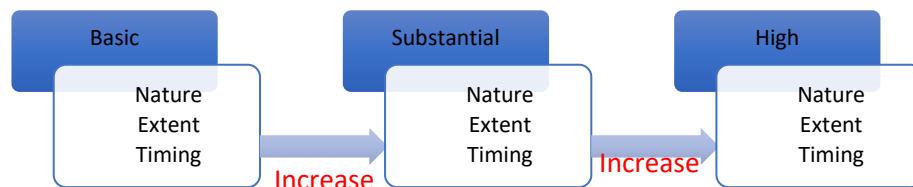
period) of evidence gathering procedures will vary between engagements. The procedures selected depend on the auditor’s judgment, including the assessment of the risks of material non-conformity of the matter being investigated;

- Determining the roles and responsibilities of the audit team members, as well as guides and observers or interpreters;
- Determining the logistics and communications arrangements, including specific arrangements for the locations to be audited (e.g. SCS-ISMS in the SCS-P premises, or in the SCS-P and SCS-BPs premises or in the locations of all SCS-assets);
- Determining matters related to confidentiality and information security of records obtained during the audit;
- Determining any follow-up actions from a previous audit or other source(s) e.g. lessons learned, project reviews.

For High Level: the approach to continuous auditing. Determining the nature, timing and extent of audit procedures

Sufficient and appropriate objective evidence can be obtained through observation, measurement, testing (if possible using sampling techniques), and inspection or by other means (see table). Objective evidence for the purpose of audit generally consists of records, statements of fact or other information that are relevant to the audit criteria (required control and security measures) and verifiable.

The nature (what kind of audit procedure), the extent (how many or how often to execute the procedure) and the timing (at what point in time or over what period) of evidence gathering procedures will vary between engagements and depends on the required assurance level and the auditor’s judgment, including the assessment of the risks of material non-conformity of the matter being investigated. All the three elements increase in scope, depth and rigour as the level of assurance increases.



Sufficient and appropriate objective evidence can be obtained through a number of activities:

- verification,
- testing (if possible, using sampling techniques),
- validation,
- review, and
- inspection,

using one or more of the following approaches:

Audit or assessment procedure	Description

Corroborative Inquiry	Conducting detailed interviews with relevant personnel to obtain evidence that the control was in operation during the reporting period and is accompanied by other procedures that are necessary to corroborate the information derived from the inquiry.
Observation	<p>In case of determining operating effectiveness: observing the performance of the control multiple times throughout the reporting period to evidence application of the specific control activity.</p> <p>The technique of sampling can be used to select the number of tests.</p>
Examination of documentation / Inspection	If the performance of the control is documented, inspecting documents and reports indicating performance of the control.

Re-performance of monitoring activities or manual controls	Obtaining documents used in the monitoring activity or manual control activity and independently re-performing of the procedures. Comparing any exception items identified with those identified by the responsible control owner.
Re-performance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.
Sampling	The size of the samples to select in order to test the operating effectiveness of controls implemented in the SCS-assets primarily depends on the nature of the

	control, the criticality of the SCS-asset within the SCS and the assurance level of the SCS.
--	--

General guidance

The CYRENE EUSCS scheme is not describing audit procedures detailed per security control/requirement, but general guidelines how to perform some of the audit activities. The scheme is not forcing the auditor to apply specific test procedures in each and every case, since although they will all have certain elements in common, the actual design, implementation and operation of the technical and organizational measures to meet the security requirements, will be different per SCS. As the actual design, implementation and operation of these measures will be different per SCS; the risks depend e.g. on the SCS view adopted, the sector and environment in which the SCS operate.

To deal with this situation, the auditor must be able to tailor the test procedures for the specific circumstances. By doing so, at least the auditor will perform an individual risk assessment to minimise the audit risk (the risk that the auditor expresses an inappropriate audit opinion).

Relation of security requirements and assessment procedure

The assessment procedure needs to be adapted to a specific security requirement and desired level of certification. Security requirements have been constructed in a way that all security requirements for level basic are applicable to levels substantial and high, while security requirements for level substantial also apply to level high. Therefore, it is necessary to assess all security requirements on the specific level, including those from lower levels. Security requirement, which was initially written for level basic, and still applicable to levels substantial and high, would be assessed in a different way according the certification level.

For each security requirement, the assessor needs to assess, depending on the assessment level:

For level basic, the assessor needs to verify that the security requirement is documented and the security requirement being implemented or followed.

For level substantial, the assessor (CAB in this case) needs to verify, in addition to the previous point that the security requirement is implemented correctly and is operating effectively, by obtaining objective evidence, by testing several known good and known bad samples.

For level high, the assessor (CAB in this case) needs to verify, in addition to the previous point, that the security requirement is functional effective

The following example illustrates the approach of a security requirement given initially for level basic, stating that a certain policy exists:

level basic: it is necessary to verify that a document describing a SCS security policy exists and that there is evidence that this policy is being followed.

level substantial: in addition to existence of a SCS security policy, it would be necessary to verify the correctness of the implementation, by trying several known good and known bad samples

level high: in addition to existence of a SCS security policy, its correct implementation, it would also necessary to verify that policy was operating correctly historically (or through a certain time period) and was monitored.

5 Execution

In the phase the auditor is obtaining sufficient and appropriate objective evidence (starting with the information, e.g. documentation of SCS-assets and controls uploaded in the SCS-ISMS) regarding:

- the suitability of the design of controls, including controls over the out-sourced processes (such as hosting, infrastructure, platform, etc.) to meet the security requirements of the proposed CYRENE EUSCS;
- the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date);
- the operating effectiveness of the implemented controls throughout a period over time (specified period);
- and for high level: the functional effectiveness of automated controls to validate their actual ability to prevent or detect security breaches.

The auditor documents the procedures executed, the evidence gained and conclusions reached.



5.2 Suitability of the Design

A control is suitable designed, when actions or events that comprise a risk (e.g. for information security) are prevented, or detected and corrected. Obtaining evidence regarding the suitability of the design of controls requires the auditor to determine whether

The risks that threaten the achievement of the control objectives to meet the security requirements of the EUSCS have been identified by management;

The controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives to meet the security requirements of the EUSCS from being achieved.

This requires the auditor to do the following:

- obtaining an understanding of management’s process for identifying and evaluating the risks that threaten the achievement of the control objectives and assessing the completeness and accuracy of management’s identification of those risks,
- evaluating the linkage of the controls with those risks, which is typically a consideration of frequency or timing of the occurrence or performance of the control (e.g. monthly, weekly, per triggering action or event such as a service request);
- party responsible for conducting the control (e.g. competence and authority of the person, group or system);

- specific activity being performed by the party to determine especially how the control is triggered, how it is executed, which tools or systems are used to support the execution and which records are kept evidencing the execution; and
- source of information to which the control is applied to determine whether this source is reliable and ensures for completeness and accuracy of information processing.

Obtaining evidence regarding the suitability of the design of controls typically requires the auditor to examine the documentation of the control that describe how the control should operate, e.g. written policies, procedures or process flowcharts.

5.3 Existence and Implementation

The controls have to be placed in operation as designed. After the auditor has concluded that a control is suitable designed, is has to be concluded per control whether the control actually exists and is implemented as designed. This requires the auditor to start by assessing the documentation of controls in the ISMS-SCS, obtain evidence related to exemplary actions or events that triggered the occurrence or performance of the controls (e.g. tickets) and to inspect the environment in which it operates (e.g. suitable configuration of the tools or systems used to execute the control in accordance with the design).

5.4. Operating effectiveness

Controls considered to be suitable in design, may be tested for operating effectiveness over a certain period of time (specified period). The auditor has to design the tests in a manner to cover a representative number of actions and events that triggered the occurrence or performance of the controls throughout the specified period, which is typically 6 to 12 months.

In determining the nature, timing and extent of the tests the following needs to considered:

- the nature and frequency of the controls being tested,
- the types of available evidential matter,
- the nature of the criteria to be achieved;
- the assessed level of control risk,
- the expected efficiency and effectiveness of the tests, and
- the results of our tests of the control environment.

A control is operating effectively, if it was consistently applied as designed throughout the specified period, and in case of manual controls, they were applied by individuals who have the appropriate competence and authority (e.g. changes being only approved by personnel who are responsible for the service being provided). It requires the auditor to perform other procedures such as inspection, observation, or re-performance in combination with inquiry to obtain evidence about the following:

- How the control was applied
- The consistency with which the control was applied
- By whom or by what means the control was applied

An inquiry alone is NOT sufficient to determine whether a control, including controls, if applicable, over the out-sourced processes to sub-service providers, operated effectively.

5.5. Functional effectiveness (applicable for level High)

Although controls maybe suitable designed in terms of documentation and operating effectively in terms of consistent implementation and application throughout a specified period, tests for functional

effectiveness of automated controls shall provide additional assurance that these controls are actually able to prevent or detect security breaches.

This requires the auditor to design technical validations to determine whether vulnerabilities in the technical implementation (e.g. configuration failures) of the controls can be exploited to breach the information security of the supply chain service.

6 Evaluation of results

6.1 Evaluation of evidence obtained

The auditor has to evaluate the sufficiency and appropriateness of the evidence obtained from the SCS-P to conclude about the suitability of the design, existence and implementation, operating effectiveness and, if required, functional effectiveness of the controls. The evidence obtained shall be sufficient to enable the auditor to take informed decisions.

In addition, when using information produced (or provided) by the SCS-P, the auditor has to evaluate whether the information is sufficiently reliable for the planned audit procedures by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise, detailed, consistent and current.

Sufficiency is the measure of the quantity of evidence. The quantity of evidence needed is affected by the risks of that the description is not fairly presented and that the controls were not suitably designed or operating and, if required, functioning effectively, and also by the quality of such evidence (the higher the quality, the less may be required). Obtaining more evidence, however, may not compensate for its poor quality. Appropriateness is the measure of the quality of evidence; that is, its relevance and its reliability in providing support for the auditor's opinion. The reliability of evidence is influenced by its source and by its nature, and is dependent on the individual circumstances under which it is obtained.

All relevant evidence has to be considered, regardless of whether it appears to corroborate or to contradict the evaluation of the description or the controls against the applicable security requirements of the EUSCS.

If the auditor is unable to obtain sufficient appropriate evidence, a scope limitation exists and the auditor shall express a qualified opinion, or withdraw from the engagement.

6.2 Evaluation of controls to meet the applicable security requirements of the EUSCS

The auditor has to consider whether the controls fully cover all aspects of the security requirements. Several controls may be required in combination per security requirement to fully meet each security requirement. An adjustment of the description may be waived if the descriptions of the auditor's test procedures clearly state how the aspects of the security requirements not covered by the control description were evaluated. Such test procedures shall be marked in an appropriate form (e.g. "Further test procedure for assessing full coverage of the security requirement").

The auditor's test procedures and the results thereof shall be documented in a repository. In describing the tests of controls, the auditor shall clearly state per control tested, whether the items tested represent all or a selection of the items in the population. The auditor shall further indicate the nature of the tests in sufficient detail to enable the report recipients to determine the effect of such tests on their risk assessments (e.g. whether the auditor's test procedures provide sufficient assurance for their needs).

A finding of nonconformity shall be recorded against a specific requirement, and shall contain a clear statement of the nonconformity,

If deviations (or exceptions, nonconformities) have been identified, the auditor shall record them against a specific control, including a description of the objective evidence on which the deviation is based, the extent of testing performed that led to identification of the deviations (including the sample size where sampling has been used), and the number and nature of the deviations noted. The auditor shall report deviations even if, on the basis of tests performed, the service auditor has concluded that the related security requirement were met.

6.3 Deviation handling

If the audit procedures reveal deviations (or exceptions, nonconformities) in the design, operation or, if required, functionality of the controls, the auditor has to determine whether the applicable security requirements of the EUSCS were still met.

Issuing Assurance Report

After evaluating the result of the audit and assessment procedures the assessor issues an assurance report. The key parts of the assurance report are:

- Management's assertion.
- Description of the supply chain service and the control framework.
- Independent auditors' report.

Once the assurance report has been delivered (using the template in Appendix E - Scheme Document Content Requirements) to the SCS-P, the assessor shall perform the following activities:

- Review of the evaluation
- Certification decision
- Certification

These steps will be clarified in Appendix C where we describe the CA for Basic Level SCSs.

Appendix C – Conformity Assessment for Level Basic

The scope of this appendix is to describe conformity assessment (CA) meta method (see Appendix B) for level Basic. We make the same assumptions here as in Appendix B that the SCS-P with the SCS-BPs have used the CYRENE enhanced risk assessment methodology (CYRENE Report 3) in order to identify and manage the SCS- cybersecurity risks and they have developed the protection profile (SCS-PP).

In the Mutual Agreement between the SCS-P and the SCS-BPs it is assumed that the following are included:

The composition of the supply chain service (in terms of business partners involved, processes, and ICT assets);

A SCS-ISMS has been created where the latest documentations of the SCS-assets and the controls is included in the inventory;

The latest risk assessment and risk treatment plan of the SCS is included in the SCS-ISMS

The security policy and all security reports (e.g. BCP, DRP) of the SCS are uploaded in the SCS-ISMS SCS-Protection Profile (SCS-PP) that describe the security requirements, objectives, etc

Direction and guidance of assessment/audit procedures;

Acceptance of risk levels' threshold

C.1 INTRODUCTION

At the Basic assurance level, the conformity assessment is greatly simplified, and it relies solely on evidence provided by the SCS-P, if needed upon explicit request from the assessor. For consistency reasons, we will use the same terminology (audit, auditor, audit team) as for the other assurance levels, also the evaluation performed is not a full-fledged audit of the SCS to be certified.

For the AL Basic the reviewer shall use the approach defined in the present Appendix.

This approach is facilitating a controlled environment for providing limited assurance while keeping the associated cost for certification affordable for smaller SCS-Ps, through limited evaluation of the control framework of the SCS-P by an independent reviewer that the SCS is built and operated with procedures and mechanisms to meet the corresponding Security Objectives and related Security Requirements defined in the EUSCS.

The EUCSA requires for the assurance level Basic that the evaluation must minimize the known basic risks of incidents and cyberattacks, and that a review of technical documentation is required at a minimum.

While the SCS-P shall be required to conduct the necessary initial verification of compliance with the objectives and controls of this scheme, at the basic level there will be a review of the documentation created or compiled by the SCS-P as a part of its internal verifications. In particular the assessor will ask to review the documentations of the SCS-assets and their controls of the SCS-ISMS.

C.2 ACCEPTING THE CONFORMITY ASSESSMENT ENGAGEMENT

Before agreeing to accept or continue a conformity assessment engagement, the assessor shall determine whether the application request is appropriate by performing a review of the application.

The assessor shall conduct a review of the information obtained for application to assess the applicability of the criteria as set in the EUSCS, including the decision whether the chosen assurance level is appropriate in the circumstances, and to ensure that:

the application request contains all the mandatory information;

the information about the SCS is sufficient for conducting of the assessment and the certification process;

the SCS-P has acknowledged and understands its responsibilities;

any known difference in understanding between the assessor and the SCS-P is resolved, including agreement regarding standards or other normative documents;

the scope of certification is clearly defined;

the means are available to perform all evaluation activities;

the resources, capabilities and competences are available to perform the engagement, including knowledge of the relevant industry, an understanding of information technology and systems and experience in evaluating risks as they relate to the suitable design of controls, and experience in the design and execution of tests of controls and the evaluation of the results.

In addition, the auditor shall obtain a legally binding declaration of the SCS-P that it acknowledges and understands its responsibility and complies at least, with the following:

the SCS-P is responsible for the preparation of the description of its system (“Description”), and accompanying SCS-P’s assertion (“Management Statement”);

if the certification applies to ongoing service provision, the certified service continues to fulfil the security requirements;

the SCS-P agrees to on-site reviews in case they would be necessary to clarify assertions or to resolve complaints disputes;

the SCS-P claims regarding certification consistent with the scope of certification;

the SCS-P does not use its service certification in such a manner as to bring the certification body into disrepute and does not make any statement regarding its service certification that the certification body may consider misleading or unauthorised;

upon suspension, withdrawal, or termination of certification, the SCS-P discontinues its use of all advertising matter that contains any reference thereto and takes any other required measure, and inform their customers;

in referring to its service certification in communication media such as documents, brochures or advertising, the SCS-P complies with the requirements of the certification body;

the SCS-P complies with any requirements that may be prescribed in the certification scheme relating to the use of marks of conformity, and on information related to the service;

the SCS-P keeps a record of all complaints made known to it relating to compliance with security requirements and makes these records available to the certification body when requested, and

takes appropriate action with respect to such complaints and any deficiencies found in service that affect compliance with the security requirements;

documents the actions taken;

the SCS-P informs the certification body, without delay, of changes that may affect its ability to conform with the certification requirements.

the SCS-P agrees to fees payable to the assessor for the execution of the conformity assessment communicated beforehand

In the case of a recertification, the assessor shall also ensure that:

the trigger for the recertification is clearly described; and

where applicable, the SCS-P has provided an impact assessment of the changes implemented since the last assessment.

Once all the review criteria are fulfilled and the assessor and SCS-P have reached an agreement about the conditions of the engagement, the auditor shall conduct the following major audit activities:

- Developing the audit plan (section C.3);
- Execution of assessment procedures (section C.4);
- Analysis of results (section C.5);
- Issue of an assurance report (section C.6) and of an evaluation report (section F.4.2).
- Once the auditor has delivered the assurance report, the assessor shall perform the following activities:
 - Review of the evaluation (section C.7);
 - Certification decision (section C.8); and
 - Certification (section C.9).

That are described in details in the following sections.

C.3 DEVELOPING THE AUDIT PLAN

C.3.1 Introduction

The assessor shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the audit to be carried out in order to achieve the objective of the conformity assessment. This can be achieved by using a predefined audit plan.

For each activity mentioned below: the auditor shall document the high-level audit plan following the requirements defined in Appendix E - Scheme Document Content Requirements, including the procedures executed, the information and documentation used, the evidence gained, and the conclusion reached.

There shall be at least one meeting between the assessor and the SCS-P during the development of the audit plan, to provide clarifications about the SCS and related controls and about the next phases of the audit.

C.3.2 Initial activities

In this phase the assessor shall:

Obtain an understanding of the SCS (which is the Target of Evaluation -TOE-) and the controls to meet the Security Control Objectives and related Security Requirements, by reviewing provided asset and controls documentation (found in the SCS-ISMS and inquiries of SCS-BPs and people involved).

The auditor shall obtain and read the SCS-TOE description and the SCS protection profile (PP) provided, identify the boundaries, the interactions and interdependencies among the SCS-assets hosted by the different SCS-partners and shall evaluate whether those aspects of the description are fairly presented.

Review the SCS-P's mapping between the Security Objectives and related Security Requirements as defined by the EUSCS and the SCS-PP:

To conclude whether the applicable Security Control Objectives and related Security Requirements of the EUSCS are covered by the SCS controls that have been implemented;

To identify any remaining risks (as a result of gaps in the mapping) and the possible impact of them;

Determine which SCS-BP to what extent, for which processes of the SCS are responsible, which SCS-assets is hosting, what controls has implemented, if the SCS-BP uses sub service providers, how the SCS-BPs control and monitors the services provided by these sub service providers and how the SCS-P is being informed

To determine which assessment approach is appropriate: using the inclusive or carve-out method.

To identify which sub service providers do have an acceptable assurance report which can be (re)used.

Review how the SCS-P and SCP-BPs deal with complementary controls towards customers and towards sub service providers, as well complementary controls of sub service providers towards the SCS-P:

Do the SCS-P and the SCS-BPs have CCC for its costumer defined?

Do the SCS-P and the SCS-BPs have an agreement regarding risk threshold acceptance and mitigation responsibilities for their subcontractors as well?

Consider the relative importance and effect of possible omissions or deviations with respect to the fair presentation of the description,

whether the description includes the significant aspects of the SCS;

whether the description omits or distorts relevant information;

Evaluate the implemented SCS-controls based on the documentation provided and if needed obtain sufficient and appropriate objective evidence about the design and implementation of the SCS-controls to meet the Security Control Objectives and related Security Requirements as defined by the EUSCS by using a review plan.

C.3.3 The audit plan

Sufficient and appropriate objective evidence about the design and implementation of the SCS-controls can be obtained through, inspection of the provided documentary evidence (control documentation found in the SCS-ISMS) and if necessary, by inquiry to be able to evaluate the provided documentary evidence in order to determine whether

1. the evidence addresses the security requirements of the scheme in a sufficiently comprehensive manner;
2. the evidence is sufficiently clear and unambiguous in how the requirements are met and how controls have been implemented by the SCS-BPs;
3. the evidence is prima facie plausible (i.e. it appears in the professional opinion of the reviewer that there are no elements in the evidence that are manifestly inaccurate, incomplete or false) and verifiable (can in principle be verified by an on-site audit).

This can be achieved by using a standardised self-assessment and audit plan. The assessor shall then provide the self-assessment plan to the SCS-P, together with indications on its specific application to the targeted SCS.

C.4 EXECUTION

In this phase the auditor shall obtain sufficient and appropriate objective evidence by evaluation the provided documentary evidence by the SCS-P regarding:

the suitability of the design of controls, including controls over the out-sourced processes (such as hosting, infrastructure, platform, etc.) to meet the Security Control Objectives and related Security Requirements as defined by the EUSCS;

the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date).

The execution phase starts when the SCS-P gives the results of the self-assessment, together with all required supporting documentation, i.e. asset/control documentation, SCS-risk assessment report, SCS-risk treatment plan (from the SCS-ISMS). The auditor shall document the procedures executed, the evidence gained and conclusions reached using a standardised document.

A control is suitably designed when actions or events that comprise a risk (e.g. for information security) are prevented or detected and corrected. Obtaining evidence regarding the suitability of the design of controls requires the auditor to determine whether

The risks that threaten the achievement of the Security Control Objectives and related Security Requirements as defined by the EUSCS have been identified by management;

The controls are, if operating effectively, able to prevent or detect Security Control Objectives and related Security Requirements of the EUSCS from not being met.

In order to prevent, or detect and correct actions that comprise a risk, the controls have to be placed in operation as designed. After the auditor has concluded that a control is suitably designed, is has to be concluded per control whether the control actually exists and is implemented as designed by examining the provided documentary evidence. To be able to conclude on this the reviewer shall obtain evidence related to exemplary actions or events that triggered the occurrence or performance of the controls (e.g. tickets) and to inspect the environment in which it operates (e.g. suitable configuration of the tools or systems used to execute the control in accordance with the design).

C.5 ANALYSIS OF RESULTS

In forming the conclusions on the evidence obtained the auditor shall:

Evaluate whether the described technical and organizational controls refer to or describe the applicable requirements of the Certification framework;

Consider whether the provided documents adequately disclose the significant information security policies and the selected and implemented technical and organizational measures;

Consider whether the information security policies and technical and organizational measures are deemed suitable to meet the Security Control Objectives and related Security Requirements of the EUSCS considering the nature of the service;

The information provided appears relevant, reliable, comprehensive and comparable.

On this basis the auditor shall assess if it can be concluded that nothing has come to its attention that causes the reviewer to believe that the technical and organizational manners warranted by the SCS provider are not meeting in all material aspects the requirements of the Basic level in accordance with the Certification framework and that the evidence presented is at least sufficient for the reviewer to obtain a limited level of assurance.

The auditor shall document the results of the review in the report according to the examples in the (mapping) Table below.

Table 6: Example of review results report

Security objectives control	<Service-Org>'s Description of Controls	Documentary evidence used or other means of evidence	Test results
Objective: Description			
ID – Security requirement	ID – Title of Control [Control Description]	Description of the evidence	Result

There shall be at least one meeting between the assessor and the SCS-P during the execution phase or the analysis of results, during which the assessor may ask for additional documentation or make specific inquiries to consolidate the evidence and the analysis of results.

C.6 ISSUING THE ASSURANCE REPORT

After evaluating the result of the audit procedures, the auditor shall form a conclusion and issue an evaluation report.

The conclusion shall be based on the evidence obtained and the procedures performed, and express whether, in all material respects, nothing has come to the reviewer's attention that the

SCS-P description does not fairly presents its SCS, including the controls to meet the Security Control Objectives and related Security Requirements of the EUSCS, and is free from material misstatements as of a specified date;

SCS-controls are not in conformity with the Security Control Objectives and related Security Requirements of the EUSCS as of a specified date.

The reviewer shall issue the assurance report using the template in Appendix E - Scheme Document Content Requirements.

This assurance report shall be first addressed to the SCS-P.

C. 7 REVIEW OF THE EVALUATION

Once an assurance report and an evaluation report (and, if required, supporting reports) have been delivered by the auditor, the assessor shall perform a review of all information and results related to the evaluation, based on these reports:

- The review shall not be subcontracted;
- The review shall be carried out by one or more people who have not been involved in the audit phase, whom will be called collectively the reviewer;
- The recommendations for a certification decision based on the review shall be documented, unless the review and the certification decision are completed concurrently by the same person;
- The persons carrying out the review shall not normally overturn a negative recommendation of the audit team. If such a situation does arise, the assessor shall document and justify the basis for the decision to overturn the recommendation.

The review shall include at least the following activities:

- A review of the sufficiency of the information provided in the assurance report and supporting documentation with respect to the EUCS requirements and the certification scope;
- A review of the nonconformities identified in the assurance report and related corrective actions;
- A review of the issues identified in the evaluation report's dependency analysis; and
- A recommendation for the certification decision, based on a documented opinion on whether or not the requirements of the EUCS have been satisfied by the SCS-P and by the auditor.

C 7.1 Review of the sufficiency of the assurance report

The assessor shall review the assurance report and supporting documentation concerning the following aspects:

General

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- Does the report contain the required parts?
- Does the provided documentation include the required support documentation?
- Is the conformity assessment performed in due time?

Security controls and requirements

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- If there is a mapping from a set of controls provided by the SCS-P to the security controls and requirements defined in EUCS, is this mapping adequate?
- For every control or requirement analysed during the audit, have the appropriate activities been performed and documented?

Nonconformities

The assessor shall review the assurance report and support documentation concerning the handling of nonconformities detected during the audit.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer.

- For every major nonconformity identified during the audit, is adequate information provided in the assurance report?
- For every minor nonconformity identified during the audit, is adequate information provided in the assurance report?
- For every nonconformity identified during the audit, does the reviewer accept the analysis provided by the auditor?

C 7.2 Review of the evaluation report

Dependency analysis

The assessor shall review the dependency analysis and supporting documentation concerning the adequacy of the assurance documentation available about subservice providers.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- For every subservice provider mentioned in the assurance report, is there adequate assurance documentation available?
- For every assumption in the assurance report about a subservice provider, is the documentation available adequate to determine that assumption correct?

Recommendation for the certification decision

The assessor shall review the recommendation for the certification decision provided in the evaluation report and how it combined the conclusions of the audit report with those of the dependency analysis.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- Is the certification decision proposed in the assurance report adequate according to the provided documentation?
- In the case of a maintenance conformity assessment, does the proposed certification decision include all the information required to maintain the certificate, with proper justification?
- If the SCS depends on subservice providers, is the assurance documentation adequate or not to support the certification of the SCS-P using these subservice providers?

C 7.3 Review reporting

The results of the review shall be documented in a report, which shall include all the answers to the questions above, together with a justification.

If the conformity assessment results in the issuance or maintenance of a certificate, this review report shall be included in the publicly available certification or maintenance report.

C.8 CERTIFICATION DECISION

The assessor shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information. The certification decision shall be carried out by a person or group of persons that has not been involved in the audit activities (but may have been involved in the review process).

The certification decision shall not be subcontracted.

The assessor shall notify the SCS-P of a decision not to grant certification, to withdraw a certificate, or to suspend a certificate, and shall identify the reasons for the decision. The SCS-P may contest the assessor's decision. If the dispute remains unresolved, the SCS-P may file a complaint with the NCCA to request their opinion on the matter of the dispute.

C.9 CERTIFICATION

If the certification decision is negative, i.e. if the SCS has been determined not to meet the EUCS scheme's requirements, the consequences are as follows:

- In the case of an initial conformity assessment, no further action is required, i.e. no certificate shall be issued;
- In the case of a maintenance conformity assessment, the certificate shall be suspended by appending the maintenance report as rationale for the suspension, and then the process for handling nonconformities shall be followed.

If the certification decision is positive, i.e. if the SCS has been determined to meet the EUCS scheme's requirements, the consequences are as follows, depending of the nature of the assessment.

- In the case of an initial assessment, the assessor shall issue a new certificate, including the full certification report, and set the expiration date three (3) years after the date of issuance, unless the assessor has explicitly indicated a shorter validity period for the certificate;
- In the case of a periodic assessment, the assessor shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed;
- In the case of a renewal assessment, the assessor shall update the existing certificate by appending the maintenance report, by setting the expiration date of the certificate three (3) years after the date of this update, and if needed by updating elements in the certificate that have changed;
- In the case of a restoration assessment, the assessor shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed, and shall return the certificate's status to "certified";
- In the case of a restoration assessment, the assessor shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed;

The reports mentioned in the paragraph above are specified in [Appendix F: Scheme Document Content Requirements](#).

Appendix D – Conformity Assessment for Levels Substantial and High

The steps of the previous section are followed here. The assessor in this case is a Conformity Assessment Body (CAB).

Appendix E - Competence Requirements for Assessors

Assessors and Conformity Assessment Bodies (CAB) that wish to be accredited shall meet the following requirements.

Non-technical competences	
1	The assessor shall be a registered entity. In case of CAB, then shall be established under national law and shall have legal personality.
2	An assessor shall be a third-party body that is independent of the SCS that it assesses.
3	A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.
10	At all times and for each conformity assessment procedure and each type, category or sub-category of the SCS, the assessor shall have at its disposal the necessary: <ul style="list-style-type: none"> • staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; • descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities; • procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.
11	The assessor shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.
12	The persons responsible for carrying out conformity assessment activities shall have the following: <p>sound technical and vocational training covering all conformity assessment activities,</p>

	<p>satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments,</p> <p>appropriate knowledge and understanding of the applicable requirements and testing standards,</p> <p>the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.</p>
15	The assessor shall take out liability insurance and will be directly responsible for the conformity assessment.
16	The assessor and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of an assessor shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under Regulation (EU) 2019/881. The assessor shall have documented procedures in place in respect of the requirements of this point.
19	In case the assessor is a CAB, then shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes and the accreditation of laboratories performing testing.

Technical Competences

1	<p>ICT Evaluations: Understanding, knowledge and experience on (a) secure IC-based design (such as smartcard, secure element, etc.) and production process, (b) secure ICT technology, (c) hardware physical attack techniques, (d) physical disruptions and (e) cryptographic attack techniques</p> <p>Protection of the environment(s) (operational environment) and the several aspects of them, in which assets are located / Storage, processing and transmission of assets, in the form of information, is delivered by IT products and equipment with specific requirements. Penetration Testing competencies are required</p>
2	<p>Business Evaluations: Understanding, knowledge and experience of complex business processes and analysis of business and security impact</p>

Appendix F - Scheme Document Content Requirements

F.1 INTRODUCTION

The objective of this Appendix is to define guidelines for the redaction of documents. Rather than providing full templates, the Appendix lists requirements for writing the documents, which typically takes three forms:

Requirements on content that shall be present, without constraints on the format;

Requirements on text that shall be included as is, for a few important statements; and

Requirements on the format and content of tables, to ease comparability of results.

These requirements will be refined by specific guidance for every assessment type (ISO-based)

F.1.1 [Conventions used in this appendix](#)

Every section below starts with an introduction, followed by the requirements on the document, presented in a sequential manner that defines the structure of the document.

Within each section, this appendix uses with the following convention:

Requirements are typeset in plain text.

Guidance is typeset in *italics*.

Mandatory text is typeset in **bold**.

Items in a document are referenced by an identifier, which is defined within brackets in <SMALL CAPS> The rules for using these requirements are as follows:

Specified sections shall be present, in the order defined, but other sections may be added before, between and after the specified sections;

Within a section, mandatory text shall be present and the section's requirements shall be fulfilled, but additional content may be added;

F.1.2 [List of the documents](#)

Requirements and guidance are provided in this appendix for the following documents:

For the application phase: The Application Document, to be filled out by the SCS-P to initiate a conformity assessment

For the audit preparation phase: The Initial Activities Planning document, to be prepared by the SCS-P at the beginning of the conformity assessment

The Detailed Audit Plan and Execution, to be prepared by the SCS-P before the audit and updated with the results all along the audit.

For the reporting phase: The Assurance Report, to be prepared by the assessor to report on the audit of the supply chain service from the SCS-P.

The Evaluation Report, to be prepared by the assessor to report on the assurance provided by the SCS-P's subservice providers and to conclude on the audit by providing a certification recommendation.

The Review Report, to be prepared by the assessor after the internal review of the Assurance and Evaluation Reports.

For the certification phase: The Certification Report, to be prepared by the CAB (please note that not all assessors can issue a certificate, only if the assessor is a CAB) when the certificate is issued

For the maintenance phase: The Impact Analysis Report, to be prepared by the assessor when a request about a potential nonconformity or vulnerability does not lead to a conformity assessment.

The Maintenance Report, to be prepared by the assessor after a maintenance conformity assessment, with a focus on the updates to the SCS and on the reason that triggered the conformity assessment

These documents do not all have the same usage and availability:

The Application Document, Assurance Report and Evaluation Report are shared between the SCS-P and the assessor

In addition, the SCS-P shall make the Assurance Report available to its SCS partners

The Initial Activities Planning, Detailed Audit Plan and Execution, and the Review Report are internal documents for the assessor.

The Certification Report is a public document, to be published together with the certificate by a CAB.

All documents may be made available by the CAB to the NCCA and NAB for review or assessment.

Finally, the Assurance Report is only available in a version suitable for the Substantial and High assurance levels. A version suitable for the Basic assurance level will be provided in a later phase. Requirements for the Review Report, for the Impact Analysis Report and for the Maintenance Report are not available in the current version.

F.2 APPLICATION DOCUMENT

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the "Application Document".

A SCS-P shall apply these requirements in its application for certification of a supply chain service. The document shall include the information an assessor needs to start a conformity assessment. The completed template provides evidence of a self-assessment process executed by the management of the SCS-P.

Mandatory field in the template

Clarification

<p>Section 1: “Identification”</p> <p>This section identifies the SCS for which the evaluation application is submitted.</p>	
SCS Identity	Identity of the SCS requesting the evaluation.
SCS Contact	Identification and contact details for the lead contact at the SCS-P that will support the evaluation process.
Service Name	Commercial name of the SCS for which the evaluation is requested.
Short Description	A short description of the functionality of ‘Service Name’.
Assurance Level	The assurance level for which the evaluation is requested. Valid values are ‘Basic’, ‘Substantial’, or ‘High’.
Security Profiles	The list of security profiles applicable to the SCS
Application Type	SCS specified evaluation application type. Valid values are ‘initial’, ‘periodic’, ‘renewal’ or ‘restoration’.
Application Period	When applicable, the period to be considered by the assessor for the assessment of operational effectiveness.
<p>Section 2: “Claim”</p> <p>This section is the SCS’s management assertion the template accurately and fairly describes the SCS and the applicable controls from the scheme’s framework.</p>	
Claim	This is a written conformity statement by the management of the SCS (management of the SCS-P and the SCS-BPs).
<p>Section 3: “ Description of the SCS”</p> <p>This section is the SCS’s assessment of the SCS’s implementation of the scheme’s requirements and control framework.</p>	
3.1: Types of Services	The specific functional purposes of the SCS.
3.2: Service Components	This is a document label for reference purpose, no text required.
- Physical Infrastructure	The physical SCS-assets of the service, datacenter, server, other hardware.
- Software	The cyber SCS-assets programs and system software that supports programs, that are part of the service
- People	The personnel involved in the governance, operation and use of the SCS
- Policies and procedures	The policies and automated and manual procedures involved in the operation of a service

- Data	the information used and supported by a service (transaction streams, files, databases and tables).
3.3: Service Boundaries	The boundaries of the system subject to certification
<p>Section 4: “security controls”</p> <p>This section is the SCS implemented controls, and of their mapping to the EUSCS objectives and requirements.</p>	
Control objectives	The security objectives and documentation of controls implemented by the SCS-BPs to protect the SCS-assets.

CONTENT OF THE DOCUMENT

F.2.1 Identification

<SCS IDENTITY>

The SCS identity shall include at least:

Commercial name;

Legal name of the SCS-P;

Contact details of the person that is legally representing the SCS-P

<SCS CONTACT>

The SCS-P Contact shall be the primary contact at the SCS for the assessor. It can be an individual person or a SCS assigned group name. It shall include at least the name of the responsible department and contact details (phone number and email address).

<SHORT DESCRIPTION>

This shall be a description of the processes/ SCS-BPS/SCS-assets of the supply chain service

<ASSURANCE LEVEL>

This is the assurance level for which the SCS applies for certification; its value shall be one of Basic, Substantial or High.

For the appropriate choice refer to the description of the assurance levels.

<SECURITY PROFILE>

This shall be security profile applicable to the supply chain service, including for every security profile its full name, reference number, version number and date of issuance.

<APPLICATION TYPE>

This is the type of conformity assessment to be performed; its value shall be one of 'initial', 'periodic', 'renewal' or 'restoration'.

For Application Types 'periodic', 'renewal' and 'restoration', additional information is required in the description of the service.

<APPLICATION PERIOD>

When applicable (levels Substantial and High), this shall be the period that the assessor will consider in the assessment of operational effectiveness.

This period depends on the date of the last assessment, and it typically will be one year. For initial assessments, there are minimum values depending on the assurance level.

F.2.2 SCS's Management Statement

<MANAGEMENT STATEMENT>

This is the management state of the SCS, which shall be dated and signed, and which shall at least point out that:

- the documentation filed for certification is complete;
- this documentation is accurate and up-to-date;
- this documentation meets the requirements for certification in the EUSCS scheme; and
- this documentation is a true reflection of the processes, procedures and systems in place within the organisation in scope of the certification;
- the organisation and its management are committed to comply with all their obligations during the conformity assessment and after certification during the entire lifecycle of their supply chain service's certificate;
- the management of the applying organisation declares to be responsible for the abovementioned points;
- the management of the applying organisation declares to fully cooperate and be transparent to the extent needed to handle the complaints in the procedure for complaints ex Art. 63 of the EUCSA;
- the management of the applying organisation declares that it is providing full cooperation in investigative activities of the NCCA ex Art. 58(8) of the EUCSA;
- the management of the applying organisation declares that it is authorising and approving to cooperate in compliance audits of the certification issuing body and applicable peer reviews ex Art. 59 of the EUCSA, and if applying for assurance level 'high' to peer assessments as defined in the EUCS scheme ex Art 54(1)(u).

F.2.3 Description of the SCS

<SERVICE DESCRIPTION>

There is no mandatory content for the item <SERVICE DESCRIPTION>. This item is also the identifier for the information in the items of this section.

The SCS may include some guidance to help the reader through the rest of the section.

<SCS partners>

<SCS processes>

<SCS assets >

<Policies and Procedures>

F.2.4 The security objectives and SCS description of controls

<CONTROL OBJECTIVES>

The item <CONTROL OBJECTIVES> shall define how the security controls defined and implemented by SCS meet the security requirements defined in the EUSCS scheme. For each security requirement, the information shall include:

If the security requirement is not applicable to the SCS, an indication of this non-applicability, together with a rationale.

Otherwise, a list of the following controls, together with a description:

security controls that contribute to meeting of the security requirement;

The content of the <CONTROL OBJECTIVES> shall be organised in a table following the template shown below:

Security Control Objectives and related Security Requirements of the EUSCS	<SCS>'Description and Documentation of Controls,
Security Control Objective: [...].	
ID – Title of Security Requirement [Description of the Security Requirement]	ID – Title of Control 1 to meet the Security Requirement or Rationale if Security Requirement is not applicable [Control Description/Rationale]
	ID – Title of Control 2 to meet the Security Requirement [Control Description and Documentation of implemented control]

The proposed format of the certificate has three main sections: Identification, Claim and Assessment Result. Main elements of these sections are as follows:

17.1 - Identification of the Process/Service/Product

Name of the SCS-P and all SCS business partners, including both commercial and legal names

Registration number of the organizations
Contact details of the legal persons/sectors in charge
SCS name and ID (and /or version)
Short description of the SCS

17.2 - Claim (Conformity Statement)

Type of SCS and sector
SCS business partners
SCS processes and assets
Security requirements of the SCS
Security controls of the SCS
Assurance level for which the evaluation is requested (e.g. 'Basic', 'Substantial', or 'High')
Application type may refer to one of the specified application types: 'initial', 'periodic', 'renewal' or 'restoration'.
Application submission date

17.3 - Conformity Assessment Result

Identify of the Assessor or CAB in charge of the certification
Assessor contact including identification and contact details for the lead contact that will manage the evaluation process

Accreditation details on the ability of the assessor to perform an audit
Application number assigned to the application document upon receipt by the assessor
Application Type
Assurance level assigned by assessor
Date of assignment
Expiry date of the certification
Certificate ID

F.3 AUDIT PLANNING

F.3.1 Initial activities planning

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the recommendations for the “Initial activities planning and execution” document.

This document is an internal to the assessor. It may be part of the documentation provided by the auditor in addition to the evaluation report for the review phase. The assessor is free to modify the format, but the elements of information are important to

An assessor should apply these recommendations in its description of the initial audit activities to be performed as a preparation to the detailed audit planning, and in its reporting of these initial activities.

Mandatory field in the template	Clarification
Section 1: “ Activities ”	This section describes the initial activities of the audit. The items described below shall be filled out for every initial audit activity relevant for the targeted AL.

Objective	Objective of the activity
Information and documentation used	Information used in support of the activity
Evidence gained	Evidence
Conclusion reached	Conclusion for the activity
Date	Date of the conclusion
Initials	Initials or signature of the auditor

CONTENT OF THE DOCUMENT

F.3.1.1 *Activities*

The items listed below are recommended for the description of one activity, so they should be repeated for each activity described.

<OBJECTIVE>

The assessor should include the objective of the activity, as listed in the assessment requirements.

<INFORMATION AND DOCUMENTATION USED>

The assessor should list the documentation on which the activity was based (from the documentation provided by the SCS in the application document and in support of the application).

<EVIDENCE GAINED>

The assessor should describe the evidence gained from the activity.

<CONCLUSION REACHED>

The assessor should describe the conclusion reached for the activity.

The conclusions are expected to lead to easier

<DATE>

The assessor should indicate the date when the conclusion for the activity was documented.

F.3.2 Detailed audit plan and execution

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Detailed audit plan and execution” document for any assessment performed at level Substantial or High.

An assessor should apply these requirements in two phases:

during its description of detailed audit activities;

during the execution of the audit.

Mandatory field in the template	Clarification
<p>Section 1: “Audit activities”</p> <p>This section describes the activities of the audit. The items described below shall be filled out for every security objective relevant for the targeted AL.</p>	
EUSCS objective	The security objective and reference from EUSCS
1.1 Procedures	
Procedure Suitability	Information used in support of the activity
- Nature	Nature of the activity
- Timing	Timing of the activity
- Extent	Extent of the activity
Procedure re Existence	Audit activities to be performed
- Nature	Nature of the activity
- Timing	Timing of the activity
-Extent	Extent of the activity
Procedure re-Operating Effectiveness	Conclusion for the activity
- Nature	Nature of the activity
- Timing	Timing of the activity
- Extent	Extent of the activity, including sampling
1.2 Execution	

Sources	Information used and people inquired in support of the activity
Evidence gained	Evidence
Conclusion reached	Conclusion for the activity
Date	Date of the conclusion
Initials	Initials or signature of the auditor

CONTENT OF THE DOCUMENT

F.3.2.1 *Characteristics of an audit activity*

The document consists of descriptions of procedures to be applied to audit how the supply chain service fulfils the EUSCS objectives and requirements. Each audit activity should be described with the following parameters:

<NATURE>

The kind of audit activity to be performed, together with a description of the activity

<TIMING>

The timing of the activity, either as a point of time, or as a period to be covered

<EXTENT>

The extent of the activity, i.e., the number of times the activity needs to be performed, including a rationale if sampling is used

F.3.2.2 *Procedures*

The items listed below are recommended for the description of the procedures related to one security objective, so they should be repeated for each security objective described.

<EUSCS OBJECTIVE>

The assessor should include the objective of the activity, as listed in the assessment requirements, including the reference from EUSCS.

<PROCEDURE RE SUITABILITY>

The procedure to be executed for auditing the suitability of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

<PROCEDURE RE EXISTENCE>

The procedure to be executed for auditing the existence of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

<PROCEDURE RE OPERATING EFFECTIVENESS>

The procedure to be executed for auditing the operating effectiveness of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

F.3.2.3 **Execution**

This section describes the execution of the audit activities and the results achieved, including a conclusion about the fulfilment of the EUSCS requirements related to the security objective.

<SOURCES>

Information used and people inquired in support of the activities related to the objective.

<EVIDENCE GAINED>

Evidence that has been gained in the activities related to the objective.

<CONCLUSION REACHED>

Conclusion reached regarding the fulfilment of the objective and related requirements by the supply chain service.

<DATE>

Date of the conclusion.

<INITIALS>

Initials of the auditor in charge of the activities.

F.4 ASSURANCE AND EVALUATION REPORT

The evaluation phase results in two reports:

The assurance report resulting from the audit of the SCS;

The evaluation report that contains the dependency analysis (if required), together with the final recommendation from the evaluation;

F.4.1 **Assurance report**

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Assurance report” document.

The assurance report is the report from the audit activity, which is then completed by the evaluation report. The assurance report shall contain a detailed report of the conformity assessment activities performed by the assessor toward demonstrating that the assessed supply chain service meets the requirements of the scheme. The assurance report shall in addition include a recommendation regarding the certification of the assessed supply chain service.

An assessor shall apply these requirements when preparing the report at the end of the audit of the SCS. When the assessor is a CAB the following template can be used:

Mandatory field in the template	Clarification
<p>Section 1: “Identification”</p> <p>This section identifies the conformity assessment body in charge of the certification, and the supply chain service being audited.</p>	
1.1 CAB	
CAB identity	Identify of the CAB in charge of the certification
CAB contact	Identification and contact details for the lead contact at the CAB that will manage the evaluation process
Accreditation details	Details about the ability of the CAB to perform an audit
Lead auditor	Affiliation, contact information and qualification of the lead auditor
Audit team	Affiliation, contact information and qualification of the audit team members
1.3 SCS	
SCS identity	Identity of the SCS requesting the evaluation.
SCS-P contact	Identification and contact details for the lead contact at the CSP that will support the evaluation process
1.4 Supply Chain service	
Service Name	Commercial name of the Supply Chain Service for which the evaluation is requested
Short Description	A short description of the functionality of ‘Service Name’.
Assurance Level	The assurance level for which the evaluation is requested. Valid values are Basic, Substantial and High
Security Profiles	The list of security profiles applicable to the supply chain service
Application Type	SCS-P specified evaluation application type. Valid values are ‘initial’, ‘periodic’, ‘renewal’ or ‘restoration’.
Application Period	When applicable, the period to be considered by the CAB for the assessment of operational effectiveness.
Application Number	The registration number assigned to the Application document upon receipt by the CAB
Mandatory field in the template	Clarification

<p>Section 2: “SCS Claim”</p> <p>This section is the SCS’s management assertion the template accurately and fairly describes the SCS and the applicable controls from the scheme’s framework.</p> <p>From the Application document</p>	
<p>Section 3: “SCS’s Description of its service”</p> <p>This section is the SCS-P’s assessment of the Supply Chain Service’s implementation of the scheme’s requirements and control framework.</p>	
Description	From the application document
Self-Assessment	Assessment of the conformity to EUSCS requirements (Basic assurance level only)
<p>Section 4:” Assessor Responsibility Assertion”</p> <p>This section is the assessor’s management assertion about their responsibility.</p>	
Responsibility	Statement from the assessor
Scope	Scope of the audit (including references to the SCS-P’s description and to the assessor’s activities)
Disclaimers	Standard disclaimers about the audit activities
<p>Section 5: “CAB’s Audit Activities and Results”</p> <p>This section describes the CAB’s audit activities and results.</p>	
4,1 Presentation	
4.2 Audit activities and results	
Reasonable assurance	Description and results of the audit activities (version for the Substantial and High levels)
Limited assurance	Description and results of the audit activities (version for the Basic level)
4.3 Nonconformities	
Requirement reference	Reference of the EUSCS security objective and requirement for which a nonconformity has been identified
Nonconformity	Description of the nonconformity
Severity	The severity of the nonconformity, which may be ‘minor’ or ‘major’
Suitability of mitigation	The analysis of the mitigation proposed by the SCS-P
<p>Section 6: “assessor’s conclusion”</p> <p>This section describes the conclusion of the C assessor’s audit regarding the suitability of the supply chain service for certification</p>	

Conclusion	Conclusion about the fulfillment of EUSCS requirements by the supply chain service
Disclaimer	A disclaimer indicating that the conclusion needs to be combined with the conclusion of the evaluation report.

CONTENT OF THE DOCUMENT

F.4.1.1 *Identification*

Identification of the assessor

< assessor IDENTITY >

The legal identity of the organisation issuing the report shall be provided, including at least:

Legal name of the organization;

Registration number in Chamber of Commerce or equivalent; and

Office and headquarter location;

If the organization operates as a subcontractor for another assessor that will issue the certificate, the same information shall be provided about that other CAB.

< Assessor CONTACT >

The contact details of the responsible department and of the person that is legally representing the organization for the purpose of that audit shall be provided

< ACCREDITATION DETAILS >

The assessor in charge of the conformity assessment shall include the information related to its ability to perform an audit:

Accreditation number and notification number and contact details of issuing body;

If assurance level High is applicable, and Article 56(6) applies, a signed statement of the NCCA authorizing the CAB to perform the conformity assessment;

If the organisation issuing the report is a subcontractor of the CAB and has obtained a separate accreditation to perform audit work, then they shall provide the following information:

Accreditation number and notification number;

< LEAD AUDITOR >

The affiliation, contact information and qualification of the lead auditor shall be provided.

< AUDIT TEAM >

The affiliation, contact information, role and qualification of every member of the audit team shall be provided.

Identification of the SCS-P

<SCS IDENTITY>

This item shall include the content of the <SCS IDENTITY> item from the Application Document.

<SCS CONTACT>

This item shall include the content of the <SCS-P CONTACT> item from the Application Document.

Identification of the supply chain service

<SERVICE NAME>

This item shall include the content of the <SERVICE NAME> item from the Application Document.

<SHORT DESCRIPTION>

This item shall include the content of the <SHORT DESCRIPTION> item from the Application Document.

<ASSURANCE LEVEL>

This item shall include the content of the <ASSURANCE LEVEL> item from the Application Document.

<SECURITY PROFILES>

This item shall include the content of the <SECURITY PROFILES> item from the Application Document.

<APPLICATION TYPE>

This item shall include the content of the <APPLICATION TYPE> item from the Application Document.

<APPLICATION PERIOD>

This item shall include the content of the <APPLICATION PERIOD> item from the Application Document.

<APPLICATION NUMBER>

This item shall contain the application number issued by the CAB upon reception of the Application Document.

F.4.1.2 SCS's claim

This section shall contain the SCS's claim from the Application Document.

F.4.1.3 SCS description

This section contains the information about the supply chain service.

<DESCRIPTION>

The description of the service provided in the Application Document.

<SELF-ASSESSMENT>

This item is only relevant for assurance level Basic.

This item shall include the self-assessment provided by the SCS-P following the template provided by the CAB.

F.4.1.4 Assessor *responsibility assertion*

This section is the assessor's assertion of their responsibility and to its compliance to the scheme, which shall be dated and signed.

<RESPONSIBILITY>

The assessor in charge of the conformity assessment shall include the information related to its responsibility in the audit:

- A declaration of independence and quality control; and
- A declaration of protection of information (confidentiality obligations and IP obligations).

If the organisation issuing the report is a subcontractor of the assessor, then they shall provide the following information:

- A declaration of independence and quality control; and
- A declaration of protection of information (confidentiality obligations and IP obligations).

In all cases, the organisation issuing the report shall also include a declaration of evaluation according to the applicable rules, stating that the conformity assessment activities described in the report were performed in accordance with the requirements of the EUCSA, of the EUSCS scheme and, if applicable, to authorisation requirements defined by the NCCA.

<SCOPE>

Based on the information provided earlier in the document, a short statement of what has been evaluated shall be provided:

Overview of the reviewed documentation,

List of on-site visits;

Overview of the testing performed; and

List of persons interviewed.

The definition of the scope shall be a short summary, without the details provided in the description of the assessor audit activities.

<DISCLAIMERS>

The assurance report shall include disclaimers that convey the information that:

No certification can lead to a 100% security guarantee, but only to a reasonable certainty that the level of security is meeting the requirements for the assurance level at the moment of certification and during the certification lifecycle;

Security controls are evaluated to the best of abilities, required skills and knowledge of the evaluating parties; and

There is no guarantee that certification excludes all forms of fraud, misleading or circumvention of controls but the EUSCS scheme is aiming to prevent such fraudulent behaviour as much as possible.

F.4.1.5 Assessor’s *audit activities and results*

Presentation

<PRESENTATION>

This item is optional. The assessor may include a presentation of the audit activities.

Audit activities and results

This section shall contain one of the two subsections listed below, depending on the assurance level of the conformity assessment.

F.4.1.6 Assurance

The assessor shall provide the following table, which presents the assessor’s test procedures and results per control. The number and depth of the testing will depend upon the assurance level.

<SCS-P>’s Description of Controls	Applicable EUSCS requirements	<Assessor’s Audit Activities and Results
ID – Title of Control [Control Description]	Ref. 1 Ref. 2 Ref. 3	Inquired the [...] <i>No nonconformities identified</i> Inspected [...] <i>No nonconformities identified</i>
ID – Title of Control [Control Description]	Ref. 1 Ref. 2 Ref. 3	Inquired the [...] <i>No nonconformities identified</i> Inspected [...] <i>No nonconformities identified</i>

Note that the example provided above indicates “No nonconformities identified”. In case a nonconformity is identified, it shall be noted, with a reference to the nonconformity’s description in the following section.

Nonconformities

This section shall list all the nonconformities identified during the audit, including a summary of the analysis of the analysis performed by the assessor of the nonconformity and of the mitigation proposed by the SCS-P.

<REQUIREMENT REFERENCE>

This item shall include a reference to the objectives and requirements that are not being fulfilled.

<NONCONFORMITY>

This item shall include a description of the nonconformity.

In the case of multiple non-conformities related to the same requirement, the description shall include enough information to support the analysis of the nonconformity's severity.

<SEVERITY>

This item shall include a summary of the analysis performed by the assessor to determine the severity of the nonconformity, as well as the conclusion (minor or major nonconformity).

<SUITABILITY OF MITIGATION>

This item shall include a summary of the analysis performed by the assessor to determine the suitability of the mitigation proposed by the SCS-P.

For a minor nonconformity, a simple analysis of the proposed mitigation actions or compensating controls is sufficient. For a major non-conformity, the mitigations shall be implemented, and the analysis shall point to audit activities that verifies the success of the mitigation.

Note that the mitigation of a major non-conformity is considered successful is it leads to no nonconformity or to a minor non-conformity. In the case of a minor nonconformity, it is also listed in the section.

F.4.1.8 assessor's **conclusion**

This section is the conclusion about the fulfilment of EUSCS requirements by the supply chain service, to the extent determined by the audit, which shall be dated and signed by the lead auditor.

<CONCLUSION>

This is the conclusion of the lead auditor regarding the audit.

The conclusion can only be partial, since it will depend on the dependency analysis. More details need to be added.

<DISCLAIMERS>

TO BE DEFINED

A disclaimer will need to be added to indicate that the fulfilment of the EUSCS requirements also depend on the dependency analysis, to be performed independently.

F.4.2 Evaluation report

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the "Evaluation report" document.

A assessor shall apply these requirements when preparing the report at the end of the audit of the SCS.

Mandatory field in the template	Clarification
<p>Section 1: “Identification”</p> <p>This section identifies the conformity assessment body in charge of the certification, the audit team in charge of the assurance report, and the SCS being audited.</p> <p>Same as for the Assurance Report</p>	
<p>Section 2: “SCS-P Claim”</p> <p>This section is the SCS-P’s management assertion the template accurately and fairly describes the Supply Chain Service and the applicable controls from the scheme’s framework.</p> <p>From the Application document</p>	
<p>Section 3: “SCS-P’s Description of its service’s dependencies”</p> <p>This section is the SCS-P’s assessment of the supply chain service’s dependencies towards subservice organizations, together with a list of the available assurance documentation for these services.</p>	
Description	From the application document
Self-Assessment	Assessment of the conformity to EUSCS requirements (Basic assurance level only)
<p>Section 4: “ASSESSOR’s Responsibility Assertion”</p> <p>This section is the ASSESSOR’s management assertion about their responsibility.</p> <p>Same as for the Assurance Report</p>	
<p>Section 5: “ASSESSOR’s Dependency Analysis Activities and Results”</p> <p>This section describes the CAB’s dependency analysis activities and results.</p>	
5,1 Presentation	An optional presentation of the activities
5.2 Activities and results	
Reasonable assurance	Description and results of the audit activities (version for the Substantial and High levels)
- Assurance documentation	Verification of the suitability of the nature of documentation available, of the framework used, of the conclusions, and other relevant criteria
- Documentation origin	Verification of the origin of the documentation guarantees about competence and independence
- Scoping	Verification of the scope of the documentation with respect to the scope expected by the SCS-P (covering both dimensions: functionality and security requirements)
- Nonconformities	Analysis of the nonconformities indicated in the assurance documentation that may affect the decision

- Analysis	Combined analysis of all the results regarding the subservice provider
Limited assurance	Description and results of the audit activities (version for the Basic level)
5.3 Nonconformities	
Requirement reference	Reference of the requirement that is not being fulfilled
Nonconformity	Description of the nonconformity
Severity	Severity of the nonconformity
Suitability of mitigation	Overview of the proposed mitigation and of its suitability to address the nonconformity
Mandatory field in the template	Clarification
Section 6: “ASSESSOR’s conclusion”	
This section describes the conclusion of the CAB’s audit regarding the suitability of the supply chain service for certification	
Dependency Conclusion	The conclusion of the dependency analysis
Recommendation	Combined conclusion of audit and dependency analysis and recommendation for the certification decision

CONTENT OF THE DOCUMENT

F.4.2.1 *Identification*

This section has the same content as the one described in the Assurance Report (F.4.1.1)

F.4.2.2 *SCS-P’s claim*

This section shall contain the SCS-P’s claim from the Application Document.

F.4.2.3 *SCS-P’s description of its service’s dependencies*

<DESCRIPTION>

This item shall contain the content of the <SUB SERVICES> item from the Application Document (F.2.3.4).

<Self-Assessment>

This item is only relevant for assurance level Basic. This item shall include the self-assessment provided by the SCS-P following the template provided by the assessor for assessing the adequacy of the assurance documentation available and the sufficiency of the controls covered by that assurance documentation.

F.4.2.4 *assessor’s responsibility assertion*

This section has the same content as the one described in the Assurance Report (F.4.1.4)

F.4.2.5 assessor's *dependency analysis activities and results*

Presentation

<PRESENTATION>

This item is optional. The CAB may include a presentation of the audit activities.

Audit activities and results

This section shall contain one of the two subsections listed below, depending on the assurance level of the conformity assessment.

LIMITED ASSURANCE

This section only applies to assurance level Basic.

This section is to be defined.

REASONABLE ASSURANCE

This section only applies to AL Substantial and High.

The assessor shall provide the following information, which presents the CAB's dependency analysis activities and results.

The items below need to be replicated for every subservice provider.

<ASSURANCE DOCUMENTATION>

This item shall include a description of the nature of the documentation followed by an analysis of its suitability. The following elements shall be considered:

Nature of the documentation (ISAE report, certificate, other) and type (ISAE report type, certification scheme);

Period covered, certificate validity;

Applicable framework and availability/sufficiency of mapping to EUCS requirements;

Sufficiency of the report for understanding the subservice organization's controls.

If the assurance documentation is an EUSCS certificate, then checks are only required of the certificate validity and of the assurance level.

More information about acceptable reports and certificates and specific attention points for every type of report will be provided as guidance.

<Documentation Origin>

This item shall include a description of the organization who issued the report or certificate, followed by an analysis of its suitability. The following elements shall be considered:

- Identity of the issuing organization and, if required of the lead auditor;
- Competence of the issuing organization and lead auditor (accreditation, personal certification);

- Independence of the issuing organization and lead auditor (accreditation, other indication) If the assurance documentation is an EUSCS certificate, then no checks are required.

<SCOPING>

This item shall include a description of the scope of the assurance documentation, followed by an analysis of its suitability with regard to the requirements (e.g. EUSCS requirements) described by the SCS-P. The following elements shall be considered:

- Systems and locations in scope that are relevant for the SCS-P;
- Applications and services that are relevant to the SCS-P;
- Carved-out components and other subservice providers;
- Sufficiency of the scope to cover the requirements of the SCS-P, including CSOCs.
- If the assurance documentation is an EUSCS certificate, then subservice providers do not need to be identified.

<NONCONFORMITIES>

This item shall include a description of the nonconformities identified in the assurance documentation, followed by an analysis of their impact. The following elements shall be considered:

- Nonconformities or deviations identified in the assurance documentation that may affect the SCS-P;
- Severity or qualification of the nonconformities or deviations;
- Description of proposed mitigation and opinion of the auditor.

<ANALYSIS>

This item shall include an analysis that considers together all the activities described above in order to reach a conclusion about the suitability and sufficiency of the assurance documentation available for the subservice provider.

Nonconformities

This section shall list all the nonconformities identified during the audit, including a summary of the analysis of the analysis performed by the CAB of the nonconformity and of the mitigation proposed by the SCS-P.

<REQUIREMENT REFERENCE>

This item shall include a reference to the objectives and requirements that are not being fulfilled.

This item may refer to an EUSCS requirement or to a CSOC defined by the SCS-P.

<NONCONFORMITY>

This item shall include a description of the nonconformity.

In the case of multiple nonconformities related to the same requirement, the description shall include enough information to support the analysis of the nonconformity's severity.

The nonconformity is not necessarily linked to a nonconformity identified in assurance documentation, as it may relate to any part of the dependency analysis.

<SEVERITY>

This item shall include a summary of the analysis performed by the CAB to determine the severity of the nonconformity, as well as the conclusion (minor or major nonconformity).

<SUITABILITY OF MITIGATION>

This item shall include a summary of the analysis performed by the CAB to determine the suitability of the mitigation proposed by the SCS-P.

For a minor non-conformity, a simple analysis of the proposed mitigation actions or compensating controls is sufficient. For a major non-conformity, the mitigations shall be implemented, and the analysis shall point to audit activities that verifies the success of the mitigation.

Note that the mitigation of a major non-conformity is considered successful if it leads to no nonconformity or to a minor non-conformity. In the case of a minor non-conformity, it is also listed in the section.

F.4.2.6 Assessor's **conclusion**

This section is the conclusion about the fulfilment of EUSCS requirements by the supply chain service, to the extent determined by the audit, which shall be dated and signed by the lead auditor.

<DEPENDENCY CONCLUSION>

This is the conclusion of the lead auditor regarding the dependency analysis, considering all subservice providers.

<RECOMMENDATION>

This item shall include the final recommendation of the auditor, based on the conclusion of the Assurance Report and the conclusion of the dependency analysis. The auditor shall determine whether or not the supply chain service meets the EUSCS requirements for the targeted assurance level, and shall provide a recommendation regarding the certification of the supply chain service.

The recommendation shall be dated and signed by the lead auditor.

F.5 REVIEW REPORT

This is an internal document, generated during the review phase, in which the reviewer records the result of its review of the audit.

A template will be provided later for guidance.

F.6 CERTIFICATE PACKAGE

F.6.1 **Certificate**

The template of SCS certificates need to be defined after the approval of the SCS scheme.

F.6.2 **Certification report**

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Evaluation report” document.

An assessor shall apply these requirements when preparing the certification report that accompanies the certificate.

Mandatory field in the template	Clarification
<p>Section 1: “Independent Conformity Assessment Body report” This section confirms the evaluation work done by the assessor.</p>	
Scope	Description of the scope of the evaluation
SCS-P Management Responsibilities	Description by the an assessor of the SCS-P’s management responsibilities in the evaluation
CAB responsibilities	Description by the assessor of the assessor ’s responsibilities in the evaluation and of the inherent limitations of the evaluation
Certification decision	Description by the CAB of the outcome of the evaluation, which led to the positive certification decision
<p>Section 2: “Management’s report”</p> <p>This section is the SCS-P’s management confirmation of its responsibilities and assertion of the effectiveness of the implemented controls in relation to the EUSCS scheme’s requirements.</p>	
SCS-P Management Statement	A written conformity statement by the management of the SCS-P
<p>Section 3: “SCS scope”</p> <p>This section is the SCS-P’s assessment of the supply chain service’s implementation of the scheme’s requirements.</p>	
Background	Information on the SCS-P as an organization
Supply Chain service	The supply chain service in scope for the evaluation, including the commercial names used for the supply chain service.
Service components	A list of the main components of the supply chain service
<p>Section 4: “Principle Service Commitments and System Requirements” Description of the supply chain service, the SCS-P commitments and requirements.</p>	
Description	General description provided by the SP of its approach to cybersecurity assurance and compliance to the scheme
a) Physical Infrastructure	Description of physical structures at the SCS-P that make up the supply chain service.
b) People	Description of (types of) personnel at the SCS-P involved in the governance and operation of the supply chain service

c) Procedures	Description of automated and manual procedures at the SCS-P involved in the governance and operation of the supply chain service
Mandatory field in the template	Clarification
d) Data	Description of the data involved in the governance, operation, and use of the supply chain service.
e) Confidentiality	Description by the SCS-P of the measures that support confidentiality in relation to the supply chain service
f) Integrity	Description by the SCS-P of the measures that support integrity in relation to the supply chain service
g) Availability	Description by the SCS-P of the measures that support availability in relation to the supply chain service
Section 5: “ Additional information ”	
This section includes the information required as to be transparent in the part of the EUSCS scheme.	
Supplementary information	The information that has to be made available by the Cybersecurity Act’s article 55
Location and legal information	Information about the location of the storage and processing of customer data, and about applicable laws.

CONTENT OF THE DOCUMENT

F.6.2.1 *Independent Conformity Assessment Report*

<SCOPE>

This item shall contain a description of the scope of the evaluation, including at least:

The targeted assurance level

If applicable, the list of claimed security profiles

A high-level description of the certified supply chain service

<SCS-P MANAGEMENT RESPONSIBILITIES>

This item shall contain a description of the assessor’s understanding of the SCS-P’s responsibilities, drawn from the SCS-P management’s statement including in the Application Document.

< Assessor’s RESPONSIBILITIES>

This item shall contain a description of the assessor’s own responsibilities, matching the statement provided in the other reports, and in particular in the Assurance Report and Evaluation Report.

<CERTIFICATION DECISION>

This item shall contain a description of the assessor’s certification decision, including at least

A statement about how an assessor has verified that the supply chain service meets the EUSCS scheme's requirements

An overview of the subservices and how they have been considered to contribute meeting the EUSCS scheme's requirements

An overview of the nonconformities and how the proposed mitigations have been determined appropriate

F.6.2.2 **Management's report**

<SCS-P MANAGEMENT STATEMENT>

This item shall contain a SCS-P management statement drawn from the statement provided in the Application Document.

F.6.2.3 **Supply Chain service scope**

<BACKGROUND>

This item shall contain information about the SCS-P as an organization and their commitment to cybersecurity.

<SUPPLY CHAIN SERVICE>

This item shall include an overview of the supply chain service that is in scope for the certification, including the commercial names and the corresponding functions.

<SERVICE COMPONENTS>

This item shall include a description of the main components used for the development and operation of the supply chain service.

F.6.2.4 **Principle service commitments and system requirements**

<DESCRIPTION>

This item shall include a general description provided by the SCS-P of its approach to cybersecurity assurance and compliance to the requirements of the EUSCS scheme.

<PHYSICAL INFRASTRUCTURE>

This item shall include a description of the physical structures at the SCS-P that are used to develop, provide and support the supply chain service.

<PEOPLE>

The item shall include a description of the personnel (categories) and key roles at the SCS-P who are involved in the development, governance and provision of the supply chain service.

<PROCEDURES>

This item shall include a description of the automated and manual procedures at the SCS-P that are involved in the development, governance and provision of the supply chain service.

<DATA>

This item shall include a description of the data involved in the governance, operation and use of the supply chain service.

<CONFIDENTIALITY>

This item shall include a description of the measures implemented by the SCS-P to support confidentiality in relation to the supply chain service.

<INTEGRITY>

This item shall include a description of the measures implemented by the SCS-P to support integrity in relation to the supply chain service.

<AVAILABILITY>

This item shall include a description of the measures implemented by the SCS-P to support availability in relation to the supply chain service.

F.6.2.5 Other information

This section is optional.

<OTHER INFORMATION>

If present, this item shall include additional information that the SCS-P considers relevant in context of the certification of its supply chain service.

Note that the information provide in this section needs to be accepted and reviewed by the CAB, like all information in the report.

F.7 MAINTENANCE REPORTS

F.7.1 Impact analysis report

In some cases, the monitoring activities will lead to requests regarding potential nonconformities or vulnerabilities that will not lead to a conformity assessment. This report would outline the answer from the SP and the analysis from the CAB.

F.7.2 Maintenance report

The need for a maintenance report is still under discussion. A maintenance report would be a version of the certification report tailored for maintenance assessments. In particular, it would focus on the changes since the last report, to make the crucial information more easily accessible to scheme users.

Appendix G – Initial Application of SCS scheme

Engaging on a more practical view of the EUSCS, an initial example scenario and the applicability of it in a modern real-world use case will be described, following the present steps and processes that an assessor and the audited organization have to consider. This example will replicate the processes of scheme application in a Vehicle Transport Supply Chain (VTS) by following the methodologies described into the Sections/Appendixes. The steps of constructing this example will be to:

- Replicate the processes, identify devices and services for VTS originally described in D2.1,
- Use the EUSCS and conduct the conformity assurance at a Basic Level of Assurance and,
- Specify the objectives in accordance with the requirements for VTS.

Considering the Appendix A- Level Basic of Assurance, there is a preparatory step of accepting the conformity Assessment Engagement. Before agreeing to accept or continue a conformity assessment engagement, the CAB shall determine whether the application request is appropriate by providing a review of the VTS application.

This review is performed in order to assess the applicability of the criteria as described in the scheme, including the decision whether the chosen assurance level is appropriate for the circumstances, and to ensure that the application complies with all the aspects defined.

In this example section we are taking as a standard that the VTS Supply Chain has the availability on resources to perform assessments, that all the review criteria are fulfilled and also the legal binding declarations are decided and met by both the CAB and the SCP.

In wide terms auditor responsibilities revolve around the:

- Development of an audit plan
- Execution of assessment procedures
- Analysis of the assessment's results
- Issuance of assurance and certification report

In the other hand CAB is responsible for:

- Reviewing the evaluation that CAB provides
- Certification decision
- Issue Certification

In the example that we are focusing on, we examine in particular the SCS-TOE II (Holistic Technical View) in the VTS as an assessment body for providing a Technical Asset interdependent view of the VTS SC. This TOE was decided to be evaluated due to the more technical approach that it has with regards to other TOES that are more business oriented. Also, this example is not meant to focus on details, therefore, it revolves around a part of the VTS. TOE II contains SCS processes, different business partners, data and all SCS assets that participate for the provision of the entire VTS SC.

As described in the ENISA’s EUCS and as a result of our proposed scheme, auditors’ main responsibility is to obtain the understanding and the controls of the SC service from SCP’s description as well as identify the boundaries of that system and how it interfaces with other systems and evaluate if it is fairly presented. As an addition there is a need of reviewing the SCP’s mapping between the Security Objectives that the schema introduces and related Security Requirements that have been introduced by the SCP.

For this particular step we will examine the most technical category that is introduced in VTS TOE II as well as the two basic sub processes. These processes contain Business Partners (Port Authority, Ship agent, Terminal Operator etc.) in which of these business partners we have a set of components and assets that interrelate with each other.

In particular, we examine the “Pre-arrival Phase Category” and its sub processes:

- C.1 Port Call Request sub process with BP:
 - Port Authority, Ship Agent, Terminal Operator, Customs
- C.2 Standard Cargo Manifest sub process with BP:
 - Port Authority, Ship Agent, Customs

For the processes given, the auditor must study the TOE Requirements and map them with the Security Objectives of the EUSCS, providing a review report as in Table below. This report contains the mapping of the objectives with the requirements from TOE, including the Objective categories and a Labelling that inquires of the assurance level for each requirement that is presented.

Table 7: Example Review Report from Assessor

Categories	Objectives	Requirements from TOE	Label
Human Resources (HR)	HR-06.1	TOE_II_CA_4 Ensure confidentiality of the communication through the different channels.	Basic
Operational Security (OPS)	OPS-13.3	ToE_II_CA_3 Ensure data privacy in all the communication with external systems following the European and National legislation	Basic
Authentication mechanisms (IAM)	IAM-07	TOE_II_CA_6 Ensure the authenticity of the involved actors avoiding identity fraud	Basic
Portability and Interoperability(PI)	PI-02.1	TOE_II_CA_9	Basic

		Assign a Business Agreement between the involved supply chain parties with an embedded Security Declaration statement	
--	--	---	--

This process is essential due to the fact that the assessor now can identify extra remaining risks that are not included inside the TOE and highlight the importance of them to the SCP. In CYRENE report 3, a detailed directive, showing an automated solution of this evaluation from the assessor regarding the requirements, will be introduced.

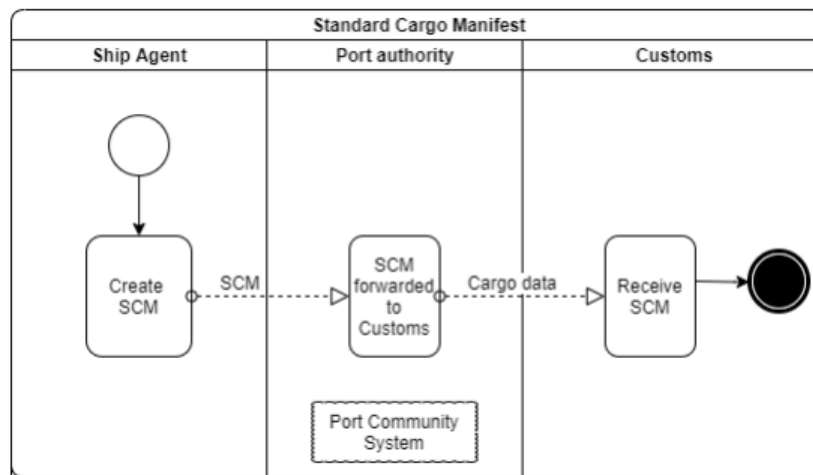


Figure 5: Standard Cargo Manifest sub-process

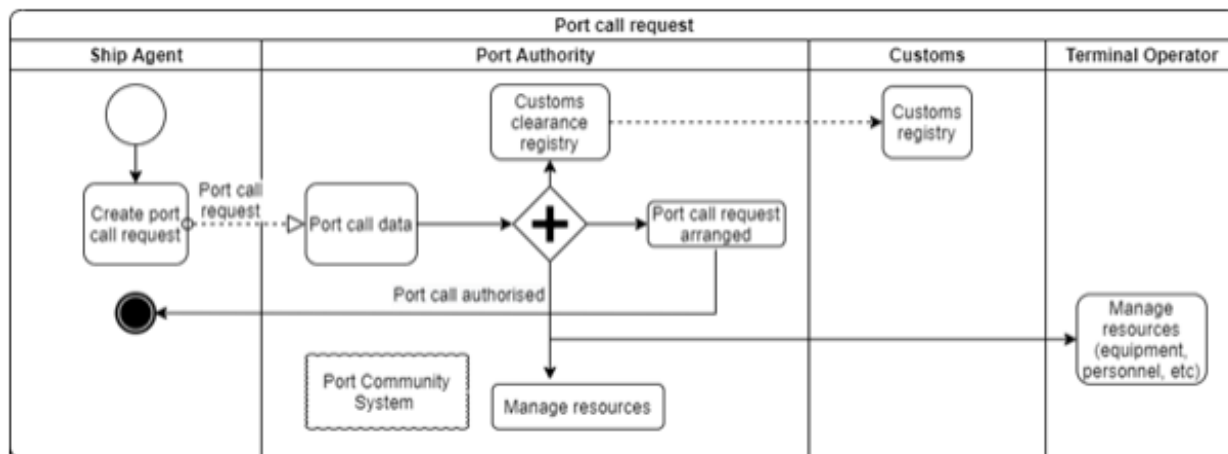


Figure 6: Port call Request

Next step for the assessor, is to decide to what extent and for which processes the SCP uses sub service providers and how these services provide their capabilities. That is made clear in order to determine which assessment approach is appropriate and to identify if a sub-service contains already an acceptable assurance report which can be used. So if for the Ship Agent Business Partner in the Pre-arrival Phase Category, is already assessed in a basic level, and the functionality on the 2 different processes (Figure 5: Standard

Cargo Manifest, Figure 6: Post Call Request) is the same, we can highlight the other Business partners that are involved in that process. In our case the Ship Agent Business Partner, is involved and has the same role in both sub-processes.

The questions that must be answered by the assessor in that step are:

- Does the description includes significant aspects of SC?
- Description omits relevant information?

These questions revolve around the importance and effect of possible omissions or deviations that the description for the processes provided might have.

After validating the description, map the TOEs and deciding upon its fulfilment state, assessor must decide for the quality of the objective evidence that are gathered. If they are Sufficient and appropriate objective evidence about the design and implementation of the SCP’s internal controls the assessor provides the self-assessment and audit plans. Execution phase starts when the SCP provides the results of their self-assessment, together with all required supporting documentation.

Port Authority	<p>The Port Authority manages the PCS, an open and neutral electronic platform, that allows a safe and smart information exchange between public and private agents in order to improve the competitive position in the port. The is composed of the following elements of software and hardware:</p> <p>(a) All PCS systems are hosted on a server HPE ProLiant DL580 Gen10. It has a recovery site with all the systems replicated, to ensure the availability.</p> <p>(b) A router Extreme Networks SLX 9640 that allows the interconnection of LAN networks and provide access to the system.</p> <p>(c) The operating system on the server is a Windows Server 2019 developed by Microsoft with extended security.</p> <p>(d) To store the data about all the actors involved in the activity and data produced, it has a relational database Microsoft SQL server 2019.</p> <p>(e) The PCS has a web application deployed on a web server IIS 10. This allows access to all information and documents available and provide the necessary documents.</p> <p>(f) The PCS has its own mail domain that allows direct communication with the users. It uses the SMTP server of Microsoft, Exchange Server 2019.</p> <p>(g) There is an FTP Server for file transferring and data interchange via PCS. The FTP Server supports the following three web services; Message Processor Service, Movement Retrieval Service, Data Movement Retrieval Service.</p> <p>(h) To ensure the security and integrity of the entire system has been installed on the server an antivirus Symantec.</p>
-----------------------	---

Figure 7: Port Authority Asset Description

A control is suitably designed when actions or events that comprise a risk are prevented and corrected. For our case, thus in the basic assurance level, any vulnerability assessment procedure will be performed on the devices involved in aforementioned processes to issue the self-assessment report. As described in D2.1

these devices are translated into assets, so for the port authority, assets that will be subdued to an assessment for the Port Call authority and in particular for the Port Authority Business Partner are described in Figure 7: Port Authority Asset Description.

It is important to pinpoint Obtaining evidence regarding the suitability of the design of controls. This requires the auditor to determine whether

1. The risks that threaten the achievement of the Security Control Objectives and related Security Requirements as defined by the EUSCS have been identified by management;
2. The controls are able to prevent or detect Security Control Objectives and related Security Requirements of the EUSCS from not being met.

Assessors, must draw conclusions, evaluating and considering that the information provided is relevant, reliable, and suitable to meet security Control objectives and following security policies. On this basis the auditor assess must come to a conclusion that nothing has come to its attention that causes the reviewer to believe that the technical and organizational manners warranted by the SCP are not meeting in all material aspects the requirements of the Basic level in accordance with the Certification framework and that the evidence presented is at least sufficient for the reviewer to obtain the level of assurance.

Table 8: Draft Assurance report

Security Control Objectives	VTS's description of Controls	Documentary evidence used or means of evidence	Test Results
Objective: Logging and monitoring			
ToE_II_CA_3	Port Call Request process	Description of the evidence	Result
TOE_II_CA_6	Standard Cargo Manifest	Description of the evidence	Result

After evaluating the result of the audit procedures, the auditor shall form a conclusion and issue an evaluation report stating that nothing negative has come to the reviewer's attention. Assessor then has to issue a report using a certain template provided by our scheme. A draft of this report is shown in Table 7: Draft Assurance report.

Appendix H – Glossary

This section contains the glossary of this report. The current glossary is an excerpt of the online glossary available and continuously updated on the CYRENE project website⁶. 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, 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 from terms referring to security and certification concepts that are considered important in the context of the proposed EUSCS. 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”⁷ 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.

Table 9 – Extracted from Supply Chain and Business Concepts CYRENE online glossary

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		

⁶ <https://www.cyrene.eu/glossary/>

⁷ <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

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 the current 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 the current 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.		

<p>SCS Business Partner</p>	<p>SCS-BP</p>	<p>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".</p>	<p>1. ISO 28001:2007 2. EU H2020-ICT-02-2020 project "CYRENE"</p>		<p>CYRENE delves into a service approach definition, whereas ISO 28001 defines it from a supply chain perspective.</p>
<p>SCS provider</p>	<p>SCS-P</p>	<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).</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>	<p>in the vehicle transport SCS, the automotive industry and all its third parties/sub-contractors belong in this type.</p>	<p>(Business Partner A)</p>
<p>SCS Commercial Business Partner</p>	<p>-</p>	<p>Participating in the provision of the supply chain service, undertaking an operational role, related to the operation of the supply chain service, including ordering, transporting, importing, and other processes.</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>	<p>in the vehicle transport SCS, the importers, transport/maritime companies and any third-party commercial partner reflect this category.</p>	<p>(Business Partner B)</p>
<p>SCS Governmental Business Partner</p>	<p>-</p>	<p>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.</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>	<p>in the vehicle transport SCS, the Ministry of Transport, Customs and other related authorities fall in this category.</p>	<p>(Business Partner C)</p>

<p>SCS Self-Assessor</p>	<p>-</p>	<p>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).</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>		<p>(Business Partner D)</p>
<p>SCS Assessor</p>	<p>-</p>	<p>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).</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>		
<p>Mutual Recognition Agreement</p>	<p>SCS-MRA</p>	<p>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.</p>	<p>EU H2020-ICT-02-2020 project "CYRENE": EUSCS, CYRENE RCA Methodology</p>		

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 utilised 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 10 – Certification and Security Concepts of the updated CYRENE online glossary

Term	Abbreviation	Definition(s)	Reference	Example(s)	Notes/ Remarks
Security Concepts					
Confidentiality	-	Property that information is not made available or disclosed to unauthorised 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 authorised 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		
Vulnerability	-	<p>1. Weakness in the TOE that can be used to violate the SFRs in some environment.</p> <p>2. Weakness of an asset or control that can be exploited by one or more threats.</p> <p>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),</p> <p>2. ISO/IEC 27000:2018,</p> <p>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).</p> <p>- Multiple vulnerabilities can impact a supply chain as a whole, compromising multiple inteconnected 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>
-Potential (unknown) Vulnerability	-	<p>1. Potential: Suspected, but not confirmed, weakness</p> <p>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),</p> <p>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.</p> <p>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>

-Confirmed Vulnerability	-	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.	CVSS v3.1 NIST NVD (FIRST)	A confirmed vulnerability example is the vulnerability of Microsoft Teams Remote Code Execution, which was published on 11/11/2020.	
-Exploitable Vulnerability	-	Weakness in the TOE <i>that can be used to violate the SFRs in the operational environment</i> for the TOE.	ISO/IEC 15408-1:2009 (CC)		
-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/La belling	-	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	

<p>Vulnerability Severity Level</p>	<p>VSL</p>	<p>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.</p>	<p>1. CVSS v3.1, 2. EU H2020-ICT-02-2020 project “CYRENE”: CYRENE RCA Methodology</p>		
<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 authorised 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 utilised 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>
<p>Common Vulnerability Scoring System</p>	<p>CVSS</p>	<p>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.</p>	<p>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</p>	<p>For instance, the confirmed vulnerability "CVE-2020-17091" Microsoft Teams Remote Code Execution has <i>Basic score metrics= 7.8</i> : Exploitability<AV= Local/AC=Low PR=None / UI=Required <i>Impact<C= High I=High A=High Temporal score metrics = 6.8</i> : E= Unproven RL=Official fix RC=Confirmed</p>	<p>(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 recognised as an international standard for scoring vulnerabilities.</p>
<p>Vulnerability Chain</p>		<p>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.</p>	<p>ANSI/API, 2013</p>		

<p>Attacker (adversary/ threat agent)</p>	<p>-</p>	<p>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].</p>	<p>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</p>	<p>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.</p>	
<p>Attack</p>	<p>-</p>	<p>Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.</p>	<p>ISO/IEC 27000:2018</p>	<p>Attack on a SCADA software (cyber), attack on a cruise terminal (physical).</p>	
<p>Cyber attack</p>	<p>-</p>	<p>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.</p>	<p>NIST SP 800-30 Rev 1, 2012</p>	<p>Man-In the-Middle attack cinderella attack ransomware attack</p>	
<p>Attack path (attack model/attack pattern/attack vector)</p>	<p>-</p>	<p>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 utilised 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].</p>	<p>1. API standard 780, 2. ISO/IEC TR 20004:2015, 3. ISO/IEC 27032:2012</p>	<p>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</p>	

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 unauthorised disclosure of information, unauthorised modification of information, unauthorised 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	-	1. Measure that maintains and/or modifies risk [ISO 31000: 2018; ISO/IEC 27000:2018]. 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]	1. ISO 31000: 2018 1.,2. ISO/IEC 27000:2018	Control – term used in [EUCSA, 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.” This term can be seen as equivalent to the Security Functional Requirements (SFRs) defined in ISO15408.	
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	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. 2. Coordinated activities to direct and control an organization with regard to risk.	1. ISO/IEC 27000:2018 2. ISO 31000:2018		
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 optimised 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					

<p>Conformity Assessment</p>	<p>CA</p>	<p>1. The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. 2. A procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled.</p>	<p>1. Regulation (EC) No 765/2008 2. Regulation (EU) 2019/881 (EU Cybersecurity Act)</p>	
<p>Conformity Self-assessment</p>	<p>-</p>	<p>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.</p>	<p>Regulation (EU) 2019/881 (EU Cybersecurity Act)</p>	
<p>Certification</p>	<p>-</p>	<p>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 activities, products and services, in line with the organization's policy and the requirements of the respective international management system standard.</p>	<p>ISO/IEC 17021-1:2015</p>	
<p>Certification scheme</p>	<p>-</p>	<p>Conformity assessment system related to management systems to which the same specified requirements, specific rules, and procedures apply.</p>	<p>ISO/IEC 17021-1:2015</p>	<p>EUCC, National schemes. (e.g. SOGIS-MRA, included NL (NLNCSA), FR (ANSSI), SE (FMV), DE (BSI)).</p>

Accreditation	-	Attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised 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		
Conformity Assessment Body	CAB	A body that performs conformity assessment activities including calibration, testing, certification and inspection	Regulation (EC) No 765/2008	One that: <ul style="list-style-type: none"> • Applies and assesses conformity to EU Cybersecurity Certification Scheme. • Certifies product conformity by a certification report. 	
Assurance Level		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	Regulation (EU) 2019/881 (EU Cybersecurity Act)		<ul style="list-style-type: none"> • Level 1: Little or no confidence; • Level 2: Some confidence; • Level 3: High confidence;

		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																																																																																																																																																																																																																																																
Evaluation Assurance Level	EAL	The definition of a scale for measuring assurance for component Targets of Evaluation (TOEs)	ISO/IEC 15408-3:2008 (CC)	<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>ENL1</th> <th>ENL2</th> <th>ENL3</th> <th>ENL4</th> <th>ENL5</th> <th>ENL6</th> <th>ENL7</th> </tr> </thead> <tbody> <tr> <td rowspan="6">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_SMP</td> <td></td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> </tr> <tr> <td>ADV_INT</td> <td></td> <td></td> <td></td> <td>2</td> <td>3</td> <td>3</td> <td>3</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_TSS</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>6</td> </tr> <tr> <td rowspan="3">Guidance documents</td> <td>ASD_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>ASD_PMB</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>ASD_OPC</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 rowspan="6">Life-cycle support</td> <td>ALC_OMS</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>ALC_OVS</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</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_LLD</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> </tr> <tr> <td>ALC_TST</td> <td></td> <td>1</td> <td>2</td> <td>3</td> <td>3</td> <td>3</td> <td>3</td> </tr> <tr> <td rowspan="6">Security Target evaluation</td> <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>ASE_ECD</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_INF</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_OBI</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_PFD</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_SPC</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="4">Tests</td> <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>2</td> <td>3</td> <td>3</td> </tr> <tr> <td>ATE_DPT</td> <td></td> <td></td> <td>1</td> <td>1</td> <td>3</td> <td>3</td> <td>4</td> </tr> <tr> <td>ATE_FLN</td> <td></td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>2</td> <td>2</td> </tr> <tr> <td rowspan="2">Vulnerability assessment</td> <td>AVA_INF</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>3</td> </tr> <tr> <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>Table 1 – Evaluation assurance level summary</p> <p><i>Assurance Levels (ISO/IEC 15408-3:2008 (CC))</i></p>	Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level							ENL1	ENL2	ENL3	ENL4	ENL5	ENL6	ENL7	Development	ADV_ARC	1	1	1	1	1	1	1	ADV_FSP	1	2	3	4	5	5	6	ADV_SMP			1	1	1	2	2	ADV_INT				2	3	3	3	ADV_SPM						1	1	ADV_TSS	1	2	3	4	5	6	6	Guidance documents	ASD_OPE	1	1	1	1	1	1	1	ASD_PMB	1	1	1	1	1	1	1	ASD_OPC	1	2	3	4	4	5	5	Life-cycle support	ALC_OMS	1	2	3	4	5	5	5	ALC_DEL		1	1	1	1	1	1	ALC_OVS		1	1	1	1	2	2	ALC_FLR								ALC_LLD		1	1	1	1	2	2	ALC_TST		1	2	3	3	3	3	Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1	ASE_ECD	1	1	1	1	1	1	1	ASE_INF	1	1	1	1	1	1	1	ASE_OBI	1	2	2	2	2	2	2	ASE_PFD	1	2	2	2	2	2	2	ASE_SPC	1	1	1	1	1	1	1	Tests	ASE_TSS	1	1	1	1	1	1	1	ATE_COV		1	2	2	2	3	3	ATE_DPT			1	1	3	3	4	ATE_FLN		1	1	1	1	2	2	Vulnerability assessment	AVA_INF	1	2	2	2	2	2	3	AVA_VAN	1	2	2	3	4	5	5
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level																																																																																																																																																																																																																																																
		ENL1	ENL2	ENL3	ENL4	ENL5	ENL6	ENL7																																																																																																																																																																																																																																										
Development	ADV_ARC	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ADV_FSP	1	2	3	4	5	5	6																																																																																																																																																																																																																																										
	ADV_SMP			1	1	1	2	2																																																																																																																																																																																																																																										
	ADV_INT				2	3	3	3																																																																																																																																																																																																																																										
	ADV_SPM						1	1																																																																																																																																																																																																																																										
	ADV_TSS	1	2	3	4	5	6	6																																																																																																																																																																																																																																										
Guidance documents	ASD_OPE	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ASD_PMB	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ASD_OPC	1	2	3	4	4	5	5																																																																																																																																																																																																																																										
Life-cycle support	ALC_OMS	1	2	3	4	5	5	5																																																																																																																																																																																																																																										
	ALC_DEL		1	1	1	1	1	1																																																																																																																																																																																																																																										
	ALC_OVS		1	1	1	1	2	2																																																																																																																																																																																																																																										
	ALC_FLR																																																																																																																																																																																																																																																	
	ALC_LLD		1	1	1	1	2	2																																																																																																																																																																																																																																										
	ALC_TST		1	2	3	3	3	3																																																																																																																																																																																																																																										
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ASE_ECD	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ASE_INF	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ASE_OBI	1	2	2	2	2	2	2																																																																																																																																																																																																																																										
	ASE_PFD	1	2	2	2	2	2	2																																																																																																																																																																																																																																										
	ASE_SPC	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
Tests	ASE_TSS	1	1	1	1	1	1	1																																																																																																																																																																																																																																										
	ATE_COV		1	2	2	2	3	3																																																																																																																																																																																																																																										
	ATE_DPT			1	1	3	3	4																																																																																																																																																																																																																																										
	ATE_FLN		1	1	1	1	2	2																																																																																																																																																																																																																																										
Vulnerability assessment	AVA_INF	1	2	2	2	2	2	3																																																																																																																																																																																																																																										
	AVA_VAN	1	2	2	3	4	5	5																																																																																																																																																																																																																																										
Vulnerability Analysis AVA_VAN	AVA_VAN	<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 with the authorised capabilities of other users.</p> <p>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.</p>	ISO/IEC 15408-3:2008 (CC)	<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); • 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		<p>1. Statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.</p> <p>2. Information security objective: Objectives that are set by the organization, consistent with the information security policy, to achieve specific results.</p>	<p>1. ISO/IEC 15408-1:2009 (CC) ,</p> <p>2. ISO/IEC 27000:2018</p>		<p>cf. EU Cybersecurity Act 2019/881 (Article 51) on Security objectives of European cybersecurity certification schemes</p>
Security Requirements	ASE_RE Q	<p>The security requirements consist of two groups of requirements:</p> <p>a) the security functional requirements (SFRs)</p> <p>b) the security assurance requirements (SARs)</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>		
Security Functional Requirements	SFR	<p>A translation of the security objectives for the TOE into a standardised language</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>		
Security Assurance Requirements	SAR	<p>A description of how assurance is to be gained that the TOE meets the SFRs</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>		
Security function	SF	<p>Function that implement the security requirements.</p>	<p>ISO/IEC 15408 - 2:2008 (CC)</p>		
Target of Evaluation	TOE	<p>A set of software, firmware, hardware and/or process possibly accompanied by guidance</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>	<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; • 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. 	<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> <p>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.</p>

<p>Protection Profile</p>	<p>PP</p>	<p>Implementation-independent statement of security needs for a TOE type.</p>	<p>ISO/IEC 15408-1:2009 (CC)</p>	<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>
----------------------------------	------------------	---	----------------------------------	--