D5.6 Preliminary certification activities

WP 5. Exploitation and dissemination plan including standardization activities

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 30/04/2019

Actual submission date: 30/04/2019

HORIZON 2020. WORK PROGRAMME 2014 – 2015			Project No	700378
Call			Instrument action	Innovation
Digital Security: Cybersecurity, Privacy and Trust			Start date	May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens			Duration	36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection			Website	www.cipsec.eu
Public	Confidential	Classified	Lead contractor	Atos Spain S.A.

The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The opinions expressed and arguments employed in this document do not necessarily reflect the official views of the Research Executive Agency (REA) or the European Commission.

This deliverable has been endorsed by Security Advisory Board.

Document contributors

Editor	**Comsec**	
Contributors		**Reviewers**
	AEGIS	
	ATOS	Antonio Álvarez
	BD	
Baruch Menahem, Yana Fesh	COMSEC	Haim Nachmias, Yael Chapal
	CSI	
	DB	
	EMP	
	FORTH	
	HCPB	
	TUD	
	UPC	
	UOP	Apostolos Fournaris
	WOS	

Document history

Version	Date	Author	Notes
0.1	08/08/2018	Baruch Menahem (Comsec)	Initial Document
0.2	23/01/2019	Yana Fesh (Comsec)	TOC change
0.3	10/02/2019	Yana Fesh (Comsec)	Preliminary writing
0.4	12/02/2019	Haim Nachmias (Comsec)	Review and comments
0.5	17/02/2019	Yana Fesh (Comsec)	Certification process in-depth
0.6	05/03/2019	Yana Fesh (Comsec)	Certification of CIPSEC as a framework
0.7	08/03/2019	Yana Fesh (Comsec)	Certification of CIPSEC separate components
0.8	17/03/2019	Yana Fesh (Comsec)	EU Cybersecurity Act 2018 release review
0.91	24/03/2019	Yana Fesh (Comsec)	Conclusion and executive summary
0.92	26/03/2019	Yana Fesh (Comsec)	Document structure alignment
QA1	05/04/2019	Antonio Álvarez (ATOS)	QA1
0.93	24/04/2019	Yana Fesh (Comsec)	Rephrasing and adjustments
0.94	29/04/2019	Apostolos Fouraris (UoP)	QA2
1.0	30/04/2019	Yana Fesh (Comsec), Antonio Álvarez (ATOS)	Answers to QA2, final check and submission to EC.

Index

Glossary

CI	Critical Infrastructure
CIS	Critical Infrastructure Systems
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IT	Information Security
IS	Information Security
SDO	Standard Developing Organization
WAF	Web Application Firewall
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NGOs	Non-governmental Organizations
ISMS	Information Security Management System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
SOA	Statement of Applicability
KPI	Key Performance Indicator
ENISA	European Union Agency for Network and Information Security

Executive Summary

In recent years, the majority of the world's Critical Infrastructures (CI) evolved to become more flexible, cost efficient and able to offer better services and conditions for modern society. These systems are able to do so by strongly relying on Information and Communication Technologies (ICT).

Along with the operational benefits of ICT integration within CI network come embedded risks in the form of cyber-attacks on the ICT in an attempt to harm the CI itself, having catastrophic real-world effect on an entire country. Therefore, proper cybersecurity countermeasures are sought out to ensure the confidentiality, integrity and availability of the critical infrastructure systems.

This leads many organizations who operate CIs, be it governmental or private sectors, to focus on information security by implementing proper security controls. A world-wide respected method to guarantee and present compliance to these security controls is to have an information security certification by an accredited third party.

With CIPSEC being a unified security framework for CI, various certification options with and for CIPSEC framework are presented in this document, underlining three different angles:

1) **Certification of CIPSEC as one framework**

   Examining the various possibilities to certify CIPSEC as a single unit combined of all its' hardware, software and services components. In this angle certification motivation is of the cybersecurity framework developers to present one's certified ability to provide a comprehensive cyber defense solution.

2) **Certification of the separate CIPSEC components**

   Discusses the certification of the single CIPSEC components. In this angle motivation is to present how this blend of separate heterogeneous security products, services or solutions may be certified each in their own area of expertise in cybersecurity and how this reflects on CIPSEC.

3) **Compliance with (the help of) CIPSEC framework**

   This angle discusses how an implemented CIPSEC framework supports organizations to comply with information security controls they are required to by local and industry regulations. The motivation for certification in this angle is of the CIPSEC clients, be it by choice or obligation.

Being certified to an information security standard is not only a competitive advantage and business enabling legitimacy for both CI operators and cybersecurity vendors, in many cases certification might even be a mandatory requirement. As is seen how cybersecurity compliance becomes an ever-growing requirement of the vendors in the ICT supply chain.

There are many available information security certifications today, and not all of them are relevant or applicable to a complex framework like CIPSEC and its' separate components. The process of certification is known to be costly and lengthy for organizations, selecting the right certification is crucial before walking down the certification process path.

This document presents the most common information security certification prerequisites and preliminary activities, as well as depicting various nuances in each of the certification angle's mentioned above, to be considered by the partners and stakeholders for the purpose of decision making on the certification path.

1 Introduction

Standardization is the process of implementing and developing technical standards based on a consensus of different parties such as firms, users, interest groups, standards organizations and governments. In recent years industry-wise standardization plays an important role in the increasing globalization of the world, supporting complex fields in a manner that is unified across countries and continents.

Cyber-threats are constantly being exploited in Critical Infrastructures (CIs) around the world in various fields. Impacts of these exploitations affect all citizens in many forms such as economic impact, national security, public safety and even peoples' health.

Fields in which CIs operate are constantly regulated and standardized by local governments, for the purpose of avoiding mistakes, minimizing error impact and malfunctions that will have critical and direct influence on modern society.

With CIPSEC being an Information Security (IS) framework[1] for CIs it applies to two fields (IS & CI) that are continuously subjected to standards and regulations, therefore the natural inclination is to have CIPSEC standardized as well, or at least inspect how it supports existing standards in these fields.

CIPSEC certification is reviewed in this document from three different angles:

- **Certification of CIPSEC as one framework** - this angle will review the available certifications for Information Security frameworks similar to CIPSEC.
- **Certification of the separate CIPSEC components** - this angle will review the option of certifying the separate components of the CIPSEC framework.
- **Compliance with (the help of) CIPSEC framework** – this angle will depict how CIPSEC framework supports existing common controls of IS standards, thus enhancing the readiness for certification of the organizations who implement CIPSEC framework.

By associating CIPSEC framework with a certification, CIPSEC will present its compliance to an IS standard, thus gaining a competitive advantage and confirming its legitimacy as an adequate cybersecurity solution provider in the supply chain for CI operating organizations.

1.1 Purpose of the document

The purpose of this document is to bring forward the discussion around various certification options available for and with CIPSEC, to present alternatives practiced in CI industries and cybersecurity field nowadays. To presume certification feasibility, necessary resources, impact, benefits or disadvantages in all the three angles for CIPSEC certification: as a unit, as separate components or as a supporting mechanism for CI operating organizations for their local compliances.

This document will depict how cybersecurity standards are based on IS standard controls, describe and provide examples of said controls, be it in respected world-wide accepted standards, or in local industry-specific regulations. Followed by presentation of the milestones of a certification process, underlining the various considerations and nuances.

The preliminary certification activities for CIPSEC framework are presented in this document.

[1] CIPSEC Project overview

2 Certification purposes and overview

Standardization is known to improve quality and efficiency by clearly setting guidelines, thus decreasing ambiguity and potential mistakes. Certification is the formal process of receiving written assurance by an accredited third party that a product, process or service is in conformity with certain IS standards.

The world of standardization is fragmented and complex. Generalizing standards can be classified into two main types: technical level and the presence of certification schemes. In the IS field specifications of cryptographic algorithms are examples of technical standards, while risk assessment methods are examples of organizational scheme standards.

According to the European Commission statement on Information Communication Technology (ICT) standardization, "having common ICT standards is one of the measures needed to ensure that European industries are at the forefront of developing and exploiting ICT technologies: they ensure interoperability and guarantee that such technologies work smoothly and reliably together."[1]

Nowadays cybersecurity certifications are well respected and sought for as a statement of one's ability to comply with IS standards, therefore the inclination to seek certification options for CIPSEC. In order to increase credibility and demonstrate how CIPSEC meets IS standard conformity, a certification process should take place by an accredited third party.

There are three angles associated with CIPSEC and certifications reviewed individually in this document:

- Certification of CIPSEC as one framework
- Certification of the separate CIPSEC components
- Compliance with (the help of) CIPSEC framework

As cyber threats become more common and impose an ever-growing risk on ICTs, many industries include IS requirements in their laws, regulations or standards, affecting not only industry specific organizations but also their supply chain in the form of partners, vendors and suppliers. The most common way to present compliance with IS standard is to be certified to it.

By certifying CIPSEC to an IS standard we will be able to present how this framework is meeting international best practices of IS, as well as legitimizing CIPSEC in the supply chain for CI operating organizations.

2.1 Standard Developing Organizations

There are several standard developing organizations (SDOs) in the world today, the ones that are also officially recognized by the European Commission for legally receiving standardization requests are:

- ETSI – the European Telecommunications Standards Institute
- CEN – the European Committee for Standardization
- CENELEC – the European Committee for Electrotechnical Standardization

While their fields of competence might overlap, the difference is in their area of effect. CEN-CENELEC membership is composed of national standardization bodies part of the ISO system, ETSI membership is mainly industry-based, while also including academic institutions and national administrations.

Development of a standard takes about 3 years, depending on the complexity and resources involved. Keeping that in mind, CIPSEC operates in a rapidly evolving world of Cyber-threats, which might often precede any standard while it is in the writing period. The need of a standardized framework of Information Security solution for CIs is present.

It is worth mentioning that there are also American SDOs which have cyber-related standards such as NIST (National Institute of Standards) and NERC (The North American Electric Reliability Corporation). NIST

[1] ICT standartisation

published[1] version 1.1 of a Framework for Improving Critical Infrastructure Cybersecurity on April 16th, 2018. However, this framework focuses on the standardizing of risk management of IT and CIs vulnerabilities into the whole risk management of an organization or CI operation, without providing technical solutions or considering any type of family of IS solutions into their framework scope (like WAF, IDS, etc.).

This document will further concentrate on standardization that is officially recognized by the European Commission, emphasizing the more relevant certifications for cybersecurity and the CI industries.

2.2 International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is an international standard setting body composed of representatives from 164-member countries and their various national standard organizations. According to ISO body "ISO was founded with the idea of answering a fundamental question: what's the best way of doing this?"

It's an independent, non-governmental, world's largest developer of voluntary international standards and facilitates world trade by providing common standards between nations.

The SDOs that are officially recognized by the European Commission for legally receiving standardization requests are CEN and CENELEC, both of whom are representatives in the process of standard setting done by ISO.

Over twenty thousand standards have been set covering everything from manufactured products and technology to food safety, agriculture and healthcare, including Information Security. It is also common for local regulations to be influenced by ISO standards, by bringing a formulated set of standards into a complex field, the governing body relies on the ISO body as having respectable, quality and robust standards created by globally-established experts and include existing necessary common factors.

A standard is developed by ISO when a stakeholder, like an industry, contacts ISO with a defined and established need. Each potential-standard that is accepted for development is being looked at carefully and comprehensively by various global components of the ISO body like the technical committee, council, relevant industry, representatives from consumer associations, academia, NGOs and governments. During the approximated 3 years while a standard is developed, it is also constantly reviewed by the involved parties of the ISO body and its advisors, all comments including public feedback, are taken into consideration. Since ISO standards are voluntary agreements, their approval is based on a solid consensus of international experts' opinions.

A draft of the standard eventually needs to be approved by two-thirds of the actively participating members of its' development process when it is brought to a vote, as well as by 75% of participating voters. Only then, when a consensus is reached, the draft actually becomes a published ISO International Standard.

The process of developing standards by ISO is the main strength which makes ISO standards so common and respected – they are created by people who need them, by industry experts throughout the entire process, taking all aspects into consideration. This high involvement of the industry itself in its own standard development assures that the standards are crafted realistically and robustly covering all complexities and needs for the benefit of the industry.

Figure 1 presents the process of standard developing of ISO.

[1] NIST Framework for Improving CI Cybersecurity

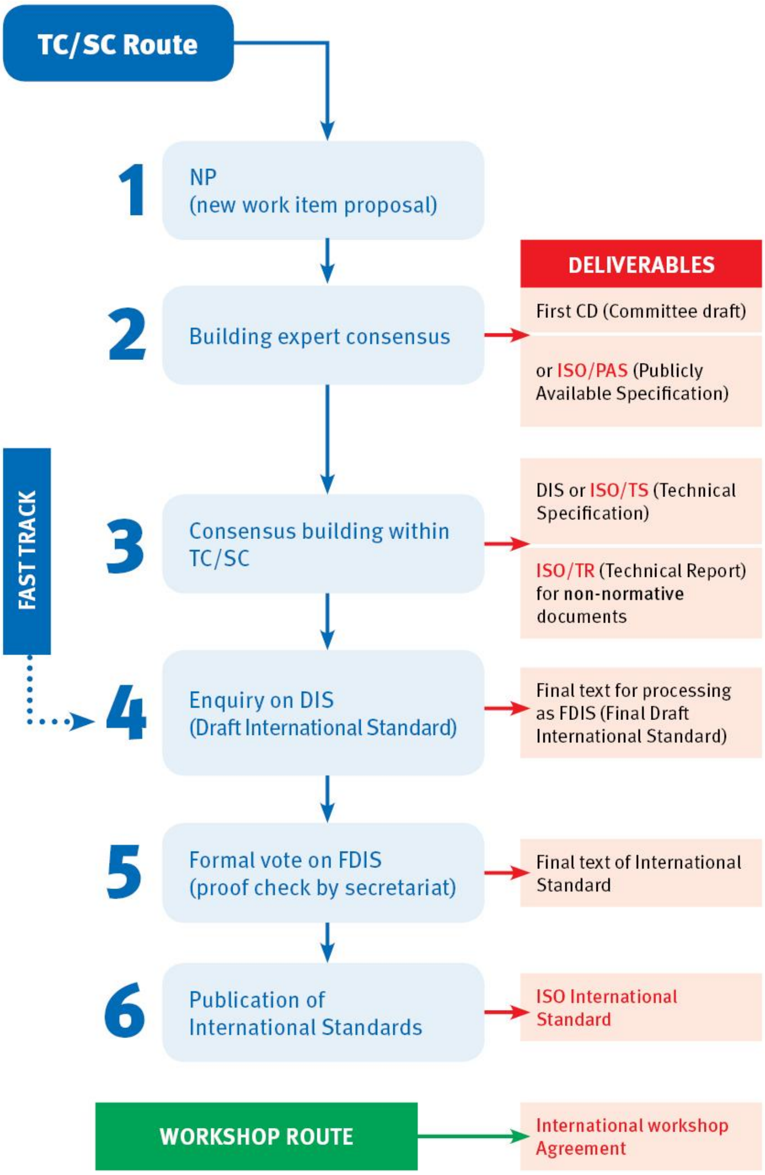
TC/SC Route
1
NP
(new work item proposal)
DELIVERABLES
2
Building expert consensus
First CD (Committee draft)
or ISO/PAS (Publicly Available Specification)
FAST TRACK
3
Consensus building within TC/SC
DIS or ISO/TS (Technical Specification)
ISO/TR (Technical Report) for non-normative documents
4
Enquiry on DIS (Draft International Standard)
Final text for processing as FDIS (Final Draft International Standard)
5
Formal vote on FDIS (proof check by secretariat)
Final text of International Standard
6
Publication of International Standards
ISO International Standard
WORKSHOP ROUTE
International workshop Agreement

Figure 1. ISO Standards development process[1]

2.3 ISO/IEC 27000-family of standards

There are many ISO standards in many fields, ISO is categorizing them by families. The ***ISO/IEC 27000-family*** is developed and published by the International Organization for Standardization (ISO) along with the International Electrotechnical Commission (IEC) to set a globally recognised framework for Information Security management standards and best practices.

The 27000-family is broadly scoped, applicable to organizations, products or systems of all sizes and sectors. New standards are constantly being developed for this family, while older standards are being updated, in order to keep up with the rapidly evolving technology, cyberspace and industrial needs.

The fundamental standard in this family is the ***ISO/IEC 27001:2013 — Information security management systems*** (ISO 27001). This standard broadly contains the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within the context of

[1] ISO standards development process

an organization. It also includes requirements for the assessment and treatment of IS risks tailored to the needs of the organization, in a PDCA model, as presented in Figure 2.

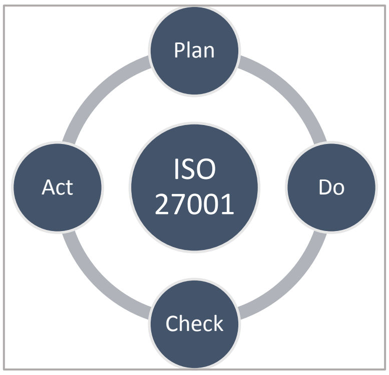

Figure 2. ISO 27000-family PDCA model

Since the requirements in ISO 27001 are broadly generic, they are applicable to any type of organization without setting specific guidelines for industries or technologies. At the same time, since there are no formally defined IS controls in ISO 27001, instead the IS controls from ***ISO/IEC 27002:2013*** are noted in Annex A of ISO 27001. These controls provide more specific guidelines for an organization to follow for implementing the standard and certification of ISO 27001.

In accordance to industrial needs, specific standards in the 27000-family exist, containing IS controls for specific fields or technologies. These types of standards in the ISO 27000-family will be now addressed as "***field*-specific**" standards or certifications. Here are a few examples from the health industry, energy industry or cloud technology:

- ***ISO/IEC 27799:2016*** — Health informatics -- Information security management in health using ISO/IEC 27002

  ISO 27799 provides guidelines for IS management and IS control in the healthcare and medical fields.

- ***ISO/IEC 27019:2017*** — Information technology — Security techniques — Information security controls for the energy utility industry

  ISO 27019 guides organizations in the energy industry (non-nuclear) to apply ISO/IEC 27002 in order to secure their electronic process control systems.

- ***ISO/IEC 27017:2015*** — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

  ISO 27017 provides guidelines for information security controls applicable to the provision and use of cloud services.

There are many more documents in the ISO 27000-family, some are standards for IS for the unique needs of a specific field, or specific technologies like cloud or IDPS (Intrusion Detection Prevention Systems), and more. While some of the ISO 27000-family documents have certifications available for them, other mere supporting documents with controls are equally important as the certifiable standards often point to them for reference.

Regardless of the specific field the controls are designed for, all ISO 27000-family documents are either complementing or heavily relying on the ***ISO/IEC 27002:2013*** controls and ***ISO/IEC 27001:2013*** ISMS structure.

ISO 27000-family is a cross-industry acknowledged and respected Information Security family of standards. With ISO 27001 being not only a common practice, but often a policy or even a regulatory requirement of the supply-chain of service providers, meaning that some industries are even compelled to maintain only certified suppliers, specifically the suppliers of their IS products. ISO 27000-family certifications are respected between many businesses of all industries and sectors, it is considered best-practice of demonstration to the stakeholders of one's ability in cybersecurity principles.

Presented in Figure 3, the number of certified bodies to ISO 27000-family standard which is increasing with each year. An example is the certification survey conducted by ISO in 2017 showing an increase of 410% certified bodies in the last 10 years between 2007 to 2017. [1]

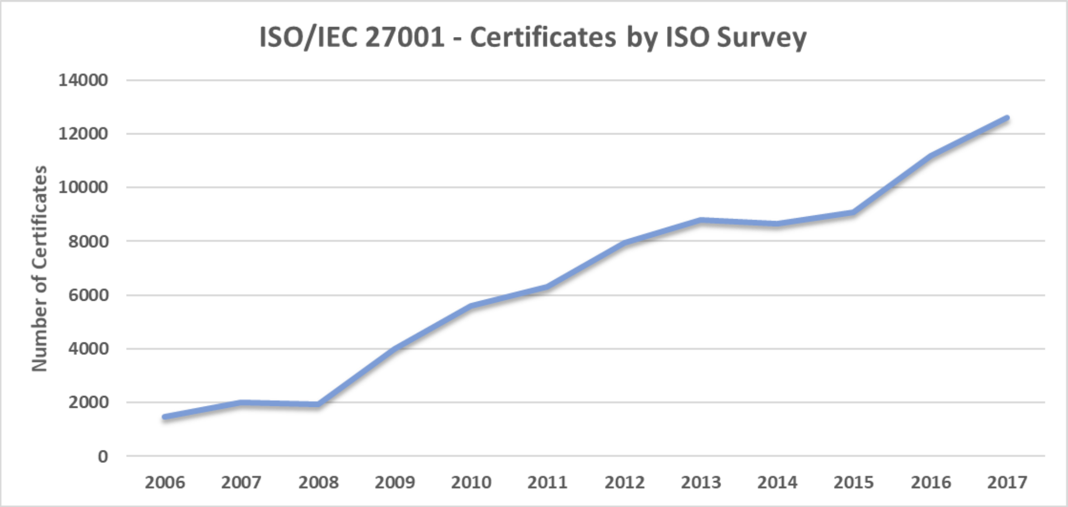

Figure 3. Growing 27001 certification rate[2][3]

[1] 03._ISO_IEC_27001_-_data_per_country_and_sector_2006_to_2017 (1).xlsm from ISO Survey

[2] ISO Survey ISO/IEC 27001 (Excel)

[3] ISO Survey 2017

3 Certification process and resources

The International Organization for Standardization body itself does not perform the certification process, nor do they issue the certificates. The certification process is performed by external third-party accredited bodies; thus, an organization, product or framework cannot be certified **by** ISO.

Organization that intends for a certification is directed by ISO to find a local accredited certification body for that organization's location, or to the International Accreditation Forum who list accrediting groups and bodies. Such accredited body will audit and prepare the globally recognized certification for the specific ISO standard.

Should CIPSEC wish to display its proficiency in Information Security of Critical Infrastructure Systems with a certification, whether if it's for CIPSEC as a unit of framework, or for its' separately combining services or products. Either way partners would implement the controls required in the ISO 27000-family standard. Following the successful implementation, the next step for CIPSEC is to contact an accredited third-party body for a certification in the ISO 27000-family, in order to set the scope and schedule an audit.

3.1 ISO 27000-family controls

There are overall 114 controls in 14 clauses in ISO 27001+2, those are the fundamental controls for Information Security ISO 27000-family standards certification. The controls vary from technical requirements to business procedural directives, from generic comprehensive outlines to more specific guidelines.

Annex number	Clause name	Number of controls
A.5	Information security policies	2
A.6	Organization of information security	7
A.7	Human resource security	6
A.8	Asset management	10
A.9	Access control	14
A.10	Cryptography	2
A.11	Physical and environmental security	15
A.12	Operations security	14
A.13	Communications security	7
A.14	System acquisition, development and maintenance	13
A.15	Supplier relationships	5
A.16	Information security incident management	7
A.17	Information security aspects of business continuity management	4
A.18	Compliance	8

Table 1. ISO 27001+2 control clauses

An organization needs to pay heed to all of the controls in the clauses above in order to be compliant with the standard. Paying heed doesn't necessarily mean being 100% compliant with each control, but address, properly review, set key performance indicators and document the process, while seeking to constantly improve compliance status with each control.

Should CIPSEC, or its' combining partners, apply for a specific certification in the ISO 27000-family, not just the fundamental ISO 27001, either way it will be audited for both controls of ISO 27001+2 **jointly** with the specific other ISO 27000-family controls.

Figure 4 shows the combination of controls one needs to comply with when applying for an ISO 27000-family certification.

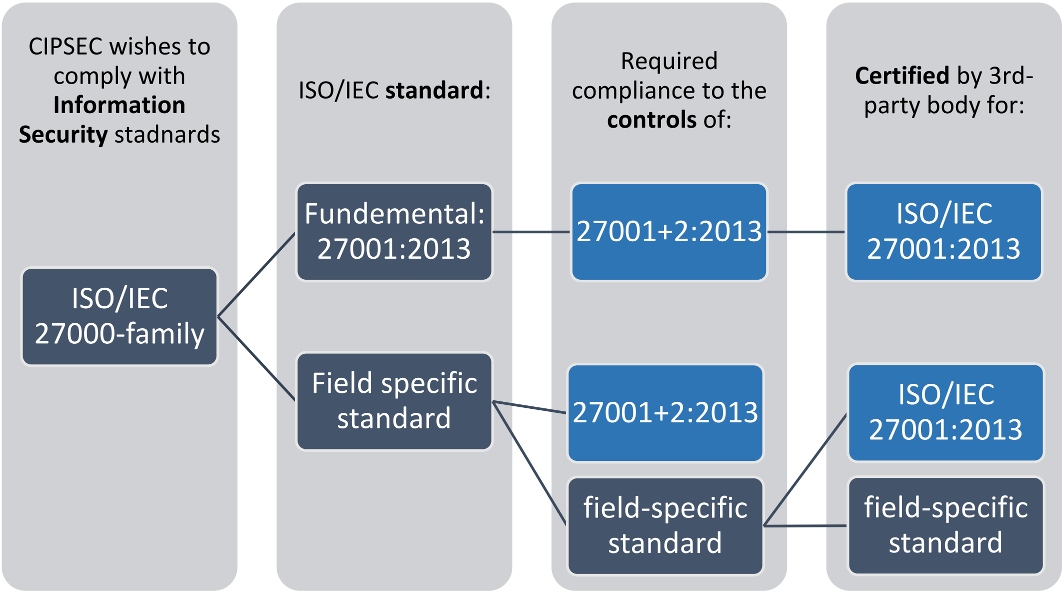

Figure 4. Certification controls implementation process example

3.2 Certification milestones

Transverse technical and organizational preparations are required of an organization to take place, prior audition of the accredited third-party body which awards the certification.

Determining whether the knowledge for this sort of process is present, or a consultancy company in the field has to be hired is advised at this point. Regardless, it is important to get familiar with the IS controls, processes and terminology of the ISMS and the ISO 27000-family.

The common milestones of preparation for ISO 27000-family certification are described below and presented in figure 5:

1) Define context, scope and objectives

The foremost and initial milestone is to determine the scope of the Information Security Management System (ISMS), which may include: the entire CIPSEC framework, separate partner organizations, specific departments within them, limited specific products or services of an organization that are components of CIPSEC and determine the geographical locations of selected scope.

When defining the scope, the needs and requirements of interested parties should be taken into consideration, it can be the European Commission, existing or potential clients, partner and vendors, governments or field regulations. All stakeholders need to be clearly identified and their call for certification needs to be defined as well.

Defining the scope is the initial core decision, which all other prerequisites steps are derived of and based upon.

2) Define management framework

Defining management framework is a related output of the scope definition, this will underline the relevant business processes which will be audited for certification, hence all preparations and prerequisites regard these processes.

Each process will include the asserting accountability of the ISMS, a schedule of activities, and regular ongoing auditing to support the PDCA model of continuous improvement.

3) Conduct risk assessment

Before conducting the risk assessment, the organization should map its' assets, in order to establish some sort of security criteria baseline, it will refer to the business processes and include legal, regulatory requirements and contractual obligations, and how they relate to information security.

A formal process of risk assessment is required to take place and be documented. The methodology of the risk assessment is up to the organization to select and follow. The risk assessment should be thorough and relevant to the selected scope.

4) Implement controls to mitigate the risks

After risks were identified, each risk will be categorized according to each organization's criteria - treat, tolerate, terminate, or transfer the risk. This process needs to be documented, for each risk the organization needs to clearly state what and when will be done in order to mitigate the risk.

5) Training and awareness

Even without compliance for an ISO standard, training and awareness of Cyber Security is on the rise in organizations. Having said that, what is required for the ISO compliance process is to document the training plan, attendees and keep tracking of the process.

Not all employees will be trained identically, depending on their role and the organization's training plan. Some employees might need to actually change the way they work to some extent, for example to comply with clean desk policy. This can also be viewed as a good opportunity to bind the employees for the organizational commitment to an ISO 27000-family information security standard.

6) Prepare required documentations

Documentation of the entire process is needed prior the audit, including ISMS scope, all policies and procedures, asset mapping, risk assessment, risk mitigation plan, trainings' audit, statement of applicability (SOA), information security objectives, evidence of competence, internal audit process, evidence of the nature of the non-conformities and any subsequent actions taken and results of any corrective actions taken.

Proper documentation is key for any audit.

7) Measure monitor and review

ISO is built in a PDCA model, compelling organizations to continuous improvement, which is also required to be properly recorded. The performance of the ISMS needs to be constantly analyzed and reviewed for effectiveness and compliance, in addition to identify improvements to existing processes and controls.

This can be done via a dedicated application system, or in a similar-to-SOA document, which contains the organization's numeric key performance indicators (KPIs) versus the monitored activities and their numeric expression of progress.

Building KPIs for self-assessment of the organization's IS standard conformity is not a simple task, it is transverse including all business aspects and departments of the scope selected. These KPIs are important as are reviewed annually and should be updated regularly decreed by the risk assessment.

8) Internal audits

The internal audit is the final preparation stage for the organization, in the form of a general rehearsal similar to the gap analysis but much more detailed. The internal audit is commonly held by an external third-party certified Lead Auditor, mimicking the real certification audition by the accredited third-party body auditor.

Some time should be reserved between the internal and actual audit, depending on the scope, for realistic changes that might be required to take place should any be raised during the internal audit.

9) Certification audits

The final phase after which, if was successful, a certification is awarded. An in-depth description of the audition is addressed in chapter 3.2.2 Audition for certification.

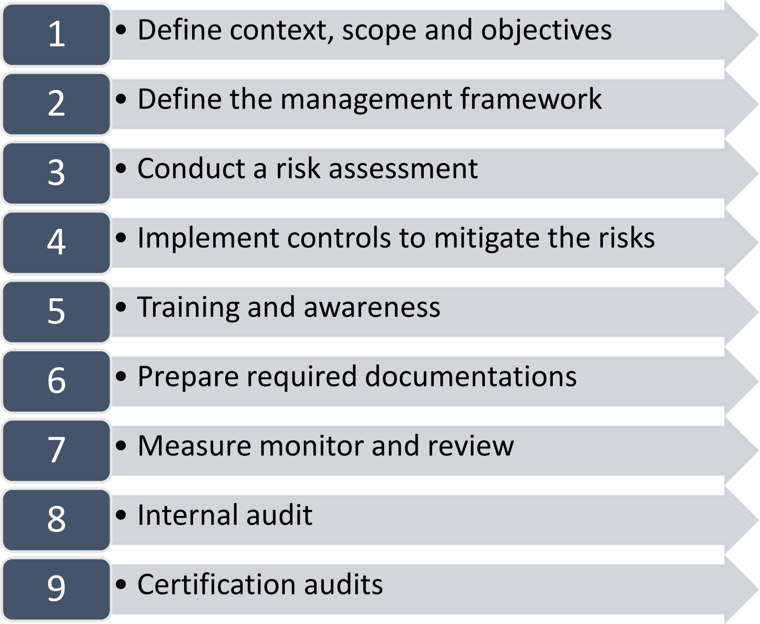
1
• Define context, scope and objectives
2
• Define the management framework
3
• Conduct a risk assessment
4
• Implement controls to mitigate the risks
5
• Training and awareness
6
• Prepare required documentations
7
• Measure monitor and review
8
• Internal audit
9
• Certification audits

Figure 5. ISO 27000-family certification process

These milestones, including in them the compliance to ISO 27001+2 controls, are the prerequisites for ISO 27000-family certification process for all organizations, systems, frameworks, big or small, whether CIPSEC will pursue certification as a framework, or for its separate components.

3.2.1 Gap analysis

The gap analysis is an independent phase that can be conducted at different stages of the certification process, it is commonly done after identifying stakeholders and selecting the scope of certification, or prior the internal audit. This is not a mandatory phase for a certification process, however it is recommended in some cases.

Gap analysis is a common practice that acts as a high-level examination to assess and compare an organizations' readiness to the requirements of the standards' controls. Conducting a gap analysis will assist in determining the resources required prior to engaging the certification activities.

Resources required for a gap analysis include time and availability of organization's personnel for questioning, the gap itself can be done by tools or internally within the organization, if the knowledge exists, but preferably be done by an external not necessarily accredited body for a more objective view.

The process of the gap analysis is to review all prerequisites of the ISO standard controls, by questioning the relevant personnel. No evidence is demonstrated at this stage, each control receives a numeric measurement of compliance percentage. Such process can take between 1-5 days per partner or product, depending on the scope and size of the intended certification and organization.

After the gap analysis is finished, it will reflect the readiness of the organization or product to certification. The gap will present what remains to be done, which controls are weak, which are compliant, and so will help estimate the required resources and remaining actions needed to be taken prior the certification audit.

3.2.2 Audition for certification

The audition for certification is the last milestone after which a certificate is awarded. Since this milestone is significantly affecting the certification process and resources, it is covered in-depth here.

The audition procedure for ISO 27000-family certification varies depending on variables such as:

- Certification scope - organization / service / product / solution
- Size of selected scope audited
- Number of sites to be visited by the auditor and their locations
- Accredited third-party body tariff which is selected as auditor
- What year of certification audition it is

The primary routine certification audition generally consists of two phases, stage 1 and stage 2, both conducted by an accredited 3rd party auditor.

Stage 1 includes an overview of all necessary documents that support the IS governance process and provide guidelines to the of ISMS activities in the audited scope. A high-level review of the ISMS and review of the internal audit, confirming they are in-line with the requirements of the standard. At this stage minor nonconformity or potential improvements of the ISMS might be suggested and should be taken into account for the success of Stage 2, and the audition of next year.

Stage 2 includes a thorough assessment of the ISMS, here the auditor will seek to confirm existing processes with standards' requirements. The auditor will dive into all controls and their supporting evidence, cross-reference them with presented practices within the audited scope and with the written documents which were presented in Stage 1.

Following the successful completion of Stage 1 and 2 the auditor will determine compliance status to the ISO 27000-family standard and award the company with confirmation of the certification. Actual certification will be sent by the accredited third-party body of the auditor depending on their practice, be it a digital or a hard-copy.

Successfully fulfillment of stages 1+2 awards the organization with the certificate and will commit the organization for an annual surveillance audit in the next 2 years, since maintaining the ISO 27000-familiy certification requires an annual mandatory surveillance audit visit. On top of that, every 3rd-year a full extensive re-audit needs to take place for re-certification composed of stages 1 and 2 again.

Not all accredited 3rd-party bodies who act as auditors for the certification process are accredited for **all** ISO 27000-family standards, and not all auditors are necessarily travelling to all destinations of all branches. Selection of the external body for the certification process needs to be taken into consideration and investigated thoroughly with several accredited bodies for price and scope comparisons.

3.3 Timeline and costs

There are many variables that affect directly and indirectly the timeline and costs of the certification process, all of which need to be taken into consideration for the certification process of CIPSEC.

1) Certificate standard selected (*ISO/IEC 27001:2013* or field-specific of the ISO-27000-family)

The difference between ***ISO/IEC 27001:2013*** or ***field-specific*** standard are additional controls, as reviewed in *3.1 ISO 27000-family controls* chapter. Should there be more controls, more prerequisites will be required of an organization before the final certification audit, this affects both costs and timeline directly.

2) Scope for certification (CIPSEC as a whole, separate products/partners)

This determines which part or parts of an organization need to prepare for the prerequisites and be a subject to auditing by the external body. As explained in *3.2 Certification milestones* chapter preparing an organization for compliance to the controls requires resources, and the amount of preparation needed depends on the organizations' readiness. The bigger the scope, means more elements will be audited and need to be compliant with the prerequisites, the bigger time and costs are, and vice versa.

3) Number of sites to be visited by the auditor and their locations

The number of sites to be visited and their location will directly affect the quotation supplied by the accredited third-party body who will conduct the certification audit, the more sites the higher the costs and time for both preparation and audition. Dividing the audition between various local accredited third-party bodies will not necessarily be more cost efficient, depending on each body's tariff, some are known to travel to other countries for auditing remote-related scope of their initial local host.

Number of sites to be visited during audition affects indirectly time and costs as well, as more sites need to be prepared for the prerequisites.

4) Readiness and year of audition

The readiness for ISO-27000-family certification prerequisites, or the readiness of selected products combining CIPSEC framework may impact the agility of the process.

Mature readiness usually means the presence of ISMS activities embedded both in business processes and IT systems, so that a strong majority of the controls have been minded and possibly are compliant, those not compliant are managed in the risk management plan. The more mature the readiness is, less additional time and costs are required of that organization to invest for prerequisites completion for the certification process.

The year of audition is also affecting time and costs resources, this is relevant if a certification of the separate partners/products is selected, since if CIPSEC is to be certified as a single framework it will be its' initial award year. Be it the initial certificate award year, or the third year which is a re-certification process, might require more resources to complete prerequisites. The two in-between annual surveillance audits generally require less preparation, reflecting as lower time and costs investments.

5) Accredited third-party body tariff which is selected as auditor

Selecting the external auditing body or even several bodies is a task on its own, and it directly affects the timeline depending on the type of certification we are looking for CIPSEC, be it ***ISO/IEC 27001:2013*** or ***field-specific*** of the ISO-27000-family. As mentioned in the *3.2.2 audition chapter*, not all auditors are accredited for all ISO 27000-family standards or travel to all locations, so the selection of the auditor will be known after the scope or wanted certification is determined.

A general rough estimation of a timeline can be suggested at this stage, for the ISO 27000-familly certification processes of separate CIPSEC partners or products, a period between 3-12 months is likely for the ISO 27000-familly certification.

An estimation of certifying CIPSEC as a framework cannot be done at this stage, as there is no existing certification for such frameworks, more is discussed in chapter *4 Certification of CIPSEC as a Framework*.

Based on all variables above, cost estimation for certifying CIPSEC partners or products cannot be done even roughly at this point, and should be re-examined when:

- A certification scope for CIPSEC is selected, and;

- A gap analysis is done.

4 Certification of CIPSEC as a Framework

The first angle of certification discussed in this document is the certification of CIPSEC as a single framework.

CIPSEC is a complex and heterogeneous security framework, a combination of application components, hardware components and services, in the form of individual products tailored together. There is a natural need of such complex framework to follow standards guidelines to maximize efficiency while minimizing errors in CIPSEC implementation and of its’ ongoing activity.

A certification of CIPSEC will display the ability of this complex solution to follow IS best practices according to a standard or a schema. The prestige and respect of having a certified framework is also a competitive advantage, given the increase in demands by CI operators of their cybersecurity solutions to be certified to IS standards.

However, when considering certifying CIPSEC as a single unit, we need to take into account the loss of modularity in the provided certified solution. Certifying CIPSEC as one unit including all tools and services **as-is**, means that any certification will be in affect only when the entire combination of tools and services is present in the solution, losing flexibility for the end-clients to tweak the heterogeneous combo of CIPSEC according to their organizational and technical needs. Therefore, this type of certification will be meaningless for clients that will not take the entire CIPSEC framework as-is, since the separate components are not entitled to any certification derived from the certification of the framework.

Additional dilemma with certifying CIPSEC as a single framework is that CIPSEC is not a legal entity, nor was a combination of CIPSEC’s products specifically identified by stakeholders to be a legal entity. Therefore, this should be established prior certification activities. The discussion of certifying CIPSEC as a single unit is theoretical at this stage and assumes all separate ingredients are in the scope of the CIPSEC framework unit.

As of the time of writing the paper, no single existing standard meets the needs of certification for CI cybersecurity framework such as CIPSEC, this section will further discuss the potential options.

The previously mentioned “*NIST publication of version 1.1 of a Framework for Improving Critical Infrastructure Cybersecurity on April 16th 2018”*[1], is published as a framework for cybersecurity for CI emphasizing on the ICT risk management aspects. It is similar to the ISO 31000-series of Risk Management.

ISO’s risk management framework was considered for CIPSEC as well, however CIPSEC presents a realistic, working and existing framework as a solution for various existing cyber-risks on CIs. CIPSEC helps an organization to technically mitigate its cyber-risks by enabling various innovative tools that identify, protect, detect and respond alongside with the IT infrastructure in which the CI is operating. Hence, the risk management framework was found to be more business oriented and not technical enough to emphasize CIPSEC’s strengths.

Two additional cybersecurity certifications were examined, however, none of them were published by the time of completing this document. They are strong candidates for certifying CIPSEC and are presented in the following two sub-sections.

4.1 ISO/IEC 27101 Cybersecurity - Framework development guidelines

On June 2018 ISO approved[2] the proposal and started the new project of ***ISO/IEC 27101 Cybersecurity - Framework development guidelines***, this standard is currently being written and will offer guidance for those developing cybersecurity frameworks.

Of what little is known about this standard at this time, is that it will define a basic set of controls to assist with creation of complex cybersecurity frameworks, like the cybersecurity framework that CIPSEC is. This new standard fits CIPSEC better than other existing field-specific standards available in the 27000-familiy.

[1] NIST Framework for Improving CI Cybersecurity (PDF)

[2] ISO/IEC WD TS 27101

We also know that since it belongs to the 27000-family, we can assume it will rely on the basic controls of ***ISO/IEC 27001+2***, with additions or changes of relevant controls for cybersecurity frameworks.

As reviewed in the chapter 2.2 International Organization for Standardization (ISO) the estimation for new standard publication is 3 years, meaning sometime during 2021 the standard will be out for the public to buy. It is worth mentioning that the external accredited third-party bodies will also need time to validate their accreditation with ISO to conduct audits of this new standard to award certifications. At this point no time estimation can be suggested as to how long will it take the accredited bodies to catch up, or how many of the accredited third-party bodies will even be able to audit this new standard.

It is difficult to assume at this stage that this certification will definitely fit CIPSEC in the future, however, should CIPSEC determine the scope of certification to constitute CIPSEC as one unit, this new standard becomes a strong potential candidate which should be re-examined once the standard is published.

4.2 EU Cybersecurity Act 2018

As this document was written, on March 12th, 2019, the European parliament has announced[1] that it will adopt the EU Cybersecurity Act 2018[2]. This act, for the first time in Europe, creates a unified EU-wide cybersecurity certification scheme to ensure that certified products, processes and services in the EU are indeed according to ENISA defined IS standards.

The Act has been already informally agreed with member states. It emphasizes the importance of certifying critical infrastructure, including, but not limited to, energy grids, water, energy supplies and banking systems as well as products, processes and services. What more, by 2023, the European Commission will assess whether any of the new voluntary schemes should be made mandatory.

This act is still new, and not fully researched by the time of this document submission, but this act is expected to simplify the certification process for IS products, processes and services in the EU. By providing common cybersecurity requirements and evaluation criteria across national markets and sectors, the complexity of time and costs for this certification should be lower in comparison to existing available certifications.

The certification scheme is to be published by ENISA (European Union Agency for Network and Information Security), it is currently being developed[3] by The European Cyber Security Organization (ECSO) ASBL, a fully self-financed non-for-profit organization under the Belgian law, established in June 2016. ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP).

No scheme publication date is available yet, nor were accredited bodies defined, and yet given the benefits of potential resources reduction, and considering the chance this certification will become mandatory for operating in European market of CIs, CIPSEC should follow-up on this new certification process of EU Cybersecurity Act 2018.

[1] European Parliament News

[2] EU Cybersecurity Act 2018 (PDF)

[3] ECS European Cyber Security Certification: A Meta-Scheme Approach v1.0

5 Certification of separate CIPSEC components

The second angle of certification discussed in this document is the certification of the various components CIPSEC framework is made of.

CIPSEC is a complex security framework that orchestrates state-of-the-art heterogeneous security products, both hardware and software, and additionally this ecosystem includes services that support the proposed technical solutions[1][2]. Therefore, when discussing the certification of separate CIPSEC components all of the three types of components are taken into consideration.

The table below presents the separate components of which the CIPSEC framework is composed, divided into hardware, software and service components. This classification assists in determining the right certification for the various components, as not all components are fit candidates for all certifications available. Simple example is of hardware versus software IS standards, even within the ISO 27000-family there are different standards for cybersecurity hardware components which don't apply for a software.

When applying for a certification the applicant is required to determine the scope of certification, this is not only the first step in the pre-requisites for compliance, but also appears in the "scope" section of the awarded certification diploma. The external accredited third-party auditor is using this scope for setting the boundaries of the audit accordingly and for its' tariff and quotation.

When determining the scope of the separate CIPSEC components, it is worth mentioning that some of the solutions and services of CIPSEC are not the entire area of business for the partner company, however only they are in the scope for certification under CIPSEC framework, not the entire company. This means partners will have to undergo the complex implication of the prerequisites' establishment for certification but have only the specific item in the scope section on the certification diploma, which is the one involved in the CIPSEC framework.

Table 2. CIPSEC products and services

Company name	Component name	Hardware solution	Software solution	Service solution
Atos	XL-SIEM		X	
Atos	NIDS		X	
Empelor	Secocard	X		
UPC	Data Privacy Tool		X	
AEGIS Research	Forensics Visualization Tool		X	
University of Patras	HSM / FPGA device	X		
World Sensing	Jammerdetector	X	X	
FORTH	Honeypot	X	X	
Bitdefender	Total Defender / Gravity Zone		X	
Comsec	Vulnerability assessment			X

[1] CIPSEC Project Overview

[2] CIPSEC System Design

Technische Universität Darmstadt	Compliance management			X
Atos,	Contingency plan			X
ATOS, Worlsensing, UOP, UPC, FORTH, Technische Universität Darmstadt, Comsec, Bitdefender, Empelor, AEGIS Research	Training courses			X
AEGIS Research	Forensics			X
Bitdefender	Updating-Patching			X

5.1 ISO/IEC 27001:2013 (ISO 27001) - Information security management systems

The basic pillar certification of the cybersecurity ISO 27000-family is ***ISO/IEC 27001:2013***, it is applicable to all organizations, regardless of type, size, industry or market. On the scope section of this certificate a certain product, service or solution can be selected, it is vast and generic enough to apply for all CIPSEC components.

Certified compliance with ISO/IEC 27001 by an accredited third-party body is increasingly being demanded from suppliers and business partners by organizations that are concerned about the security of their information, and about information security throughout their supply chain. This is even more emphasized in CI industries, where this certification of the vendors in the ICT supply chain is often a requirement documented in local industry regulations.

Being generic enough to be able to include all CIPSEC separate components, whilst being respected across markets and industries, this standard is a strong candidate for the certification of the separate CIPSEC components.

5.2 Other available certifications

There are other available certifications within the cybersecurity family of ISO 27000, as well as of other families. These are the so called previously ***field-specific*** certifications, however as the name suggests, these certifications are to very specific standards that might not apply to all of the components of CIPSEC. This document will present a few of such field-specific certifications available and applicable for some of the CIPSEC components.

- **ISO/IEC 27017:2015[1] (ISO 27017) - Code of practice for information security for cloud services**

This standard addresses the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific IS controls, it relies on the controls of ***ISO/IEC 27002***, but supplements as necessary as well as provides additional cloud-context controls. The standard advises both cloud service customers and cloud service providers, with the primary guidance laid out side-by-side in each section.

[1] ISO/IEC 27017:2015

This standard is applicable to cloud-components of the cloud-based version of CIPSEC framework, where CIPSEC offers to host some of the components on cloud infrastructure instead of on the clients' premises.

- **ISO/IEC 27037:2012[1] - Guidelines for identification, collection, acquisition and preservation of digital evidence**

ISO/IEC 27037:2012 sets the standard for identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, emphasizing on preserving its integrity. Since each country has its own unique legislative system, a crime committed in one jurisdiction may not even be regarded as a crime in another.

Cross-border cyberattacks on CI are not an unusual case, there is a real challenge to processes such cybercriminals due to the lack of common practice methods to collect and processes forensic investigation of digital evidence. Today investigators and organizations retain certain methods, however they are not unified and often don't fit the demands of the court.

Some CIPSEC tools are collecting evidence and presenting them, therefore they are valid candidates for certification of this "digital evidence" standard.

- **ISO 15408-1:2009[2] - Evaluation criteria for IT security**

This standard of The Common Criteria for Information Technology Security Evaluation (aka CC) contains a set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. Therefore, it allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements.

The CC was developed through a combined effort of six countries: The United States, Canada, France, Germany, the Netherlands, and the United Kingdom. It is considered to be one of the most thorough certifications processes for cybersecurity products to comply with, since It was especially designed for products destined for highly security-intensive markets, such as governmental, banking or military sectors.

However, this standard is both old and collides with a very necessary IS principle – the need to have updates to deal with new vulnerabilities. Whenever certifying a product for CC, a specific version is certified, meaning the certification doesn't apply to any update released afterwards. Therefore, this certification is seen less[3] in recent years in the industry, whilst on the contrary an increase in cybersecurity solutions is seen in the market, meaning even top cybersecurity firms don't apply for this certification unless specifically required by a stakeholder for a specific version of their product.

This certification can be relevant to the hardware solutions of CIPSEC, in case they are not planned to be subject for frequent updates.

[1] ISO/IEC 27037:2012

[2] ISO/IEC 15408-1:2009

[3] CC statistics

6 Compliance with CIPSEC framework

It has been established that CI relies heavily on ICT for its' control and operational systems. As modern society relies more on these infrastructures, they become more precious as well as targeted by adversaries, needing stronger measurements for securing their ongoing operation and integrity of the data within them. CI information and privacy protection is consequently prominent in the public's eye across countries and industries.

All this brings an increasing involvement in the IS requirements of CI operating organizations in all industries in the form of pressure from local government laws and regulations. In some cases, the pressure merely forces organizations to act in **compliance** to certain IS rules and practices dictated in the locally published procedures. Whilst in other cases, similar laws and regulations dictate the organization to be **certified** to certain IS standards, like the ISO 27001, 27799, SOC2, SOX, etc.
In both cases, a CI operating organization finds itself with the need to comply with **IS controls**.

These laws and regulations are made for the protection of CI organizational information to ensure its operation and availability for the general public. Therefore, CI organizations have to adopt various IS practices to provide the foundation for building a robust response to regulatory requirements. They have to incorporate specific legal requirements in their IS practices for meeting the legal obligations for information security.

Consequently, significant changes within organizations such as the standardization of operational processes and practices have to be made to show the conformity with such laws and regulations. Failure to do so can result in stringent legal actions against the CI operating organization or even its top management.

One example is a constant upward trend in the mandatory ISO 27799 certification requirement of governments in the EU of their various healthcare providers, in the forms of local law or regulations. These laws are broad and include various healthcare industry organizations, but it most definitely includes hospitals which are considered a CI operating organization. This being an example of how CI operating organizations have the need to be certified to an ISO 27000-family standard, therefore comply with IS controls.

The ISO 27000-family controls are commonly used as a baseline by the different local regulations, laws or policies that dictate local IS controls of their own for the CI organizations. The implementation of CIPSEC framework within the boundaries of a CI operational network offers compliance for many of such IS controls.

Below presented a few of the more common **IS controls** as examples, to which implementation of CIPSEC is a supporting measure for providing compliance. Need to mind that these are out of context here, since each organization applies controls differently based on its' assets and risks.

- **[A7] Human Resources**

Proper IS training is expected of all employees, depending on their role in the organization and their use of IT and ICS. Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

This includes training of employees, when necessary technical training, which is available as part of CIPSEC services under **Training Courses** service.

- **[A10] Cryptography**

Appropriate cryptographic controls need to take place in order to meet the information security policy objectives.

While other organizations can decide for themselves whether to implement cryptographic means, CI networks and systems are often pressed by a regulation to use a cryptographic solution while managing data both at rest and in transit, depending on the data type, classification, industry and country.

CIPSEC provides levels of encryption solutions in several of its' combining products such as the **Secocards** and **HSM / FPGA device**.

- **[A12.2] Protection from malware**

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls.

With the protection of the **Total Defender / Gravity Zone** software solution this control can be addressed by CIPSEC.

[A12.4] Logging and Monitoring

The control defines that event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

CIPSEC provides a comprehensive logging platform with its' **XL-SIEM** solution. Event logs can contain sensitive data and personally identifiable information, appropriate privacy protection measures are also part of CIPSEC framework in the **Data Privacy Tool** solution.

[A13] Communication Security

The Networks should be managed and controlled to protect information in systems and applications. Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access.

This control is addressed by the **Antijamming detector** software and hardware solution of CIPSEC, as well as the encrypting mechanisms mentioned earlier.

As mentioned, the above are mere examples, there are more controls in the ISO 27000-family which in the correct context within an organization are being compliant with the assistance of CIPSEC products, solutions and services. Since local regulations are often based on the ISO 27000-family controls, it is safe to predict that the implementation of CIPSEC in a CI organizational network will assist in compliance with local IS controls as well.

7 Conclusions

Certification to information security standards gains popularity in recent years, as a way to present one's conformity to necessary measurements to keep the confidentiality, integrity and availability of the data and systems.

Similarly, the involvement of local governmental regulations across industries that operate critical infrastructures, pushes to include more information security directives and requirements. Many of such local regulations are based on best practices of existing information security standards such as the ISO 27000-family.

Together this brings critical infrastructure operating organizations to the need to comply with information security controls, some of such controls are technical and can be adhered by CIPSEC framework. Other controls are governing the organization to certain supply chain policies, such as mandatory requirement of doing business with only certified vendors.

Having said that, stakeholders for CIPSEC certification are not yet clearly identified. Since the existing available certification processes are complex and lengthy, the stakeholders should first be identified and set concrete certification objectives and scope, this will allow detailed certification process assessment.

As this document was written, on March 12th, 2019, the European parliament has announced that it will adopt the EU Cybersecurity Act 2018[1]. Part of this act is the creation of a unified EU-wide cybersecurity certification scheme, which will be assessed during 2023 by the European Commission, whether to be made mandatory or not.

In case a mandatory certification will be required in the EU of critical infrastructure information security operations, then this is the certification CIPSEC should pursue. But until more is known, with the existing available certification options, stakeholders should first be identified in order to establish certification objectives and scope. Following these establishments, a detailed certification process can be assessed including accurate time and costs estimations.

Figure 7 depicts the conclusion of this document as by the order suggested for preliminary certification activities. Initially stakeholders should be identified, they provide the objectives as the actual need of engaging in certification activities. Once objectives are defined, the proper scope shall be selected considering the objectives set by the stakeholders and the available certification options.

After the scope is selected, next step is to conduct a gap analysis which will result in estimations of the necessary resources for compliance with the information security controls of the standard or schema of the selected certification. Planning the process of mitigating the gap with the requirements of the IS controls is the final stage of the preliminary certification activities, the smaller the gap the smaller are the resources required to mitigate it.

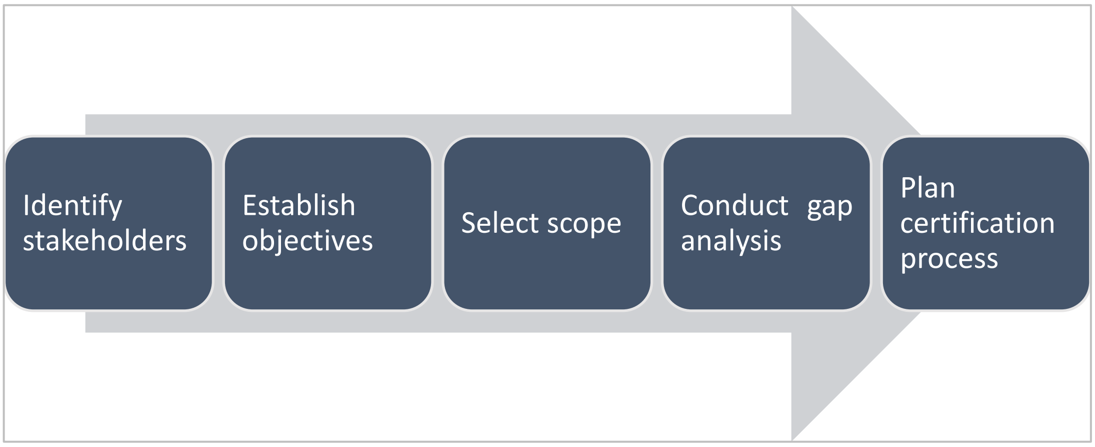

Figure 6. Preliminary certification activities

[1] EU Cybersecurity Act 2018

8 References

i. Economic benefits of standardization Summary of results Published by DIN German Institute for Standardization e. V. 2011
Available online:
https://www.iec.ch/about/globalreach/academia/pdf/academia_governments/economic_benefits_standardization.pdf

ii. Information Security Standards in Critical Infrastructure Protection, by Alessandro Guarino. ISSE 2015 - Highlights of the Information Security Solutions Europe Conference 2015, 2015
Available online:
https://www.academia.edu/14707972/Information_Security_Standards_in_Critical_Infrastructure_Protection

iii. Information Security Compliance in Organizations: An Institutional Perspective, by Ahmed AlKalbani, Hepu Deng, Booi Kam, Xiaojuan Zhang, published in DE Gruyter open, Data and Information Management, 2017

iv. CYBER; Protection measures for ICT in the context of Critical Infrastructure, by ETSI. Published ETSI TR 103 303 V1.1.1 (2016-04)

v. INTERNATIONAL STANDARD ISO/IEC 27001 + 27002, published by ISO, 2013

vi. https://www.iso.org/about-us.html

vii. https://www.iso.org/the-iso-survey.html - survey and statistics

viii. http://www.iso27001security.com/html/27101.html

ix. https://www.iso.org/standard/54534.html

x. http://www.iso27001security.com/html/27019.html

xi. http://www.iso27001security.com/html/27001.html

xii. https://www.commoncriteriaportal.org/products/

xiii. https://www.sciencedirect.com/science/article/pii/S0166497215000929

xiv. https://ec.europa.eu/growth/industry/policy/ict-standardisation_en#rolling_plan_ict_standardisation

xv. http://www.exemplarglobalcollege.org/how-iso-standards-are-developed/

xvi. https://www.iso.org/developing-standards.html

xvii. https://www.iso.org/members.html