D11.5

International and national cybersecurity certification initiatives – Updates

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D11.5 / V1.0
Work package contributing to the deliverable	WP11
Due date	January 2022 – M36
Actual submission date	28th February, 2022

Responsible organisation	CETIC
Editor	Nikolaos Matskanis
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable is an update on the analysis of national European cybersecurity initiatives (D11.1) and their adoption of SPARTA research programs as well as other European pilot projects with which SPARTA partners have collaborated.
Keywords	Cybersecurity, Certification, Standard, SME, Process, European Cyber Act

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Nikolaos Matskanis (CETIC)

Contributors (ordered according to beneficiary numbers)

Philippe Massonet, Sébastien Dupont, Guillaume Ginis (CETIC)

Nicolo Maunero (CINI)

Tiziano Inzerilli (ISCOM)

Reviewers (ordered according to beneficiary numbers)

Franck Sadmi (ANSSI)

Hervé Debar (IMT)

Gabriele Costa (CINI)

Disclaimer

Content Updates Table

The following table provides a list of all content that has been updated in this report from the Deliverable D11.1.

Chapter or Section	Pages	Description of changes
4.1 CAPE (WP5) Continuous assessment in polymorphous environments	46-66	Recommendations, specifications of certification standards and frameworks relevant to CAPE
4.2 WP6 HAII-T – High-assurance intelligent infrastructure toolkit	66-69	Standards and framework relevant to HAII-T Analysis of adoption of cybersecurity initiatives and integration of the GDPR certification tool with the cybersecurity certification processes
Chapter 5 Collaboration with other European Pilot Projects	70-73	Description of the collaboration opportunities

Executive Summary

The cybersecurity landscape is changing quickly in Europe with the entry into force of the EU Cybersecurity Act and the creation of a European wide cybersecurity certification framework. The current favourable context for cybersecurity certification in Europe is an opportunity for SPARTA to show that some of its results, and notably the assessment tools developed in the CAPE program, can be useful in a certification context.

D11.5 is an update of D11.1 that was submitted at M12. It provides an overview of the European security certification landscape, identifies relevant cybersecurity schemes and associated standards, and provides concrete recommendations about integrating cybersecurity certification activities into the SPARTA research programs. A broader list of cybersecurity frameworks, best practices and standards is available in the annex. A draft method for comparing cybersecurity certification schemes and associated standards can be used to make different comparisons than the ones presented in the deliverable.

This deliverable starts with an overview of the cybersecurity certification landscape at European and international levels. It presents a global analysis of cybersecurity, in general and for some specific industries. Certification schemes can help companies and other actors to prevent and mitigate cyber-attacks and their consequences. Then, we focus on the new European regulation, the European Cybersecurity Act, with a description and analysis of the cybersecurity certification framework and its current priorities. This regulation will have a large impact in the cybersecurity certification world and the European Union Agency for Cybersecurity (ENISA). In the chapter that follows, we analyse several standards and frameworks in cybersecurity certification and highlight how they can be relevant for the SPARTA project.

Recommendations for each of the four SPARTA research programs are then presented. Fifteen concrete recommendations were provided for the CAPE research program. These recommendations were aimed at creating collaboration with WP11 on the topic of certification. The final status of each of the recommendations is summarized. A summary of the collaboration with the HAIIT research program is then provided.

For the other two research programs, some cybersecurity certification schemes, and associated standards were identified. Some technologies such Artificial Intelligence for SAFAIR are less covered due to their lack of maturity regarding certification. However there was not sufficient interest in certification to develop a collaboration with the SAFAIR and T-SHARK SPARTA research programs.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

In view of the increasing digitization [1], the European Union aims at improving resilience and security of Europe's information systems by strengthening European competences as well as coordinating prevention and response across the Member States. To this end, various legislative initiatives have been developed. The Network and Information Security (NIS) directive dpotool.cs.ut.ee, which at the time of writing the updated version of this document a revision was under preparation, was introduced in 2016 to better protect the network and information systems of operators of essential services and of digital service providers. It also aims to ensure the general functioning of the crucial services for citizens and businesses [2]. In addition, the EU introduced the General Data Protection Regulation (GDPR) in 2016/2018 and the Cyber Security Act in 2019.

The GDPR is a European legislation that applies to all organizations, including SMEs or associations, that collect and personal data of European citizens. This legislation can be an opportunity for Cybersecurity and Compliance to converge [3]. If a company or association is not in line with the European regulations, it may risk heavy fines. Therefore, it is important for an organization to know exactly where personal data is stored, and how it is processed and protected.

The Cyber security Act, on the other hand, aims to increase cyber resilience by introducing an EU-wide certification framework for information and communication technology (ICT) products, services, and processes. It will provide an opportunity for Europe to play a leading role in global cybersecurity policy and governance [4] P. Lorenzo. Industry can use this new mechanism to certify products, processes and services and increase confidence in innovative digital solutions. This will give users more confidence in security of the products and services they buy. It should lower the threshold for companies to obtain certificates and to enter new markets. The European certificates under this regulation are divided into three levels of assurance: basic, substantial and high. The level varies according to the extent of cyber security testing. The EU cybersecurity certification framework is currently applicable on a voluntary basis and is not mandatory, nevertheless it brings certain responsibilities for example the setting up of relevant Authority (NCCA) and implementation into domestic legislation.

Which certificates will be developed shall be decided by the European Commission, in cooperation with various stakeholder groups and ENISA, the European Union Agency for Cybersecurity. These European certificates, issued under this regulation, will be valid in all EU Member States.

Europe, Cybersecurity and the Role of SPARTA

Europe is holding several strong positions in research and innovation, including Cybersecurity. We are pioneer in fields such as secure components or cryptography and striving to achieve excellence in other domains. Yet, we are not able to transform this excellence in large scale advantages and obtain a real edge in several competitive fields. One of the biggest strengths of Europe is its diversity but it can also be a severe disadvantage if not mastered and harnessed in the same direction. This is nothing new and numerous projects have been created to enhance the collaboration inside Europe. But the need is still there, especially in Cybersecurity, a field in constant flux and growing importance these last years.

SPARTA will setup unique collaboration capability and will help re-thinking how cybersecurity is performed in Europe, both in academia and academy. The project is aiming to form world-leading expertise centres. To achieve this, it can count on a variety of actors, dedicated to Cybersecurity but

all bringing a different set of skills in scientific excellence, technological innovation, and societal sciences.

Composed from 44 beneficiaries coming from 14 countries, the project is articulated around 14 Work Packages. Four of these WP (4, 5, 6, 7) are dedicated for research programs. They are tackling critical topic ranging from artificial intelligence to improved infrastructure. Two WP are dedicated toward the construction and organisation of the future network of expertise centres. One the WP (11) will ensure that SPARTA's roadmap and Programs are aligned with international, European and national certification program.

Other work packages are dedicated for the dissemination, awareness, roadmap design or ethics consideration.

Short description of the four research programs:

Program #1: T-SHARK – Full spectrum cybersecurity awareness:

Cyber-threats are growing in complexity, size and scope with alarming speed. In order to say ahead, new approaches need to evolve and be more comprehensive and cover a wider spectrum.

Program #2: CAPE – Continuous assessment in polymorphous environments

The IT world is increasingly complex and providing a complete and useful assessment of systems is more and more challenging. CAPE will provide new way to achieve meaningful and continuous assessments in a large variety of systems.

Program #3: HAII-T – High assurance intelligent infrastructure toolkit

IoT has open a wide new field of applications for industry and society and we are evolving toward an Intelligent Infrastructure. But new opportunities often equal new vulnerabilities that enable attackers to steal or affect sensitive data or control devices remotely

HAII-T will develop a secure-by-design development framework and a toolkit supporting the design, development, and verification of security critical, large-scale distributed Intelligent Infrastructure systems

Program #4: SAFAIR – Secure and reliable AI systems for citizen

We are facing 2 mains issues regarding AI systems: the cybersecurity area is not well developed, and we are sorely lacking regarding trust, fairness, legal and social challenges. SAFAIR will ensure a better trustworthiness of AI systems.

The SPARTA research programs will need to be in phase with the certification landscape at international, European, and national level. To achieve this, this document will deliver a comprehensive mapping of certification in cybersecurity in the following manners.

Chapter 2 introduces a global analysis of cybersecurity, the context of certification, including the European Cyber Act and several state of the art, in general and for more specific industries. Chapter 3 presents an analysis of certification schemes and standards relevant to SPARTA. Chapter 4 presents the recommendations for the SPARTA CAPE and HAIIT research programs and how they can benefit from existing certifications. Chapter 5 a summary of collaboration on the topic of cybersecurity certification with the other three pilot projects. Chapter 6 presents our conclusion and the future work. Chapter 7 contains the annexes.

Benefits of D11.1 and D11.5 for SPARTA

WP11 aims to align SPARTA certification support activities with the different European and different national cybersecurity certification initiatives. The role of task 11.1 with respect to this objective is to map international and European cybersecurity certification initiatives to understand how SPARTA research could be impacted by cybersecurity certification.

From the large number of cybersecurity schemes and associated standards described in the Annex (see Figures in section 7.3), deliverable D11.5 identifies relevant certification schemes and associated standards for the research programs. This is described in section 3. Beyond identification of schemes and standards, D11.5 provides concrete recommendations for the CAPE and HAIIT research programs. CAPE is the only research program that included certification related activities during the design of the SPARTA project and roadmap. The CAPE recommendations are described in section 4.1. CAPE is developing a set of cybersecurity assessment tools that could help make the certification evaluation process more flexible and lightweight. Developing tools to support the implementation of the EU Cyber Act is one of the objectives in support of policy implementation identified in the ECSO input to the Digital Europe Program (DEP) –2021-2027. The recommendations provided in section 4.1 aim to determine if and how the SPARTA assessment tools can support cybersecurity certification and more broadly the EU Cyber Act. Section 4.1 provides a summary of CAPE results related to each of the recommendations, illustrating the results of the collaboration between CAPE and WP11.

Beyond the recommendations for the CAPE research program, section 4.2 of D11.5 identifies certification schemes and associated standards that could be of interest to the HAIIT research program. The section reports on collaboration between HAIIT and WP11 on the topic of privacy standards and GDPR.

In section 3.2 guidance on how to compare cybersecurity certification and related standards is provided. This can be used to compare schemes and standards that are not described in chapter 3 and are listed in the general overview of existing cybersecurity schemes and associated standards presented in the annex (see Figures in section 7.3).

Contribution to the diversity of work already being done on certification in Europe

The state of the art relevant to SPARTA activities is described in section 2.3. The CAPE research program is developing a unique set of cybersecurity assessment tools that could have an impact on the way certification preparation and evaluation is carried out both at the product and process levels. At the product level integrating SPARTA assessment tools along the major software lifecycle phases is expected to produce more secure software leading to higher levels of assurance. At the process level, the use of CAPE assessment tools could enable incremental and more flexible certification evaluation processes. Achieving more flexible and lightweight product certification schemes is a key challenge that is being investigated in task 11.3. CAPE and the automotive vertical are acting as an experimental use case to investigate key cybersecurity certification challenges.

Collaborations on cybersecurity certification and use of cybersecurity standards and initiatives has been introduced also in the HAIIT research program. The participants of this program were introduced to the standards and initiatives and have considered integrating in their processes cybersecurity certification evaluation steps similar to those of the CAPE program.

Collaboration with the other three pilot projects is reported in chapter 5. Collaboration resulted in the organization of the CyberCert 2020 and 2021 workshops collocated with the IEEE European Symposium on Security and Privacy.

Chapter 2 Certification context and state of the art

2.1 General analysis of cybersecurity

Cybersecurity can be perceived as a remote concern for many companies until the first attack hit them. The impact can be staggering for many of them and the recovery, when possible, is long and costly.

The cost and frequency of cyber-attacks are increasing on a yearly basis: a report from Hiscox [5], based on a survey with 5,400 firms in the US, UK, Belgium, France, Germany, Spain, shows that in 2018, 45% of these companies report at least a cyber-attack. In 2019, that number cited in the report jumps to 61% and the cost is also increasing. Approximately three out of four businesses failed a cyber-readiness test. These numbers are bound to be incomplete as many attacks still fly under the radar.

Figure 1 shows the increasing trend of cyberattacks targeting listed companies in the EU28.

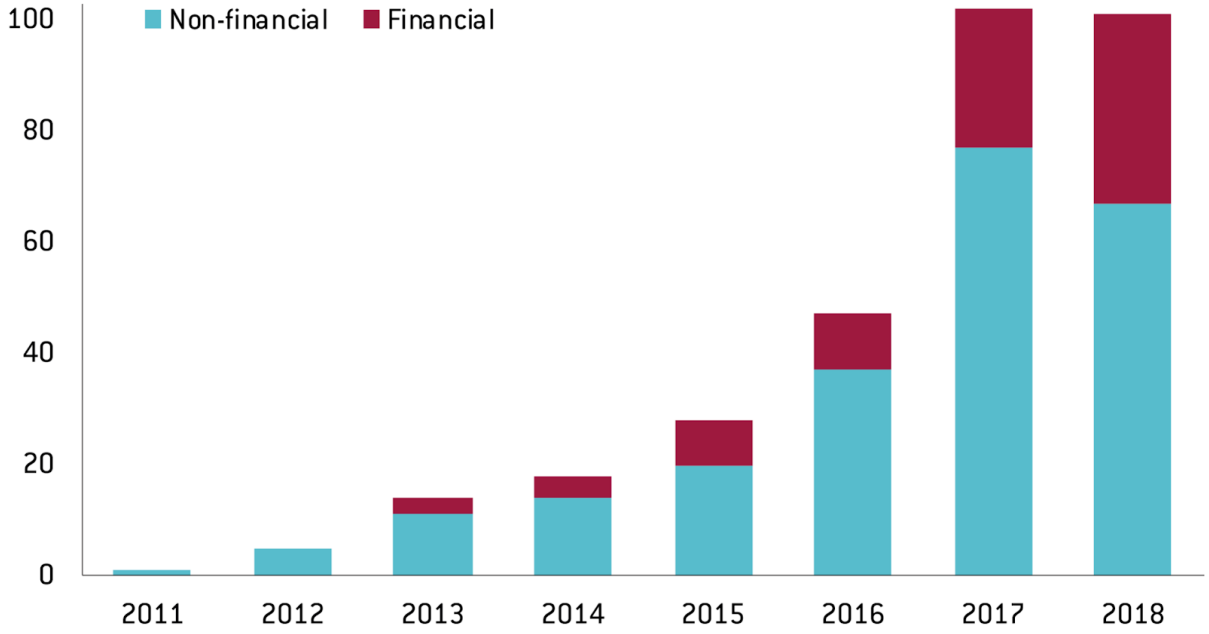

Figure 1: Number of ‘cyber-attack events’ affecting listed companies domiciled in the EU28, financial and non-financial sector, as reported by the media [6]

You can see in the Figure 2 that the medium and small companies are experiencing the worst of the situation. They are also the least well equipped on cybersecurity solution and certifications [7].

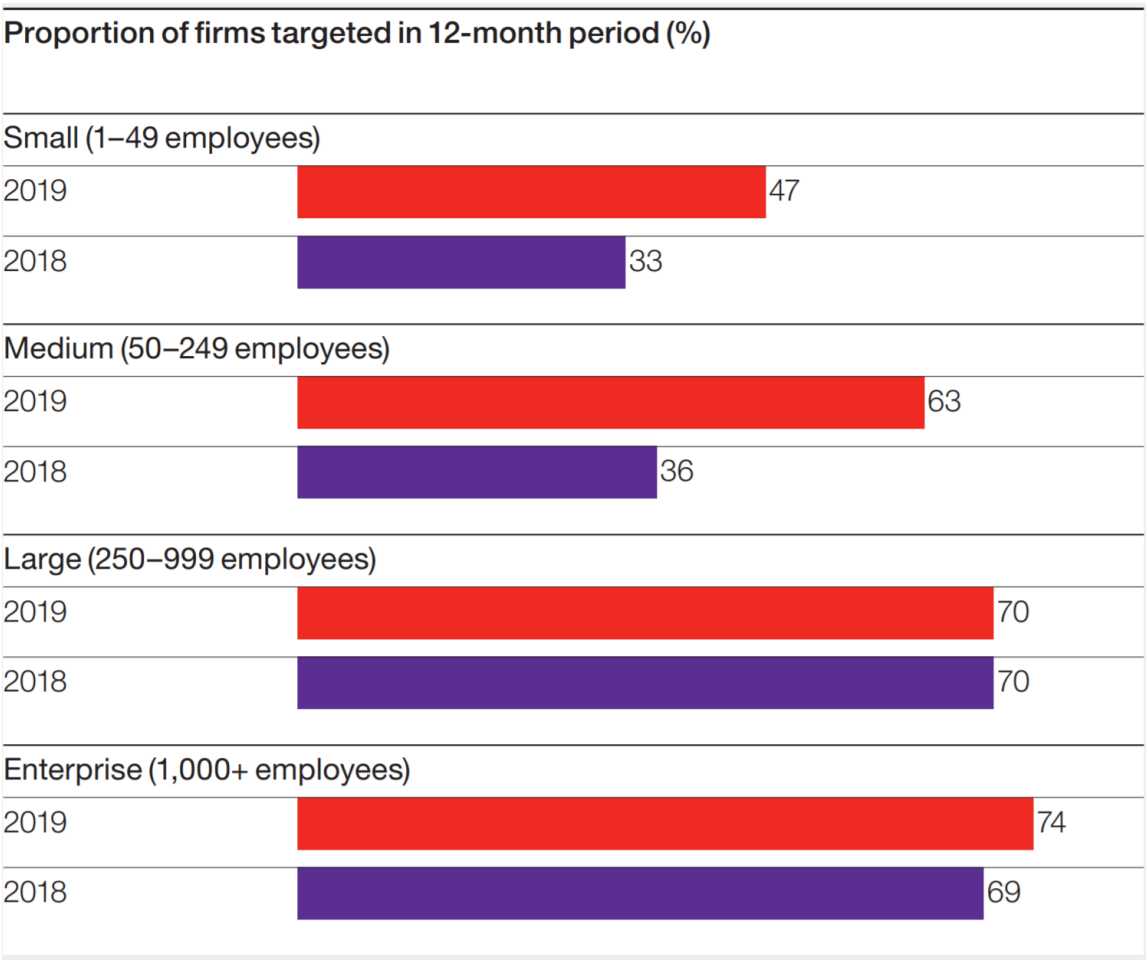

Figure 2: Proportion of firms targeted in 12-month period (%) [6]

Cyber-attacks in general are on the rise: the same report [6] as shown in the following statistics. Cyber incident has risen from 45% last year to 61%, and the figures are higher in every category of breach. The classic attacks such as worms or viruses are still working for almost a quarter of the respondent and 17% are reporting a ransomware incident. This is exactly the area where even a basic security certification can help a company of any size to be more resilient. Distributed denial-of-service (DDoS) attacks are also up from 10% to 15%. The frequency of attacks has also increased markedly during the year.

The implementation of GDPR last year has several advantages, including the fact that bigger companies– which can receive bigger penalties for non-compliance in a timely manner – to become more watchful of security incidents and to report them, partly explaining the raise of in the statistics.

Almost every industry is under an increasing wave of attacks from non-profit to the energy sector and government entities. You can see in the figure 3, below, that the almost no sectors are safe from large attacks.

Figure 3: Notable cyber-attacks in the EU28 in the year to July 2019 as reported in the press [7]

Speaking of attacks, one of the most neglected vectors is in the supply chain. When companies invest in cybersecurity, they often don't include that aspect in their contracts with their suppliers. Many companies have suffered a cyberattack where the root cause was found in a weak link in their supply chain [6].

The cybersecurity certification of smaller companies, often part of the supply chain of bigger companies or even critical operators (according to the NIS directive [8]), can improve the global security landscape et raise the global cyber hygiene [9].

The financial impact of cyber-attacks on business is also rising sharply. According to Europol, cybercrime is costing around €265 billion per year [10] and can represent almost 50% of the crime committed in some EU countries.

The landscape is now ever more complex as Sovereign states are waging cyber-wars on the internet. Some actions in the real world are now met by retaliation in the cyberspace. One of the first and most iconic occurrence is probably the Stuxnet virus, attributed to Israeli and US government and

allegedly developed to take down the industrial equipment used by Iran in nuclear exploitation. Another famous case as explained by Øverland & All [11] was the cyber-attack on the power grid in Western Ukraine, resulting in a massive blackout.

Europe is aware of these challenges and is developing several answers to tackle them. One of the biggest and latest projects, spearheaded by ENISA, is the European Cybersecurity Act.

Since June 2019, it introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes [12].

We can also cite the Directive on security of network and information systems (NIS Directive) [13], the first legislation boosting the overall level of cybersecurity in Europe especially by the creation of national CSIRT, a better cooperation and the promotion of a culture of security across vital sectors such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

We can't conclude this without speaking about the General Data Protection Regulation or GDPR [14], which has put stronger rules on data protection and regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

Even if it's not strictly cybersecurity, it helps companies to improve their data management and cyber security.

The European Commission has created the European Cybersecurity Certification Group (ECCG), a set of expert groups with the following tasks:

- The lifecycle of a European Cybersecurity Certification Scheme
- Coordination of policy approaches
- Cooperation, capacity-building, information exchange
- Peer assessment and review mechanisms
- (International) Standardisation

They are currently doing preparatory work on defining certification scheme for priority areas: Cloud Computing, IoT and Industrial Automation and Control System.

2.1.1 Cloud

Since the adoption of the European Cloud Computing Strategy in 2012 by the Commission, it never stopped promoting Cloud Computing towards companies and public administrations.

The latest iteration of that strategy [15] published in 2019 continues this path and refines the vision of the future in cloud computing for Europe.

Several actors are working to make that vision a reality, such as The Cloud Service Provider Certification Working Group (CSPCERT WG), a private and public stakeholder, created in December 2017.

Their goal, as explained by B. Larrumbide Martinez and L. Orue-Echevarria [16]] in their latest recommendations is "to establish an EU-wide framework for cybersecurity certification of ICT services, products and processes, including those services provisioned by Cloud Service Providers (CSP)".

This working group has been a crucial provider of multiples recommendation, linked to the security certification of cloud services, for the Member States, ENISA, and Commission.

Their work is articulated around three main milestones, as described in their recommendation:

- "The security objectives that an EU-wide certification shall include, based on existing standards, best practices and schemes"
- "A comparative analysis of the most relevant conformity assessment methodologies"
- "A document, the result of the 2 previous milestones, formulating recommendations toward the European Commission and the ENISA for establishing an EU-wide cloud certification scheme"

ENISA has been officially tasked by the Commission to prepare a cybersecurity certification candidate scheme for cloud services and will communicate soon on the necessary steps to achieve it.

2.1.2 IoT

The Internet of Thing, as defined by ENISA, is "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making". It is one of the fastest growing segments of the internet. It enables connectivity between devices who are gathering, transmit and receive data. It is the equivalent of the World Wide Web but for smart machines.

The existing IoT devices can be almost anything from routers, thermostats, kitchen appliance webcams, printers, sensors, to devices powered by Amazon Alexa our Google Assistant. The next wave of devices will be even more complex and interconnected with infotainment systems, medical devices, navigation in vehicles etc.

The security risks are tremendous for 3 main reasons:

- The number of devices is growing exponentially, the number of "machines-to-machines" were estimated around 500 million in 2014 [19] and early 2019 the numbers were around 7.5 billion, forecasted to triple by 2021 [20]
- They are collecting, sharing, and processing myriads of sensible information on users, processes and products. Personal assistant such as Amazon Alexa or Google home, is hacked, are literally a wealth of information for malicious actors and they are already in almost 12% of European houses [21].
- The impact of a vulnerability, even an old one, in network of this magnitude can be potentially devastating: a 10-year-old vulnerability left around half a billion of IoT devices vulnerable and sometimes difficult to patch [22]

The number of attacks is also increasing at a furious pace with a surge of 300% in 2019, for a staggering 2.9 billion of events recorded by F-Secure (2019) and their honeypot network.

All this only shows that an effective security is primordial and one of the best ways to achieve this is via a strong certification scheme. Europe through ENISA is working on such initiatives, like the European Cybersecurity Act.

It will have a decisive role to play to bring a cybersecurity scheme specifically designed for the IoT world. The New Legislative Framework (NLF) will also help to improve the situation, it aims to set mandatory product safety requirements that are necessary to put products on the EU market (CE marking) and is looking at how to include cybersecurity in the process.

2.1.3 Industrial systems

The world is now entering in the fourth industrial revolution, based on cyber-physical systems or IoT. According to Frost & Sullivan [23], manufacturing companies around the world are looking for operational efficiency, productivity, and customization features. Industry 4.0 provides processes and tools to deal with huge data volumes, improving communication between physical and digital environments

Industry 4.0 needs interconnection to provide the most benefits. Connections between partners, customers, employees, systems, and sensors enable new opportunities and improved business performances.

This interconnection also brings some concerning issues, Industry 4.0, which rely on IoT, is facing the same problems seen in the previous paragraph with even more dire consequences in case of successful cyber-attacks. They are also following the increased rhythm of evolution in strength and complexity that “classic” cyber-attacks.

Their aim was mainly to steal money, disrupt industrial activity or gather information on competitors.

To stay ahead of the threats, security budgets are expected to grow exponentially, and the industrial world is no exception.

It can be even more challenging due to the (often) aging infrastructure, obscure protocols and a culture based on safety and not cybersecurity first.

As explained in the ISACA’s [24] document, the field of Information Technology (IT) and Operational technology (OT) need to converge to provide efficient answers to the rising threats the sector is facing as shown in Figure 4.

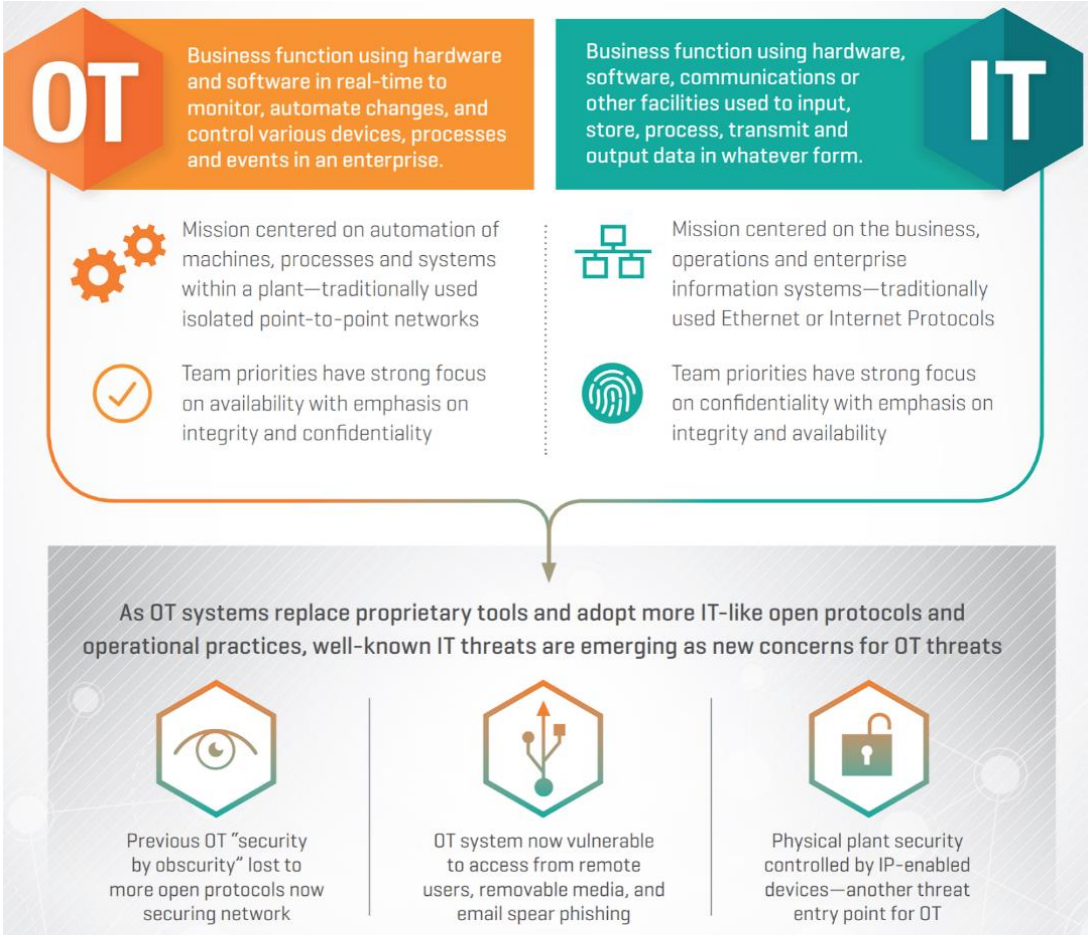

Figure 4: OT and IT convergence [24]

Several initiatives such as the IACS Cybersecurity Certification Framework [25] (ICCF) is an initiative supporting the implementation of the European Cybersecurity Certification Framework for Industrial Automation and Control Systems (IACS)

ICCF will, in the timeline shown in Figure 5:

- Elaborate the ECCS (Scheme) for IACS products (the "ICCS") with stakeholders
- Deliver the support processes and guidelines for an ICCS
- Generalise to an "ECCS engineering process & guidelines"
- Document findings & recommendations for the benefit of DG CONNECT & ENISA
- Contribute to the Union Rolling Work Program for European Cybersecurity Certification

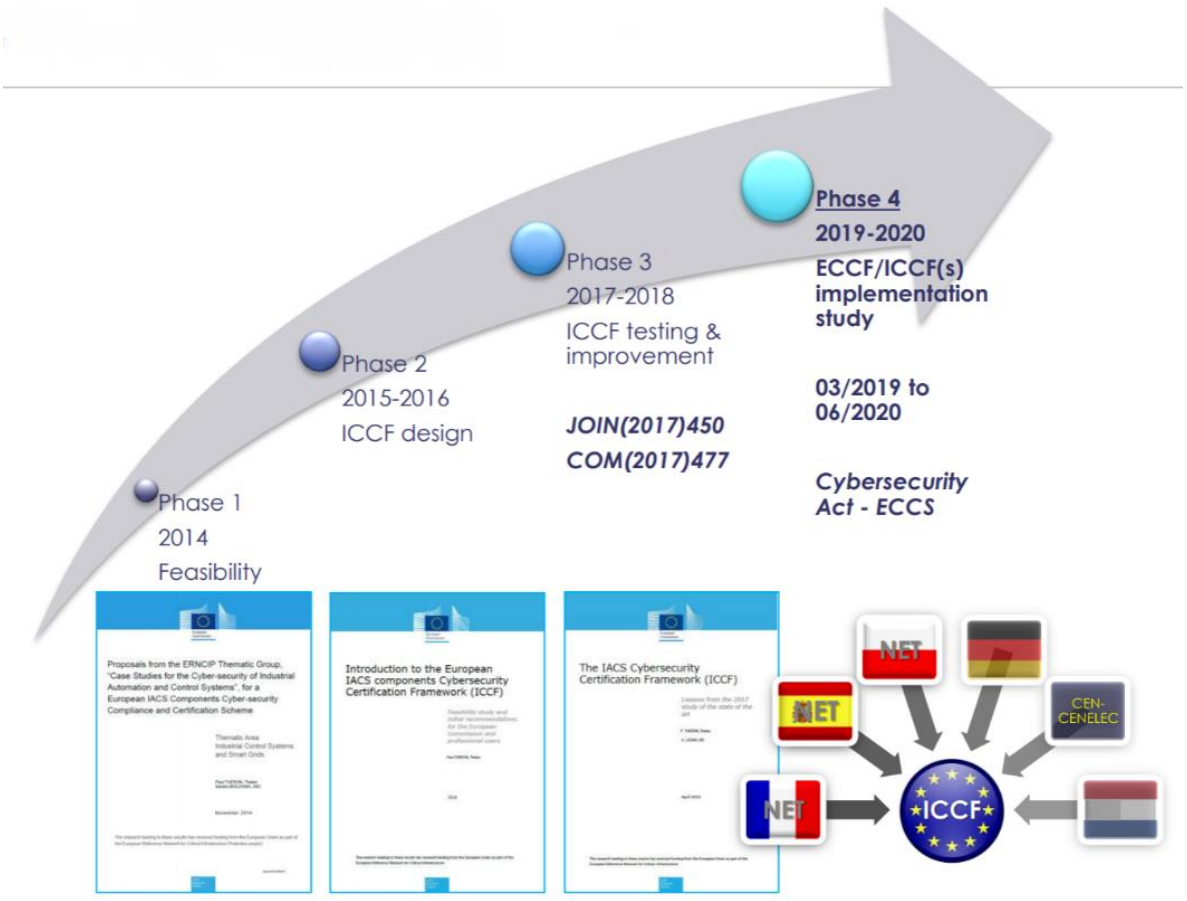

Figure 5: Actual state of ICCF [26]

2.2 European Cybersecurity Act

The EU Cybersecurity Act, effective since June 2019, revamps and strengthens the European Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services, and processes. This is translated in these two main items:

A new mandate for ENISA

ENISA, the European Union Agency for cybersecurity, has received from the EU Cybersecurity Act a permanent mandate, more resources, and more tasks to perform.

ENISA will have an essential role in the creation of the European certification cybersecurity framework by preparing the technical aspects for specific certification schemes and informing the public on the certification schemes

The agency is also now responsible of helping, if requested, EU Members States regarding cybersecurity incidents, ENISA will also support the coordination, in the EU, of any large-scale and cross borders incidents. This is summed up in Figure 6.

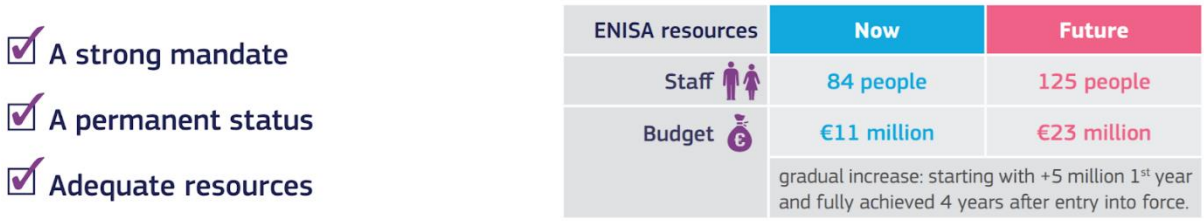

Figure 6: The "new" ENISA [27]

A European cybersecurity certification framework

The EU Cybersecurity Act introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services, and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognized across the European Union." [28]

2.2.1 General objectives

Certification is playing a major role in increasing trust and security in products and services.

This is crucial for Europe and the Digital Single Market. Right now, there are many different security certification schemes for ICT product co-existing in the EU. This situation is creating potential barriers and fragmentation in the single market. The European Cybersecurity Act is the answer to this situation and ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products and services.

It is important to signal that for the coverage of the EU Cybersecurity Act is quite stunning if you look at these definitions:

- Article 2(9) A European cybersecurity certification scheme "means 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."
- Article 2(11) A European cybersecurity certificate "means a document issued by a relevant body, attesting that a given ICT product, ICT service, or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme."
- Article 2(12), ICT product "means an element or a group of elements of a network or information system."
- Article 2(13), ICT service "means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems."
- Article 2(14), ICT process "means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service."

2.2.2 EU Cybersecurity Certification Framework

The process

National cybersecurity authorities take part in the European Cybersecurity Certification Group (ECCG), chaired by the European Commission. The Commission, with their help, will identify the strategic priorities for future European cybersecurity certification schemes.

These future schemes will then be prepared by ENISA or (exceptionally) the ECCG. During the preparation of a candidate scheme, ENISA will create an open, transparent, formal and inclusive consultation process. The agency will then put in place an ad hoc working group per scheme (see article 20(4) of the regulation) to gather the needed expertise and recommendations

Each scheme will have to comply to a comprehensive set of rules, technical requirements, standards and procedures.

The Commission, based on the scheme elaborated as described before, may adopt implementing acts providing for European cybersecurity certification schemes for ICT products, services and processes.

ENISA is also responsible to review each adopted scheme at least every 5 year, taking into account the feedback from relevant stakeholders.

The decision of certifying a product, process or service against a certification scheme is not mandatory. However, it is still possible that, in the future, the EU legislation will prescribe a mandatory certification for certain category of products or services.

Assurance Level

As described in the regulation [29] (article 52), a European cybersecurity certification scheme may specify one or more assurance levels for ICT products, services, and processes. The assurance level must be proportionate with the appropriated risk level related to the intended use of the product, service, or process.

The level of assurances is basic, substantial, and high. Each of them has their own set of security requirements, linked to security functionalities and the amount of effort needed to assess the product, service, or process.

Basic

The “basic” level of assurance will ensure that the product, service or process meet the defined security requirements and that enough effort have been put in the evaluation. It shall at least minimize the known basic risk of incidents and cyberattacks. The technical documentation needs also to be reviewed during the evaluation process.

Substantial

The “substantial” level of assurance will ensure that the product, service or process meet the defined security requirements and that enough effort have been put in the evaluation. It shall at least minimize the known cybersecurity risks and the risks of incidents or cyberattacks performed by attackers will a limited skill set and resources. At least the two following steps need to be performed during the evaluation process: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the products, services, or processes correctly implement the necessary security functionalities.

High

The “high” level of assurance will ensure that the product, service or process meet the defined security requirements and that enough effort have been put in the evaluation. It shall at least minimize the risks of sophisticated cyberattacks performed by skilled actors backed by significant resources. At least the following steps need to be performed during the evaluation process: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the products, services or 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.

2.2.3 Current priorities

The EU Cyber Act cannot cover every topic at once, even is several sectors are in needs of EU-wide certification. So far, the work is ongoing or will start soon on the following topics: Common Criteria and SOG-IS MRA, Cloud Computing, Industrial Automation and Control Systems, IoT, Software and system security lifecycle management and the Healthcare sector (IoT and safety/security implication).

2.3 State of the art related to CAPE activities

2.3.1 Lightweight certification

Not all products and services require the level of assurance delivered by a full certification schemes such as ISO/IEC 15408 Common Criteria. There is a need for more cost-effective approaches with a predictable time frame (“fixed time evaluation”) so that products can be delivered with a sufficient level of assurance regarding how security is handled and implemented.

Several national cybersecurity schemes are already offering a response to that need in the form of evaluation methodologies based on simplified approaches to The Common Criteria. Below is a summary of a few of them and a short comparison in Table 1.

- LINCE (Spain): This is an evaluation and certification methodology for ICT security products. It has been developed by the Spanish CCN (National Cryptologic Center) with a strong focus on secure information handling. This scheme is designed for products requiring low or medium certification in security. The evaluation process is focused on vulnerability analysis and penetration testing.
- CSPN (France): The first level security certification was introduced by ANSSI (The National Cybersecurity Agency of France) to provide an alternative to The Common Criteria in order to estimate the resistance of a product to a moderate level of attack. The assessment is less exhaustive than CC certification and places a greater emphasis on product analysis. The tests are done under time and workload constraints.
- BSZ (Germany): The Accelerated Security Certification, developed by the Federal Office for Information, Security trades the flexibility of CC for a more constrained time frame and reduced documents requirements. The certification is a combination of conformity testing and penetration testing. The installation guide and cryptography are also evaluated.
- BSPA (Netherlands): The Dutch BSPA is managed by the Netherlands National Communications Security Agency (NLCSA). It is inspired by the French CSPN and like it, focuses on hardware and software security products for the sensitive, but unclassified domain. The only requirements for an evaluation are an installed, working product and the accompanying documentation.

Table 1: Global comparison between lightweight certification schemes [30]

Criteria	LINCE	CSPN	BSPA	BSZ
Workload	25 man/days	25 man/days	25 man/days	25 man/days
Calendar Duration	8 weeks + 2 weeks per additional modules	8 weeks	8 weeks	No constraints
Optional Modules	Crypto evaluation and source code review	No	No	No
Lab Accreditation	Follow the CC Process. ISO17025 and Pilot evaluation are required.	Specific Procedure. ISO17025 is not required. Pilot evaluation is required.	Specific Procedure. ISO17025 is not required. Pilot evaluation is required.	Specific Procedure. ISO17025 is require. Pilot evaluation is required.
Required Evidences	- Security Target - Operational and installation Guidance - Testing Environment - Product Samples - Source Code (if module chosen) - Crypto Information (if module chosen)	- Security Target - Operational and installation Guidance - Crypto Information - Product Samples	- Security Target - Operational and installation Guidance - Testing Environment - Product Samples - Public Information	- Security Target - Operational and installation Guidance - Product Samples (3 copies) - Crypto Information - copy of the unencrypted firmware - an overview of the principle design of the TOE and the libraries used - a brief technical description of the update mechanism
Steps	- Security Target analysis	- Security Target analysis - Product installation	- Conformity analysis	- Review the toe, the cryptography,

Criteria	LINCE	CSPN	BSPA	BSZ
	- Product installation - Functional tests - Vulnerability analysis - Source code review (if module) - Cryptography evaluation (if module) - Penetration testing	- Documentation analysis - Source code review (if available) - Functional tests - Resistance of the mechanisms/functions - Vulnerability analysis - Host system vulnerability analysis - Ease of use analysis - Cryptography evaluation (if the product implements cryptographic mechanisms)	- Strength analysis - Host system vulnerability analysis - Deployment advisory	and the Security Targett - Estimate the evaluation - Evaluate the secure user guide - Evaluate the conformity - Evaluate the resistance (vulnerability analysis and testing) - Cryptography evaluation
Documentation review	Yes	Yes	Yes	Yes
Product Installation	Yes	Yes	Yes	Yes
Source Code Review	Optional	Yes	No	Yes for crypto
Security Functionality Testing	Yes	Yes	Yes	Yes
Vulnerability Analysis	Yes	Yes	Yes	Yes
Penetration Testing	Yes	Yes	Yes	Yes
Ease of Use Analysis	No	Yes	No	No
Impact assessment on the security of the host system	No	Yes	Yes	No

2.3.2 Integration of certification in development process

In recent years, the need to improve software delivery in terms of speed and quality has given rise to a set of practices that combine continuous build, testing, integration, delivery, ... The DevOps approach, closely related to Agile software development method, combines software development (”Dev”) and operations (”Ops”) processes to ensure that new features are added to a software solution in the shortest time possible, and with a high level of quality.

This approach, some even speak of culture, emphasizes the importance of communication between the involved parties, including the whole production chain: developers, sys-admins, network team, … One of the goals is to break the classic “silos” of specialists and keep channels of communication open.

The DevOps approach itself can be complemented with security procedures to ensure continuous security assessment. It is then called DevSecOps. DevOps is focused on producing quality code, quickly and reliably. It’s aiming toward increasing release velocity and reducing the time to market for applications and products. The security problem was not directly addressed in this approach and DevSecOps is aiming to correct that fact as illustrated in Figure 7.

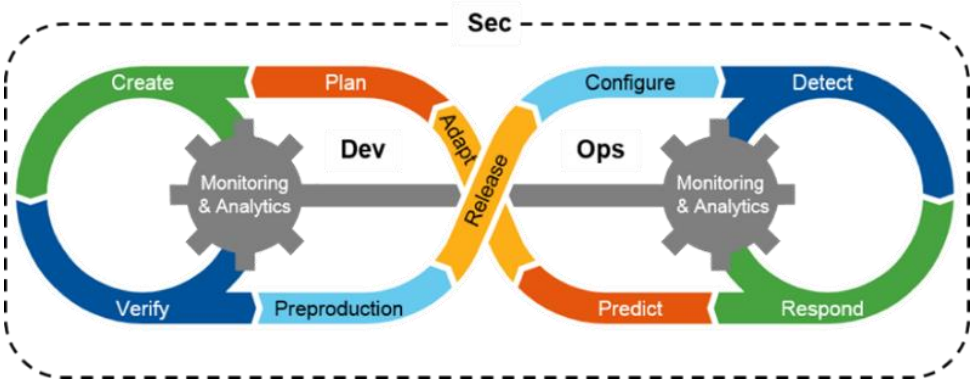

Figure 7: DevSecOps lifecycle [31]

Even before DevOps, security processes were often isolated and given to a dedicated team. This is not working in the actual context and security needs to be addressed and taken care of by all the links of the production chain.

As described by N. Tomas [32], security is now a shared responsibility between all the actors of a project, at every stage of the software development lifecycle. To reach that goal, cybersecurity has to be taken into account from the very beginning and several tools will be needed, along with a good deal of automation. A well-designed environment of continuous integration is a heavy investment but can provide many benefits. But DevSecOps, and DevOps, is not only about tooling but also about changing mentality and bad habits.

DevSecOps could be a perfect opportunity to establish a certification program in a development process. With the multiple automated checkpoints and the improved channels of communication between teams, this is a perfect opportunity to raise the level of maturity and prepare the needed documentation for almost any certification.

2.3.3 Safety/Security certification

Safety and cybersecurity engineering have followed different paths mainly due to the reason that safety critical systems were seldom connected and were thus not subject to cybersecurity threats. Now that safety critical systems are becoming more and more connected, they need to be protected from cybersecurity threats. As described in [33] safety and security have developed their own separate engineering methods. Now that many critical embedded systems are connected, safety

and security engineering need to evolve towards co-engineering. Two European research projects have worked in this area: AMASS [34] and AQUAS [35]. AMASS created a platform for assurance and certification to reduce certification costs of CPS when faced with rapidly changing features and market needs. One of the results of AMASS is the OpenCert tool. It is one of the tools being extended in the CAPE research program. AQUAS follows a holistic approach to Safety/Security/Performance Co-Engineering (CE) through a domain-flexible framework, that supports the entire Product Life-cycle. Some safety certification schemes such as ISO 26262 have attempted to make extensions to include cybersecurity. Parallel efforts such as SAE J3061 provide guidance on cybersecurity and reference ISO 26262.

2.3.4 Certification monitoring

A certification process is, in most cases, certifying a snapshot of a product or services. The version considered for certification is frozen and a new or patched version will need again to go through a complete certification process “Assurance Continuity” as agreed by Common Criteria Recognition Arrangement (CCRA)[75].

This can be a huge hindrance for any companies willing to certify their products, especially software based.

One solution can be to improve the monitoring and the quality control processes. That way, it is possible to prove that the level of security stays at the same level during the whole development process and respect at any time the conditions to be certified.

Via an efficient monitoring, we can continuously monitor and evaluate the certification criteria through the automation of metrics gathering and checks. All this information can be gathered in dashboards to display and manage the certification activities status with alerting capabilities when diverging from the parameters acceptable for certification.

The Cloud Security Alliance (CSA) is building a "Continuous Certification" scheme in the area of Cloud Computing. A working group is working on the definition of security attributes and metrics associated with the control objectives defined within the Cloud Control Matrix (CCM).

2.3.5 Process certification

Software quality is becoming increasingly important as our society and companies become more and more dependent on computers to perform reliably. To achieve the required level of quality, the software development process needs proper attention, often formalized via certification. This is especially important for critical sectors (defence, aerospace, rail...). Three major process certification frameworks, standards and models are described below.

CMMI: Capability Maturity Model Integration was developed by Carnegie Mellon University to make maturity models (which measure the ability of organizations to have ongoing improvement in a particular area). The first version was released in 2002 and is still being actively developed. It helps organizations in their process improvement and the development of behaviour that decrease risks in service, product, and software development. An organisation can decide to undertake a CCMI appraisal, to evaluate how the organization’s processes compare to CMMI best practices and to determine areas of improvement.

The rigor and cost of the appraisal may vary, following the type selected, ranging for the quicker class C to the formal Class A. It can:

- Help organizations with the development of an improvement strategy that prioritizes key issues.
- Help to mitigate risks.

- Showcases the soundness of organizational processes by having results available in the Published Appraisal Results site.
- Provides the organization with a CMMI maturity level (only A class appraisal).

After a class A appraisal, the organization will receive a CMMI maturity level, ranging from 1 to 5.

1. Initial: processes are seen as unpredictable, poorly controlled, and reactive. Businesses in this stage have an unpredictable environment that leads to increased risks and inefficiency.

2. Managed: processes are characterized by projects and are frequently reactive.

3. Defined: processes are well-characterized and well-understood. The organization is more proactive than reactive, and there are organization-wide standards that provide guidance.

4. Quantitatively Managed: processes are measured and controlled. The organization is using quantitative data to implement predictable processes that meet organizational goals.

5. Optimizing: processes are stable and flexible. The organizational focus is on continued improvement and responding to changes.

COBIT 5: This is an IT governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues, and business risk.

COBIT enables [37] the development of clear policy and good practice for IT controls across the organization. It emphasizes regulatory compliance and helps organisations to increase the value created from IT.

It is based on 5 principles (figure 8) and 7 enablers (figure 9):

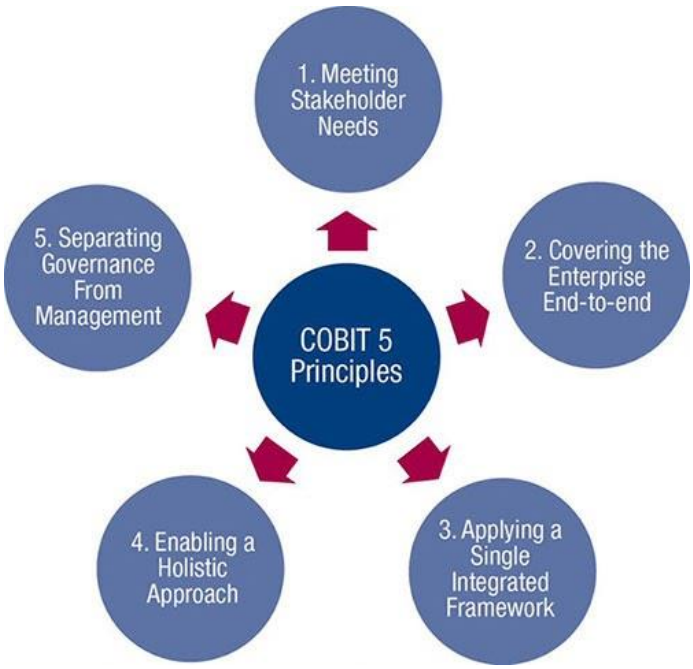

Figure 8: COBIT 5 Principles [36]

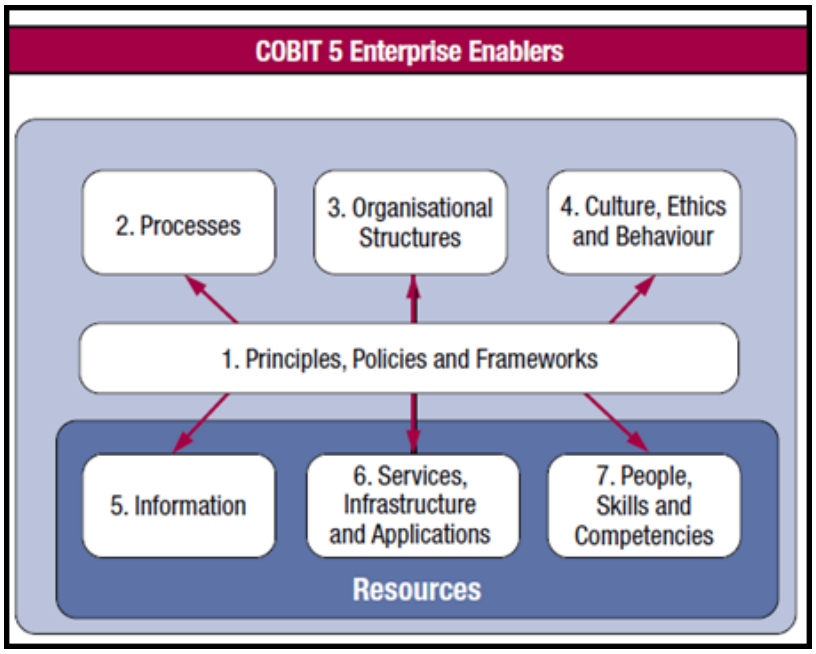

Figure 9: COBIT 5 Enablers [37]

COBIT 5 puts a strong emphasis on the following key areas to address the common issues related to software development:

- Awareness & training
- Assessment & audit
- Development & Quality Assurance
- Response Management
- Metrics & Accountability
- Operational Security

It can provide a holistic and business-oriented approach to managing information security and software development while providing a common language between IT and Business departments.

ISO/IEC 27034: This standard (who will be used in the WP5, Task 5.3) provides guidance to assist organizations in integrating security into the processes used for managing their applications. It gives guidance on how to specify, design, program, implement and use application systems with information security in mind.

It is a multi-part standard, process oriented, dedicated to place information security controls in the heart of an organization's Systems Development Life Cycle/s (SDLC).

It addresses all aspects from determining information security requirements to how to prevent unauthorized use of an application. This standard is method agnostic regarding SDLC and is written to be applicable with most of them.

It puts a strong emphasis on the early phases of software development: specification, design, testing and reusability. You can summarize it by "Do it properly, do it once and reuse it often".

There are three main concepts in ISO/IEC 27034:

- **Application Security Control (ASC)** is a control put in place to prevent a security weakness in an application. Each ASC is relevant to a particular application in a particular context (technical, regulatory or business).
- **Application Level of Trust** is determined at the creation of an application. Not all applications have the same need of security controls and the level of trust will helps determine the number and severity of these controls
- **Organization Normative Framework (ONF)**. It is a company or project-wide repository of Application Security Controls and processes. This allows the ASC to be stored and updated alongside the relevant process.

2.3.6 SME Certification scheme

The place of SMEs is easily downplayed in the world of Cybersecurity. However, according to the European Cyber Security Organisation [38], on the 60.000 companies in the EU cybersecurity market, 98% of them are SMEs and start-ups. They are often located in niche markets and lack the capacity to scale up their business [39]. In a context where many actors can and will ask for companies, products and services to undergo different certification process, certification schemes adapted for SMEs can make a real difference.

We have done a survey on cybersecurity labels and frameworks accessible for SMEs in Europe and a comparison of the different schemes we have studied as described in Figure 10.

	CyberEssentials	ANSSI certification	BSI	VDS	Italy National Framework	ISO27001	NIST CSF	ISSA 5173	SANS Top 20
Type	Label	Label	Recommandation	Certification (private)	Framework	Standard	Framework	Standard	Good practices
Country	UK	France	Germany	Germany	Italy	International	US/Intenational	UK	US/International
website	http://www.cyberessentials.org/	https://www.ssi.gouv.fr/uploads/2014/10/certification_en.pdf	https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html	https://www.vds-quick-check.de/en/	https://www.cyberwiser.eu/italy-it	https://www.iso.org/fr/isoiec-27001-information-security.html	https://www.nist.gov/cyberframework	does not seem available	https://www.sans.org/critical-security-controls
Organisation	UK Government	ANSSI	German Government	VdS	CLUSIT	ISO	NIST	ISSA	Center of Internet Security
SME	Yes	Yes	Yes	Yes	Includes SME guidelines and contextualization	No (guidelines)	Adaptation provided	Yes	Yes
Controls	5 main controls - Firewalls/gateways - Secure config - Access control - Malware protect. - Patch mngmt		Based on the ISO 2700x family	4 areas - Organisation - Technology - Prevention - Management (39 quick checks)	Based in NIST CSF 11 operational guidelines	130 individual security controls grouped into 11 key areas	5 functions - identify - protect - detect - respond - Recover	about 10 categories	20 controls
Available tool	Online self assessment		Threat catalogue to "Elementary Threats"	Online self assessment		Many ISMS tools available	CSF Reference Tool (Windows/Mac OS)		Lot of tool providing control automation
Scheme	Certifying Bodies licensed by accreditation Bodies by UK government.	Based on common criteria		Certification body approving service providers for limited time.					
Levels (maturity or progress)	2 levels of badges	2 levels: "first level" and then Common Criteria with different EALs		4 levels	4 levels		4 tiers	3 maturity levels	First 5 and then all the 20
Started in	2013	2015	2008	2017	2015	2013 (current)	2014	2011	2008

Figure 10: Comparison of main SME-oriented approaches

They are multiple solutions currently operating in European countries, but SMEs are still lacking a unified certification scheme dedicated to their needs. The EU Cybersecurity Act, initiated by the European Commission will help to mitigate this issue and provide a comprehensive, EU-wide

framework for the certification of ICT products, services, and processes. It is still on a voluntary basis, but it can help by harmonizing cybersecurity certification across Europe and removing existing barriers that prevent SMEs from scaling up and doing business across borders.

Chapter 3 Analysis of certification schemes and standards relevant to SPARTA

3.1 Definitions and differences (organisation vs implementation)

This section begins by giving some precisions on standards and frameworks. There can be differences in many areas like coverage, certification, visibility, recognition, or the robustness of the controls described.

It is important to first define what is exactly needed in a project and why, to choose the right scheme before going too far. Some of them request a heavy investment in time and resources, and thus should be only applied when needed. A proper use of these standards and frameworks can bring an insurance of quality and a recognition impossible to achieve otherwise.

3.1.1 International standard

According to the International Organization for Standardization (ISO) [40], an International Standard provides rules, guidelines, or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context and ensure interoperability. It can take many forms. Apart from product standards, other examples include test methods, codes of practice, guideline standards and management systems standards. We can cite the ISO standards family, IETF standards, Cipher suite, the ANSI/SIA standards series…

3.1.2 Cybersecurity framework

In our context, a Cybersecurity framework provides voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk such as the NIST CSF Framework or Industrial Internet of Things Security Framework.

Another way to define these standards and frameworks is to examine how they are providing assistance or recommendations. We can distinguish two main categories:

3.1.2.1 Management level assistance

These standards and frameworks are focusing on the company level. They are mainly helping on the topics of organization, process management, compliance, and risk management. They can provide a common language between the IT and Business department of a company, allowing a better comprehension between them. They will not provide technical guidance or technical controls and are for most of them technology agnostic. We can cite COBIT 5, ISO 27001, NIST, ISO 27034, and others.

3.1.2.2 Implementation guidance

They provide technical guidance regarding the correct implementation of security controls in an organization or project. They will give detailed information to technical teams looking to fix a particular security issue or raise the general level of security. We can cite the CIS 20 controls as a prime example.

3.2 Method for comparing cybersecurity certification schemes and associated standards

The area of software cybersecurity certification and associated standards has been driven by many independent and parallel efforts over several decades resulting in a complex set of cybersecurity certification schemes and standards. Whether the motivation is to identify schemes and standards that could improve protection levels of one's products, processes or organisations, to improve existing schemes and standards or create new ones, it is often useful to compare existing schemes and standards.

Cybersecurity certification schemes and standards can be categorised in different manners to compare them. In [41] a model for designing certification schemes is presented and proposes three broad categories to compare certification schemes and standards: reach, scope and enforcements methods:

- Reach: includes different criteria such as country (global or country), Government issued or not, industrial sector (global or specific sector)
- Scope: includes criteria such as principles, policies, guidelines, standards, or practices
- Enforcement methods: includes criteria such as tests or audits, and certification (mandatory) compliance (voluntary)

If we take the example of Common Criteria in Figure 11 it would then be classified as follows (reproduced from an article of Warren Axelrod [41]):

Names of "Standards"	Reach				Scope					Enforcement Methods	
	Country	Gov't	Non-Gov't	Sector Industry	Prin-ciples	Pol-icies	Guide-lines	Standards	Prac-tices	Tests Audits	Certification Compliance
Common Criteria [5]	Global	Yes	No	Number of Governments	No	No	Yes	Yes	No	Tests	Certification

Figure 11: Common Criteria example

More structured approaches for comparison of standards in general have been investigated. In [42] the authors present FACTS, a Framework for Analysis, Comparison and Testing of Standards. The framework itself is based on the Zachman framework to compare standards by separating two dimensions: stakeholder concerns, and technical analysis. FACTS facilitates the comparison of standards and helps to identify gaps and overlaps between them.

In this article [43], the authors compare standards and certifications schemes aimed at SME. To this end the authors selected the following criteria for comparison:

Table 2: Criteria used for comparison for SME's approaches

Criteria	Value
Type	Is it a label, a certification, a recommendation, a framework, a standard, a set of good practices?
Country	Country of origin
Website	Official website
Organisation	Organisation responsible of the initiative
SME	Is it tailored for SME's needs?
Controls	Are there any specific security controls?

Criteria	Value
Available tools	Is there specific tooling provided?
Scheme	Short description of how the scheme is organized
Level of maturity or progress	Is the scheme can be divided in multiple levels?
Starting date	Since when the scheme is operating

In the table below we present frequently used criteria that cane used to create customs comparisons of certification schemes and associated for different purposes. The criteria are grouped into the following categories: Administrative, targeted systems, contents of scheme or standard, application and certification.

Table 3: Criteria used for our comparison method

Criteria	Domain of values	Description
Administrative		
Issuer	Professional organisation, Government, Country	What is the nature of the entity defining the certification scheme?
Sector	Global, sector specific	Is the certification dedicated to a specific sector?
Targeted systems		
Scope	products, processes, organisation, personnel...	The scope of the scheme can be products/services, processes, organisation level, IT personnel competences.
Type of companies or individuals	SME, large companies, government entities, cybersecurity professionals	Is the target of the certification a large, medium, small companies, the government...?
Technology areas covered	Cloud, IoT, network, artificial intelligence, …	Some schemes and standards are specific to technologies
Phases of software lifecycle covered	Complete lifecycle, Requirements, architecture, unit tests, integration tests, deployment, …	Is the software development process part considered in the scheme?
Contents of Scheme or standard		
Certification, technical standard, security framework or technical guidance	Certification, technical standard, technical guidance	Is it a formal attestation, a formal document describing an established norm, a voluntary guidance or a guide helping to implement technical solution?

Criteria	Domain of values	Description
Structure of scheme	fixed, extensible, general/specialised	Is the certification scheme fixed? Can it be extended in some ways? Can it be specialised?
References to other certification schemes or standards	List of referenced schemes or standards	Some schemes and standards make references to each other.
Application of scheme or standard		
Workload	Light, time-consuming	Is the certification scheme lightweight, or does it require a time-consuming process? This may depend on the level of certification
Certification		
Frequency of re-certification	Frequent, infrequent	How frequently certification has to be redone?
Incremental certification	Yes, No, Planned	Is it possible to certify incrementally?
Continuous auditing and certification	yes, No, Planned	Is monitoring and continuous certification possible?
Insurance scheme associated with certification	yes, no, planned	Is cybersecurity risk insurance linked to the certification?
Non-compliance	Yes, no	Are there consequences in case of non-compliance?
Types of certification	Self-certification, certification by external auditor, continuous certification, on- site, external location	How, by who and where is the certification verified?
Different levels of certification	Yes, No	Some certification schemes have different levels of certification, such as Common criteria that has seven different Evaluation Assurance Levels (EAL).
Conformance	Mandatory, voluntary	Is the certification scheme mandatory or voluntary? It may also depend on the level of certification.

To illustrate how the above table of criteria can be used, it is used below to compare ISO 27001, the NIST CSF and ISO/IEC 15408 Common Criteria:

Table 4: Comparison between SO 27001, the NIST CSF and ISO/IEC 15408 Common Criteria

Criteria	ISO27001	NIST CSF	ISO/IEC 15408 Common Criteria
Administrative			
Issuer	ISO/IEC	NIST	CCRA/SOG-IS
Sector	Global	Global	Global
Targeted systems			
Scope	Organisations, processes	Organisations, processes, SME's	Processes, products and services
Type of companies or individuals	Large companies, government entities	Large companies, government entities, SME's	Large companies, Defence industry, Aerospace industry, heavily regulated sectors
Technology areas covered	Management system for Information security	Five security functions: Identify, Protect, Detect, Respond, and Recover	Computer security products and systems
Phases of software lifecycle covered	no	Yes	Yes
Contents of Scheme or standard			
Certification, technical standard, security framework or technical guidance	Certification	Security Framework	Certification
Structure of scheme	Fixed and general	Fixed and general	Fixed and specialized
References to other certification schemes or standards	ISO 2700X family	Via the Informative Reference Catalogue	ISO standards
Application of scheme or standard			
Workload	Six to twelve months	Several weeks to a year depending on the scope	Nine to twelve months
Certification			
Frequency of re-certification	Every three years	N/A	5 Years
Incremental certification	No	N/A	Yes
Continuous auditing and certification	No	N/A	No

Criteria	ISO27001	NIST CSF	ISO/IEC 15408 Common Criteria
Insurance scheme associated with certification	No	No	No
Non-compliance	Certification removed	N/A	Certification removed
Types of certification	Certification by external auditors	N/A	Certification by external testers in specialized laboratories
Different levels of certification	No	N/A	Yes, EAL level 1 to 7
Conformance	Voluntary	Voluntary	Voluntary

Figure 12 below gives a view of the main concepts currently defined in the certification model:

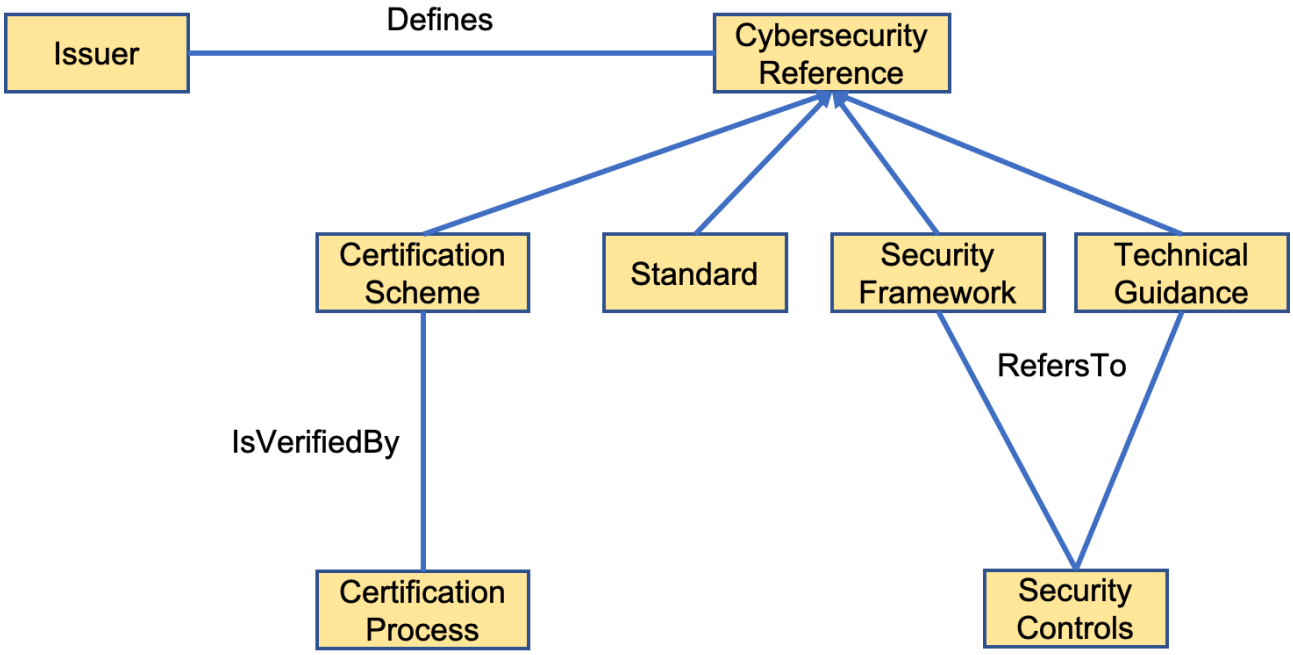

Figure 12: Main concepts for comparing cybersecurity certification schemes and standards

3.2.1 Table of chosen standards and frameworks

Table 5: List of chosen standards and frameworks

Name	Type	Issuer	Country	Sector	Scope
ISO/IEC 27001	Standard	ISO/IEC	International	General	Service providers and organisations
NIST CSF	Framework	NIST	USA	General	Critical infrastructures
Common Criteria	Standard	CCRA/SOG-IS	International	General	Product and services
CIS Critical Security Controls	Set of controls	Center for internet security	International	General	Service providers and organisations
Industrial Internet of Things Security Framework	Framework	Industrial Internet Consortium	International	Industrial IOT Systems	IOT
Cloud Security Alliance Cloud Controls Matrix	Framework	Cloud Security Alliance	International	Cloud service providers	Cloud
ISKE	Standard	RIHA	Estonia	State and government	E-government
IT Grundschutz	Standard	BSI	Germany	General	Service providers and organisations
ISO-SAE 21434 & SAE J3061	Standard	ISO/SAE	International	vehicles	Road Vehicles
ISO 27034	Standard	ISO/IEC	International	General	Application Security
IEC 62443	Standard	ISA/IEC	International	Industry	Automation controls

Another more complete view of this table is presented in the diagrams of Figure 39 for products and services, Figure 40 for Cloud Service Providers, Figure 41 for security professionals, and Figure 42 for Services providers and organisations, in the Annex 7.3 of this document.

3.3 Organisation level certification and standards

3.3.1 ISO/IEC 27001

Almost every IT professional around the world has heard about ISO/IEC 27001 [44]. It is one of the best-known family of standards, providing a complete set of requirements for information security management system (ISMS). ISO adopts a systematic approach when describing the secured management of the sensitive data of a company. The standard covers companies globally, including people, processes, and IT systems via a risk management process. The company must set its security objectives and determine the risks that threaten them.

To manage the identified risks, the company can establish a risk treatment plan. This plan is mainly composed of selected controls. ISO 27001 provides a plethora of controls for every security objective. It is crucial to select and implement the appropriate controls for the company and not try to implement everything. ISO27001 and its controls can be combined with other standards and controls when needed.

The ISO 27001 family of standards has been growing quickly over the last years, and now includes almost 40 standards. The table below gives an overview of the most relevant of these within the context of this document.

Table 6: Overview of ISO27KX standards [45]

ISO/IEC number	Focus
ISO/IEC 27002	Gives a more detailed description of the controls described in Annex A of ISO 27001
ISO/IEC 27003	Gives implementation guidance for ISO 27001
ISO/IEC 27004	Gives guidance on monitoring, measurement, analysis and evaluation of an ISMS
ISO/IEC 27005	Provides guidelines for information security risk management
ISO/IEC 27017	Adds requirements, guidance and controls specific for cloud services
ISO/IEC 27032	Adds requirements, guidance and controls for improving cybersecurity
ISO/IEC 27033	Adds requirements, guidance and controls for network security
ISO/IEC 27034	Adds requirements, guidance and controls for application security

Evaluation and Governance

To have their information security management certified to the ISO27001 standard, a company needs to call an independent certification body. These certification bodies are accredited by a national accreditation body that ensures sufficient quality.

Certification Process

An ISO 27001 certification is often achieved by developing and documenting the necessary procedures and controls. The implementation of these procedures and controls should be done according to these documents. A compliant ISMS should not stay inert and should be regularly updated and to do so, management reviews and regular internal audits must be performed. If any non-compliances are detected, they must be mitigated or corrected by corrective and preventive actions. Errors must be found, corrected, and should not happen again.

Once all of this is in place, the certification process can start. This process is divided in two steps Stage 1 and Stage 2 audit. The Stage 1 audit, or Documentation review, will focus on the company's documentation and checks if it is compliant with ISO27001. The Stage 2 audit, or Main audit, is centred around all organisation activities and if they are compliant with both ISO 27001 and their documentation.

If the auditor finds any non-compliance, the company needs to take corrective action in a certain period. Once the audit is satisfactory, a certificate is granted and is valid for three years. It needs to be renewed via another round of Stage 1 audit and Stage 2.

Figure 13 below shows the growing traction of such certification frameworks.

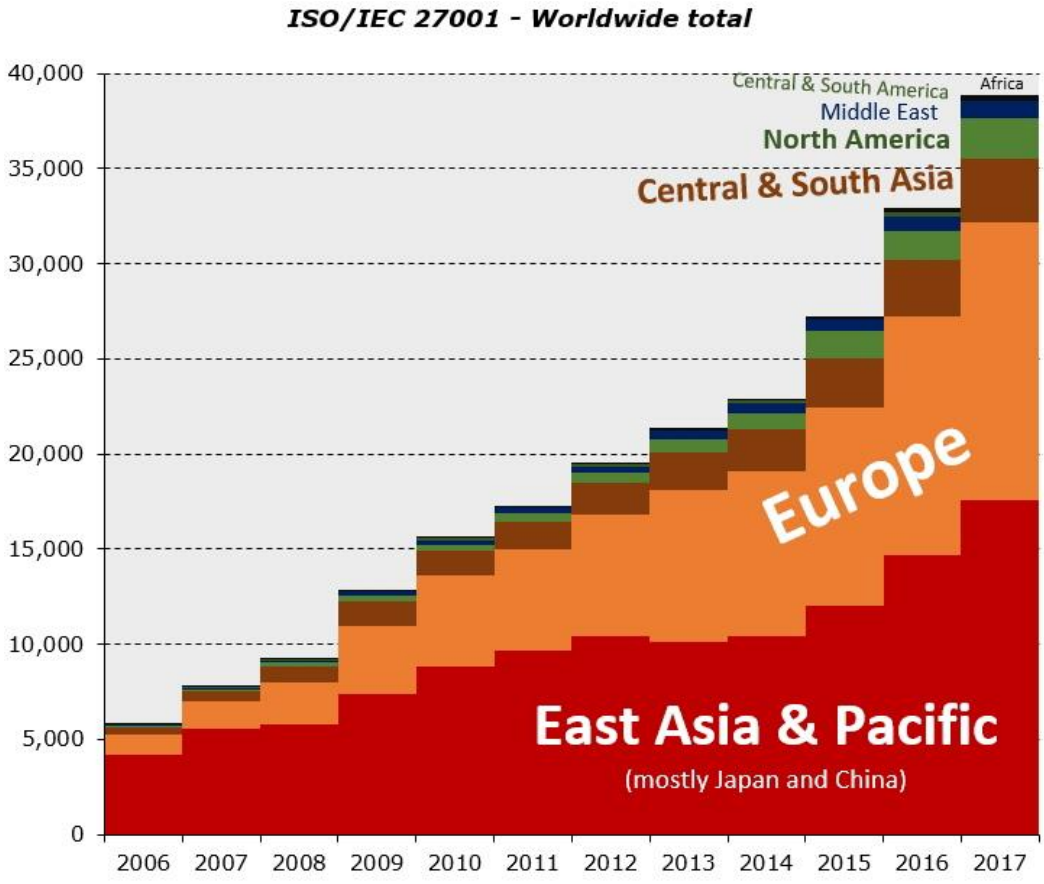

Figure 13: ISO/IEC 27001 Worldwide total [46]

3.3.2 NIST CSF Framework

The U.S. National Institute of Standards and Technology (NIST) oversees The NIST Cybersecurity Framework [47]. It aims to provides a common and accessible language for dealing with cybersecurity risk. It is easily adaptable for many technologies, sectors or even lifecycle phase. The framework is revolving around the notion of risk and how to identify and reduced them. It provides the means to align business, policy and technology in a holistic risk-based approach. It can cope with the management of entire organisation of a single department.

The framework was design with the critical infrastructures in mind but is flexible enough to enables organisations, regardless of their size or complexity, to apply the principles and best practices of risk management in order to improve the security and resilience of their infrastructure. It is based on international standards for cybersecurity and thus could be easily used by other organisations located outside the United States.

The Framework is a risk-based approach to address cybersecurity risk, and is composed of three parts:

- The Framework Core is divided in five Functions, Identify, Protect, Detect, Respond and Recover (see Figure 14), covering both prevention and reaction. It described the desired outcomes in an understandable manner, applicable to all kind of risk management. The Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References such as existing standards for each Subcategory.
- The Framework Implementation Tiers (see Figure 15) describe how an organisation's cybersecurity risk management is performing against the characteristics described in the framework. The tiers are going from Tier 1 (Partial) to Adaptive (Tier 4).
- A Framework Profile is a representation of the outcomes that a particular organization has selected from the Framework Categories and Subcategories. By developing a 'Current' Profile and a 'Target' Profile, organisations can establish a roadmap for reducing cybersecurity risk.

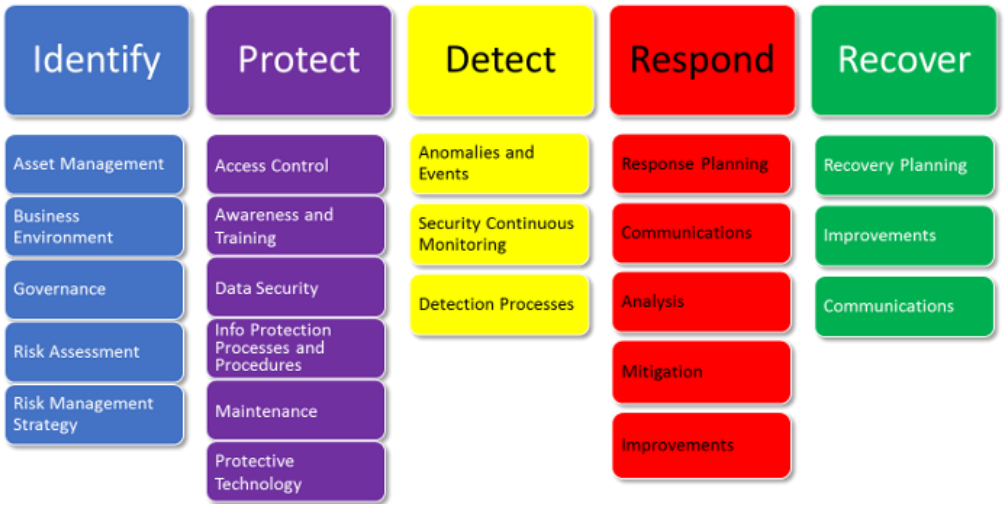

Figure 14: The five core functions of the NIST Cyber Security Framework [48]

Figure 15: The NIST Cyber Security Framework Tiers [48]

Evaluation and Governance

Currently, the U.S. National Institute of Standards and Technology (NIST) has no plan to develop a certification or conformity assessment based on the framework.

Certification Process

There is no official certification or evaluation process, as the use of the framework is fully voluntary. Still, useful information can be found on https://www.nist.gov/cyberframework/industry-resources. Several use cases of the implementation of NIST in specific industry are described.

3.3.3 Common Criteria

"The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently at version 3.1 revision 5. The standard comprises catalogues of functional requirements (CC part 2) and assurance requirements (CC part 3), together with instructions on how to construct security specifications (also called 'Security Target', see CC part 1) and conduct independent security evaluations based on these requirements (CEM).

Common Criteria is a framework in which product users can specify their security functional and assurance requirements using a Security Target, which itself may be based upon a certified Protection Profile (PP). Testing laboratories (ITSEFs) can then evaluate the product against its Security Target to determine whether it actually meets the functional and assurance claims. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner.

Apart from stating the Security Functional Requirements of a class or product, a Protection Profile or Security Target also defines the evaluation work units through the security assurance processes:

- *Security Assurance Requirements (SARs) are descriptions of evaluation work related to the product development environment and actual security features and/or evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that design documents are kept in a change management system, that full functional testing is performed by the developer of the product, or that penetrating testing is performed by the testing laboratory in order to verify that a certain level of vulnerability analysis is reached.*
- *The Evaluation Assurance Level (EAL) is a numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Higher EALs always includes all the evaluation work defined for the lower ones.*

Higher EALs do not necessarily imply 'better security', they only mean that the claimed security assurance of the target of evaluation (TOE) has been more extensively verified. However, for lower EALs the bar to pass vulnerability analysis is lower. A specific scale defines the level of the vulnerability analysis depth: from VAN.1 (basic attack potential, script kiddies) to VAN.5 (high attack potential). Therefore, in practice there is a correlation. EALs may be augmented with additional assurance activities from Part 3 of the CC, resulting in an EAL level such as EAL4+.

Evaluation and Governance

The Common Criteria Recognition Arrangement (CCRA) is an arrangement between participating evaluation schemes and other interested organisations. The participating schemes ensure that products are evaluated by competent and independent licensed laboratories to common standards, so as to determine the fulfilment of particular security properties, to a certain extent of assurance. The resulting certificates may then be recognised by all the signatories of the CCRA.

Note that certificate recognition means that CCRA participants recognise that the evaluation scheme in the certificate authorising nation correctly performed all of the activities involved in CC and CCRA processes. This does not imply that the certified IT product meets the security requirements of another CCRA participant nation. To help achieve the latter purpose, collaborative Protection Profiles (cPP) are developed by International Technical Communities consisting of vendors, test laboratories, CCRA nations, and academia. cPPs are developed with strong engagement and endorsement of all CCRA participant nations.

Within the CCRA, all evaluations using a cPP are mutually recognised. This may include augmentation with flaw remediation. In some specific cases a cPP can reach Evaluation Assurance Level EAL4, see below for an explanation of the concept of the EAL. Evaluations that are not based on a cPP are recognised up to EAL2.

In parallel with the CCRA, the European countries within the former ITSEC scheme recognise higher EALs under the so-called SOG-IS European Mutual Recognition Agreement (SOG-IS MRA). The SOG-IS MRA covers two technical domains: Smartcards and Similar Devices and Hardware Devices with Security Boxes for which evaluation are recognised up to EAL7. Evaluation outside of those technical domains are recognised up to EAL4.

The overall governance of the Common Criteria scheme is similar under both agreements. Certificates can be independently issued by any of the Certificate Authorizing Schemes. Each of these Schemes has recognized several evaluation laboratories, which carry out the actual product evaluations. The status of Certificate Authorizing Scheme is obtained via a peer review process by means of so-called CB audits. SOG-IS CB audits require further verification than the CB audits performed in CCRA, with a strong focus on technical expertise of both the CB personnel and the CB's licensed labs.

Certification Process

The evaluation serves to validate claims made about a product. To be of practical use, the evaluation must verify the product's security features. This is done as follows:

1. *A Protection Profile may be created by a user community, which identifies security requirements for a class of products (for example, smart cards used to provide digital signatures or network firewalls).*
    1. *a. Security Functional Requirements are taken (and adapted) from Part 2 of the Common Criteria standard (ISO/IEC 15408).*

1. *b. Security Assurance Requirements are taken (and adapted) from Part 3 of the Common Criteria standard (ISO/IEC 15408).*

2. *The Protection Profile is certified by an independent test laboratory to make sure that it complies with all applicable CC requirements.*

3. *A product vendor chooses to create a product complying with one or more PPs and writes a Security Target explaining how the security requirements in these PPs are met by the product. If a PP does not exist for the product type the vendor may prepare their own Security Target directly.*

4. *A recognized evaluation laboratory selected by the vendor evaluates the product (Target of Evaluation, ToE) against the Security Target to make sure that the functional and assurance claims made by the vendor in the ST are actually valid. Its results are documented in an Evaluation Technical Report (ETR).*

5. *Based on the evaluation report, the Certificate Authorizing Scheme that has licensed the laboratory validates the ETR and may issue a Common Criteria certificate for the product.*

Note that Common Criteria describes the set of general actions the evaluators must carry out.

Supporting documentation (https://www.commoncriteriaportal.org/files/operatingprocedures/2006-09-003.pdf) can be defined to describe how the criteria and evaluation methods are applied when evaluating specific technologies. They help harmonising CB (Certification/Validation Bodies) approaches by replacing multiple individual interpretations, and hence provide clarity for developers, evaluators, and certifiers. Their relevance and use for particular technologies are approved by the respective Management Committee (SOG-IS and/or CCRA) following submission of a suitable rationale. There are two classes of CC supporting documentation:

- *Those that are termed 'Mandatory Supporting Documents' have to be applied when evaluating a product involving the particular technology. If the documentation is not applied, the certificate will not benefit from mutual recognition.*

- *Those that are termed 'Guidance Supporting Documents' contain more general advice and best practices.*

Currently most of technical CCRA supporting documents have been provided to the CCRA community by the SOG-IS after a period of trial use.

SOG-IS supporting documents are available at http://www.sogisportal.eu/uk/supporting_doc_en.html. Examples of this include:

- *The SOG-IS Agreed Cryptographic Mechanisms which list agreed cryptographic mechanisms, in particular about their security strength.*

- *The SOG-IS Joint Interpretation Working Group (JWIG) Minimum Site Requirements, which defines a set of minimum requirements for the security of the site where a smartcards and similar devices t is developed. These requirements are applicable from EAL3 upwards, but especially for EAL4+ and higher. They are mandatory for Common Criteria evaluations of smartcards and similar devices, including related software development, but can be verified during any type of Common Criteria evaluation.*

Practice

A typical evaluation can take anywhere from six to fourteen months. Consequently, evaluation is costly; the exact amount depends on the complexity of the product, the security maturity of the developer and the desired Evaluation Assurance Level. In practice, higher EALs do not necessarily lead to longer evaluations, and the overall maturity of the ecosystem is a much stronger factor.

Protection Profiles and supporting documents agreed upon by a community (on the model of the JIWG) contribute to more relevant evaluation methods and shorter lead time.

The maturity of the developer is also a key factor with regard to the throughput time of the evaluation: in case of failure of a work unit, the developer is allowed to make corrections and resubmit the product to the evaluator, and CC does not limit the number of fixes made during an evaluation. Evaluations can therefore be impacted by delays due to product being insufficiently fixed, or delays in fixing the product.

Note that all previous indications only cover evaluations of a specific TOE against an existing Protection Profile or using no Protection Profile. In case a new Protection Profile is necessary, the process of certification of such a PP generally last less than three months.

CCRA

The CCRA covers mutual recognition between evaluation schemes for evaluations up to EAL1-2; in some specific cases cPP evaluation could reach EAL4.

A list of Certificate Authorizing Schemes under the CCRA can be found at http://www.commoncriteriaportal.org/ccra/schemes/; it lists 17 nations. An additional 10 countries are listed as Certificate Consuming Members, meaning they accept Common Criteria certificates but do not issue them.

A list of certified Protection Profiles can be found at http://www.commoncriteriaportal.org/pps/. Currently over 130 PPs are listed, 6 of which are cPPs (at the moment no cPP are fully recognised). A list of licensed laboratories can be found at http://www.commoncriteriaportal.org/labs/; it lists 69 labs. However, there is some overlap in this list, as some laboratories are licensed under multiple Authorizing Schemes.

A list of certified products can be found at

https://www.commoncriteriaportal.org/rss/certified_products.xml. As of March 2017, the list contained over 2800 products.

SOG-IS MRA

The number of European countries participating in the SOG-IS MRA is 10. Each of these countries has licensed a number of IT Security Evaluation Facilities (ITSEFs) that carry out the actual evaluations. An ITSEF may be qualified for 'All Products' on EAL 1-4, for 'Smartcards and similar devices' on EAL1-7, and/or for 'Hardware Devices with Security Boxes' on EAL1-7. The full list of ITSEFs can be found at http://www.sogis.org/uk/status_participant_en.html.

Common Criteria is often used as the basis for a government-driven certification scheme, and typically evaluations are conducted for the use of government agencies and critical infrastructure. Certification may also address other contractual objectives that sometimes are defined by the private sector. Sometimes software vendors or industrials use the certification process to differentiate their product from the competition." [45]

3.3.4 CIS Critical Security Controls

The CIS Critical Security Controls is a list of 20 controls as shown in Figure 16, each subdivided in several sub-controls. They are maintained and published by The Center for Internet Security (CIS) [49] (a US-based non-profit organisation). The implementation of these controls could help an organisation to be more resilient against cybersecurity attacks.

The list is prioritised, beginning with the controls that an organisation should implement first and divided between three categories, "basic", "foundational" and "organizational". Every control, quite

generic, consists of several ‘sub-controls’, which are concrete actions an organisation can take. The reasons for each control are explained, and procedures and tools that can help implementing the control are described.

Figure 16: Three levels of controls of the CIS20 [50]

Evaluation and Governance.

There is no official evaluation scheme for the CIS Controls. The CIS published regular updates of the list. The total number of controls is always 20, older controls disappearing to be replaced by new one. Their priority may change, according the cybersecurity landscape and the ever-evolving threats.

Even without a certification, these “simple” but effective controls help organization in bolstering their defences against cyber-attacks.

Certification Process

The center of Internet Security does not have any certification process. To aid organisations in implementing the CIS Controls, the CIS maintains mappings, use cases, measurement tools and other documentation on its website.

3.3.5 Industrial Internet of Things Security Framework

The Industrial Internet of Things Security Framework (IISF) [51] has been developed by the Industrial Internet Consortium (IIC), with the implication of members from over twenty-five organizations coming from large and small companies, public sector and academia. It is a common security framework and an approach to assess cybersecurity in industrial IoT (IIoT).

The framework is divided in three parts, part 1 described the key systems characteristics (security, safety, reliability, resilience, and privacy), how they should be assured together to create a trustworthy system and what make an IIOT system different. Part 2 reviews the security assessment for organizations, architectures, and technologies. Part 3 deals with the functional and implementation viewpoints of the Industrial Internet of Things Reference Architecture (IIRA).

Evaluation and Governance

IISF does not have an evaluation scheme but the IIC proposes five testbeds for the following sectors: Energy, Healthcare, Manufacturing, Smart cities and Transportation. The testbeds can be used for developing new applications or products for IIoT and rigorously tested before they reach the market.

Security testing is a huge part of these evaluations and provides a feedback who is then included in the IISF, improving the framework.

Certification Process

To access the testbeds, a proposal must be sent the IIC for evaluation. In order to be accepted, a successful proposal needs the following elements:

- Provides rigorous, transparent, and replicable testing of new technologies.
- Applies new technologies to create new products & services.
- Shows how new technologies can be usefully deployed.
- Fuels R&D ideas and opportunities.
- Generates an appreciable and measurable impact on new and existing markets.

Once approved, requests for potential partners are posted in the members area of the IIC.

3.3.6 CSA Security Trust Assurance and Risk (STAR)

The Star program is centred around three key areas, the principle of transparency, a rigorous auditing, and the harmonization of standards. Companies using the STAR program send a clear signal that they are following the best practices and implementing security in their cloud services [52].

The program is driven by the CSA, promoting the use of best practices for providing security assurance within Cloud Computing, and providing education on the uses of Cloud Computing.

One of the major tools provided by STAR is the Cloud Controls Matrix (CCM), a cybersecurity control framework for cloud computing. It is a list of requirements for security assurance in the cloud, designed to strengthen information security control environments for service provider and consumer. It helps reduce an audit complexity by mapping controls with several widely accepted security standards, other controls framework and regulations. The CCM provide an easy way to normalize the cloud taxonomy, security measures and security expectations.

It is composed of 133 controls, structured in 16 domains (incident management, incident reporting, datacenter security asset management…) covering the essential aspects of cloud technology.

Evaluation and Governance

The STAR program is an incremental and multi-layered certification scheme to cloud service providers. There are three different levels of security assurance requirements as listed in the CCM. The first level is a ‘self-assessment’ for organisations with a low/moderate risk profile, powered by the Consensus Assessments Initiative Questionnaire (CAIQ), a set of more than 140 questions based on the CCM. The second and third levels are intended for organisations with increased risk

profiles, through 3rd party assessment-based certification and continuous monitoring-based certification respectively.

Certification Process

As stated above, a STAR audit can be performed at different levels, depending on the requirements of the CSP, as shown in Figure 17:

- Level 1 (self-assessment): Cloud providers either submit a completed, or a report documenting compliance with Cloud Controls Matrix (CCM).
- Level 2 (attestation): A report is made by a third party, indicating if the CSP is compliant or not with the CCM. This attestation does not have a validity in time, it just describes the state of the CSP at the time of the assessment.
- Level 2 (certification): A CSP is certified after a third-party assessment on the CSP's compliance with the ISO/IEC 27001 information management system standard, the certificate is valid for three years.
- Level 3 (continuous monitoring): High-risk cloud stakeholders require certifications schemes that provide high assurance and high transparency. To achieve this, an application, provided as a Software as a Service (SaaS) called STARwatch helps organisations manage compliance with CSA STAR requirements. STARWatch delivers the content of the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ) in a database format.

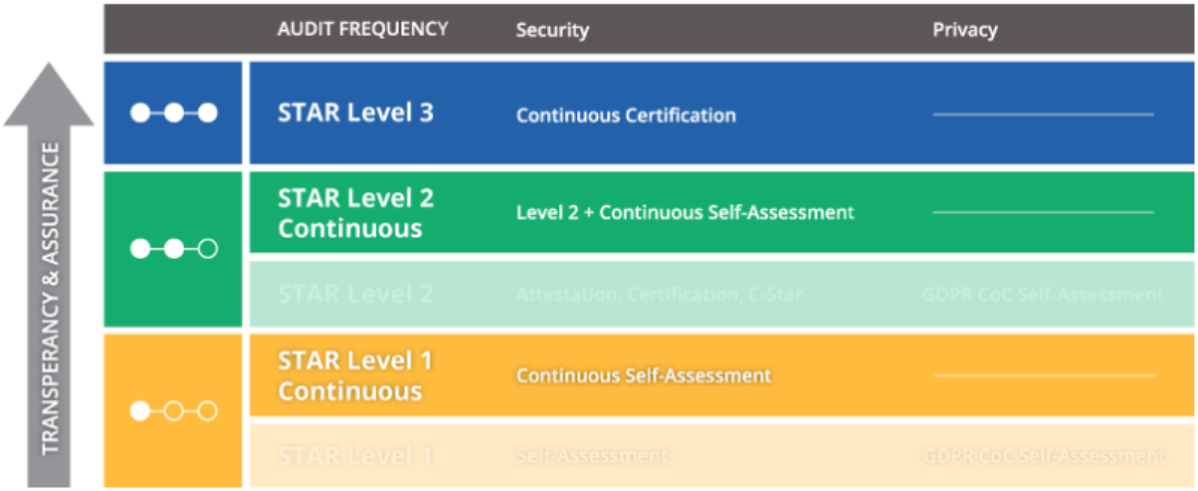

Figure 17: STAR Open Certification Framework [53]

3.4 Process certification standards

3.4.1 ISKE

In need of an IT security standard, the Republic of Estonia started the development of ISKE [54] in 1998, achieving a first version in 2003. Its utilisation for the public sector is mandatory since 2008. The goal of ISKE [55] to ensure a sufficient level of security for the data processed in the system. A sufficient level of security is reached by the implementation of standard organizational, infrastructural, and technical measures. The standard proposes three levels of protection, Low,

Medium, or High. ISKE is based the IT-Grundschutz standard developed by the Federal Office for Information Security of Germany (BSI), described later in this section.

Evaluation and Governance

The administration of the scheme is organised and governed by the Administration System for the State Information System (RIHA in Estonian). There is no certification process yet, only an obligation to be audited for the public sectors. Every ministry, agency or important database manager connected to the state information system has to be audited according to a specific security level depending on the criticality of the databases or registers. Low classification needs to be audited every 4 years, Medium classification needs to be audited every 3 years) and High classification needs to be audited every 2 years.

Certification Process

There is no certification process developed by RIHA yet. A simplified view of the 7 seven steps for the audit process can be found below:

- *"Mapping databases.*
- *Mapping information systems and other information assets.*
- *Identifying links between databases, information systems and other information assets.*
- *Identifying the required security class and level for databases.*
- *Identifying the required security class and level for information systems and other information assets.*
- *Identifying the typical modules, which comply with information systems, and other information assets.*
- *Identifying the required security measures for information systems and other information assets." [56]*

3.4.2 IT Grundschutz

The Federal Office for Information Security or Bundesamt für Sicherheit in der Informationstechnik (BSI) have developed the BSI Standards. They contain recommendations on process, methods, procedures, approaches and measures regarding Information Security. They are numbered from 01 to 04 [57], starting with the definition of an Information System up to the Business Continuity management. We will take a closer look the BSI-Standard 100-2: IT-Grundschutz Methodology and the BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz

The IT-Grundschutz is a step by step methodology, based on the general requirement from ISO/IEC27001. It describes how security management can be set up and operated. Practical security concepts are detailed in great lengths as how to select the proper security safeguards and implement them.

The methodology is providing not only what needs to be done but also the how with very specific information to achieve it. You will find below the systematic approach required to design the security process according to the BSI (2008):

- *"Initiation of the security process*
    - *Accepting of responsibility by the management.*
    - *Designing and planning the security process.*

  - *Creation of the policy for information security.*
  - *Establishment of a suitable organisational structure for information security management.*
  - *Provision of financial resources, personnel, and the necessary time.*
  - *Integration of all employees in the security process.*
- *Creation of a security concept*
  - *Structure analysis.*
  - *Determination of the protection requirements.*
  - *Selection and adaptation of safeguards.*
  - *Basic security check.*
  - *Supplementary security analysis.*
- *Implementation of the security concept.*
- *Maintenance of information security during live operations and implementation of continuous improvement process."*

The BSI-Standard 100-3 or BSI Catalogues also provide a risk-analysis method in order to deploy the correct amount of efforts to resolve risks. It must be used in conjunction with the threat catalogue, regularly updated.

The BSI Catalogues contain recommendations for standard security safeguards for typical business processes, applications, and IT systems.

The Catalogues are divided in modules. Each of them contains a description of the applicable components, approaches, and IT systems, as well as an overview of the threat scenario and the recommended safeguards. The modules are grouped into the following catalogues according to the IT-Grundschutz layer model described by BSI (2013):

- *"Layer 1 Generic aspects: covers the comprehensive security aspects equally applicable to all or most of the information system. This particularly applies to comprehensive concepts and the regulations derived from such.*
- *Layer 2 Infrastructure: covers the physical, technical circumstances. In this layer, various aspects of infrastructural security are merged.*
- *Layer 3 IT Systems: addresses the individual IT systems of an information system that may have been divided into groups. This layer addresses security aspects both for clients, servers, and stand-alone systems.*
- *Layer 4 Network: examines the networking aspects not directly related to specific IT systems, but to the network connections and the communication*
- *Layer 5 Applications: ultimately addresses the actual applications used on the information system".*

Evaluation and Governance

The implementation of IT-Grundschutz can be certified and the BSI has developed a certification scheme also based on ISO/IEC27001. Unlike the original ISO/IEC 27001 certification, the "ITGrundschutz based" version not only covers the information security management system, but also the detailed technical implementation.

Certification Process

To get an ISO 27001 certificate based on IT-Grundschutz, the audit performed by an external auditor who is certified with the BSI. At the end of the audit, an audit report is produced and presented to the certification department. It then decides if the certificate can be granted or not.

The auditors will audit the information security management system (ISMS) documents and verify if they are indeed complete and correct via an onsite audit. This audit doesn't stop at the simple implementation of technical measures but also verifies if the management is also involved and takes its responsibilities.

The process of fully implementing IT-Grundschutz can be quite long, it can be divided in two preliminary stages, the initiation stage and the expansion stage. The auditors can already certify certain subsets of the safeguards defined in the catalogues, in the initiation stage, before they have been implemented.

An ISO/IEC 27001 certificate is issued for three years. A brief auditing visit is made once a year to ensure the level of security is being maintained.

3.4.3 ISO-SAE 21434 & SAE J3061

Both the ISO-SAE AWI 21434 and the SAE J3061 standards describe the process of cybersecurity engineering. The ISO-SAE AWI 21434 focus on the cybersecurity risk management for ground vehicles and the SAEJ3061 on cyber-physical vehicle systems. Those frameworks are similar to the already existing ISO 26262 standard (functional safety management).

ISO-SAE AWI 21434 Road vehicles – Cybersecurity engineering

ISO-SAE AWI 21434, published in August 2021, aims to standardise the cybersecurity engineering process. It specifies requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design, development), production, operation, maintenance, and decommissioning) as described by A. Barber [58].

"*A framework is defined that includes requirements for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders. This document is applicable to road vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications. This document does not prescribe specific technology or solutions related to cybersecurity. It is planned that the J3061 will be retrieved after publication of this standard*" [59].

SAE J3061 – Security Guidebook for Cyber-Physical Vehicle Systems

The SAE J3061 elaborated a process framework for a security lifecycle for cyber-physical vehicle system. It provides high-level guidance and information on best practice, tools and methods related to cybersecurity, which can be adapted to existing development processes in an organization. It builds on many existing works on security engineering and secure system development methodologies and has a strong relation to the automotive system functional safety standard ISO 26262 as stated by C. Schmitter & all (2018).

The framework of SAE J3061 considers the entire lifecycle of the development of Cybersecurity related products from concept phase through production and operation. The product development follows the V-Model and is segmented in system-, hardware-, and software-levels. The security lifecycle management activities should include overall needed aspects as a security culture and not only be focused on technical aspect.

Evaluation and Governance

The ISO-SAE AWI 21434 not yet published. The SAE J3061 is only a guidebook summarising activities for the engineering process.

Process

N/A

3.5 Product certification standards

3.5.1 ISO 27034

ISO/IEC 27034 proposes a model to facilitate the integration of security in application lifecycle. It is designed for internal or external development. The standard offers guidance to those involved in the specification, design, programming, and procurement of application systems and helps to achieve the desired or necessary level of security.

ISO 27034 consists of six parts [45], some of which are still drafts:

- Part 1: Overview and concepts – published 2011.
- Part 2: Organisation normative framework – published 2015.
- Part 3: Application security management process – published 2018.
- Part 4: Application security validation – as of January 2022 is in DRAFT status. .
- Part 5: Protocols and application security control data structure - publication 2017.
- Part 5-1: Protocols and application security control data structure – XML schemas – Published 2018.
- Part 6: Case studies – published 2016 (informative).

ISO/IEC 27034 allows any professionals involved in application development to know what and when Application Security Controls should be applied, how to integrate Application Security Controls in their activities and how meet the requirements of the Application Security Controls associated measurements. One of the key principles of the standards is that if you use the same code across multiple applications or systems, it is worth to heavily invest in the specification, design and testing phase: “Do it properly, do it once, and reuse it”.

It can also provide auditors with the tooling needed to evaluate the security of an application. The standard support them via a process, a methodology and multiples controls, making audit results repeatable and generating enough evidence to demonstrate that the application has reached the desired level of security and trust.

Evaluation and Governance

It does not seem currently possible (yet) to be evaluated by an independent certification body against ISO 27034 specifically. Despite this, several companies have issued self-declarations for conformance against ISO 27034-1.

Process

See section 4.2 on the certification process for ISO 27001.

3.5.2 IEC 62443

"The ISA/IEC 62443 standard is an international standard for security of the industrial automation and control systems in the operational technology domain. The standard was initiated by the International Society of Automation (ISA) and is carried worldwide and being further developed by the IEC. The standard applies to all types of plants, facilities and systems in all industries, including:

- *Hardware and software systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) and Supervisory Control and Data Acquisition (SCADA) systems.*
- *Associated interfaces, APIs or HMIs used to provide control, safety and manufacturing operations.*
- *Continuous, batch and discrete processing systems" [45].*

It covers the whole security problematic via different norms or guides:

- Organisation,
- Methodology,
- System development,
- Security profile.

The ISA/IEC 62433 standard consists in several parts, arranged in four groups, corresponding to the primary focus and intended audience as described in the ECSO state of the Art (2017):

- "*General – This group includes parts that address topics that are common to the entire series.*
- *Policies and Procedures – Parts in this group focus on the policies and procedures associated with IACS security.*
- *System Requirements – The parts in this group address requirements at the system level. Component Requirements – The fourth and final group includes elements that provide information about the more specific and detailed requirements associated with the development of IACS products."*

The overview in Figure 18 provides more information on the topic and current status of each part of ISA/IEC 62443.

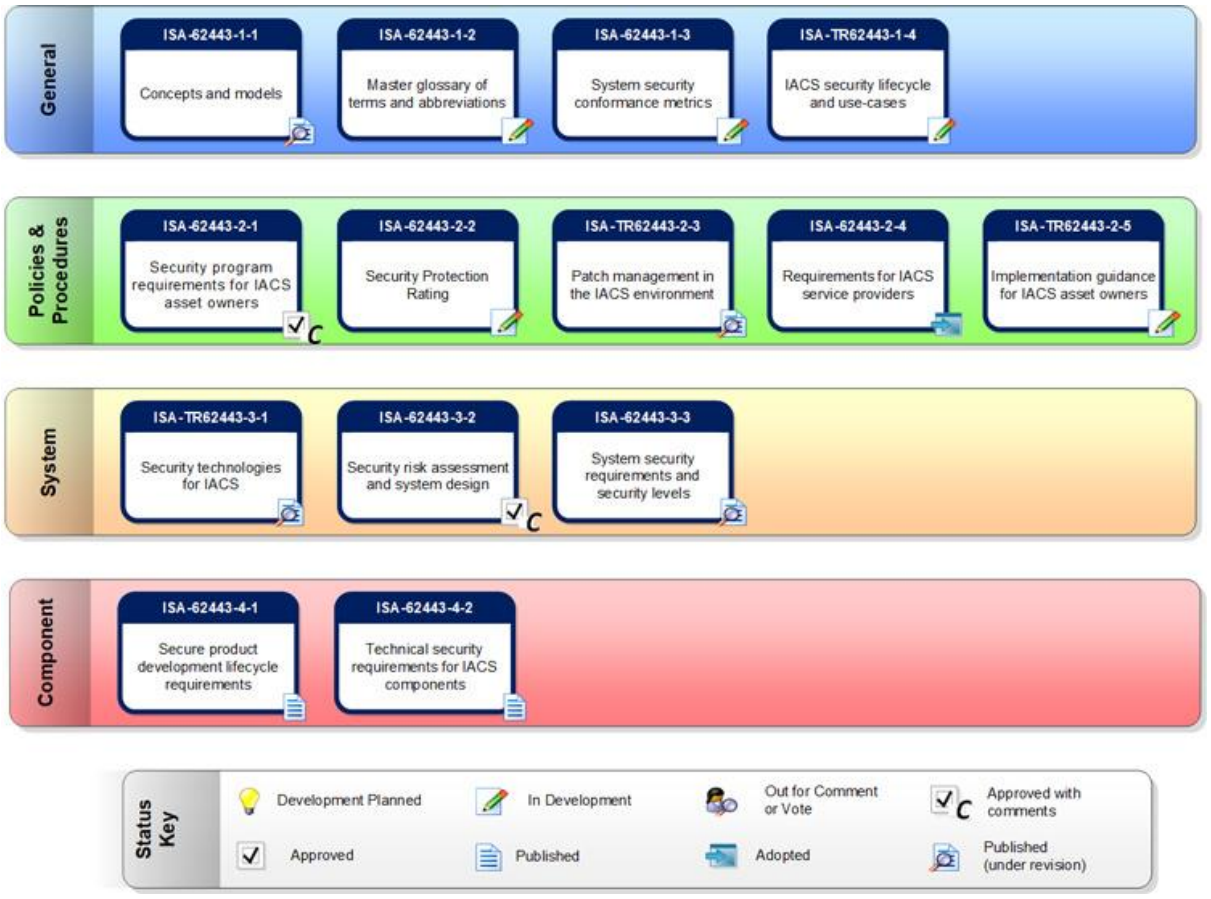

Figure 18: Status of the various work products in the ISA/IEC 62443 [60]

As it can be seen, some of these standards are Technical Reports, which means they are not formal standards and do not contain binding requirements.

Evaluation and Governance

"The IECEE is a multilateral certification system based on International Standards prepared by the IEC. Its members use the principle of mutual recognition of test results to obtain certification or approval at national levels around the world.

The IECEE has an active Task Force Cyber Security, which is working towards a unique approach for conformity assessment to the IEC 62443 series. A guidance Operational Document has been published to describe how the conformity assessment can be handled; this document can be found at http://www.iecee.org/search/?q=62443. It shows that IECEE intends to have separate certification processes for Processes, Products and Solutions, and for each offers two assessment scenarios:

- *Scenario 1 – Capability Assessment: An assessment of a set of capabilities typically described in a plan or set of policies / procedures.*
- *Scenario 2 – Application of Capabilities Assessment: Use of a Scenario 1 capability for a specific product or solution."*

Process

"*The applicant is responsible for both identifying the standards within the IEC 62443 series to be utilised in their assessment and for selecting the specific security requirements from the identified standards that are to be evaluated within the scope of the assessment. It is not required to select all security requirements from the identified standard. The Applicant selects the specific requirements*

for which they are requesting to be assessed. In addition, the Applicant may be required to identify the product(s) or solution to which the assessment applies.

As part of the submittal, the Applicant completes the applicable portions of a Test Report Form (TRF) and additionally provides evidence in support of the capabilities that are intended to demonstrate compliance to the selected requirement(s). Each selected IEC 62443 security requirement is evaluated against the supporting evidence supplied by the applicant."

ANSI/ISA 62443 is a series of standards, technical reports, and related information that defines procedures for implementing secure Industrial Automation and Control Systems (IACS).

Chapter 4 Recommendations in terms of certification for the SPARTA Research Programs

The following table provides a summary of the different cybersecurity certification schemes and standards that have been taken into consideration for the CAPE, HAIIT, T-SHARK, and SAFAIR research programs. The table contains one safety standard (ISO 26262) that was included because it is relevant to task T5.2 of CAPE. In the design of the SPARTA roadmap, emphasis was put on the collaboration between CAPE and WP11 to align SPARTA cybersecurity assessment tools with cybersecurity certification. During the design of the SPARTA research roadmap, there was some interest in cybersecurity certification from HAIIT and less from T-SHARK, and SAFAIR research programs, consequently less collaboration was planned. In the table some certification schemes that are relevant to HAIIT, T-SHARK, and SAFAIR have been identified. Workshops with the research programs that showed some interest to the certification schemes took place. In these workshops we have tried to analyse in more detail their interest in the certification schemes.

Table 7: Certification and standards / Research programs

	CAPE	HAIIT	T-SHARK	SAFAIR	Certification
Management level assistance					
ISO/IEC 27001	x	x	x	x	x
IT Grundschutz		x	x		x
Implementation guidance					
NIST CSF Framework	x	x	x	x	
CIS Critical Security Controls	T5.2	x	x		
Product and services certification and standards					
Common Criteria	T5.1, T5.2	x			x
CSPN	T5.1	x	x		x
Industrial Internet of Things Security Framework		x			
CSA Security Trust Assurance and Risk (STAR)	x	x	x	x	x
ISKE	T5.1 (eGov vertical)			x	x
ISO 26262 (safety)	T5.2				
Process technical standards					
ISO-SAE 21434 & SAE J3061	T5.2	x			
ISO 27034	T5.3	x	x	x	
IEC 62443	T5.3				
SME certification					
KIS	T5.1				
Cyber Essentials	T5.1	x			x

4.1 CAPE (WP5) – Continuous assessment in polymorphous environments

Cybersecurity assessment is difficult due to the complexity of systems and their pace of change. The CAPE research program aims to provide practical cybersecurity assessment tools to product and service developers. Assessment is a key concept in many cybersecurity certification schemes. In this section we examine the link between security engineering phases and the Common Criteria certification process with the aim of understanding how assessment tools outputs from the CAPE research program can be useful for certification evaluation.

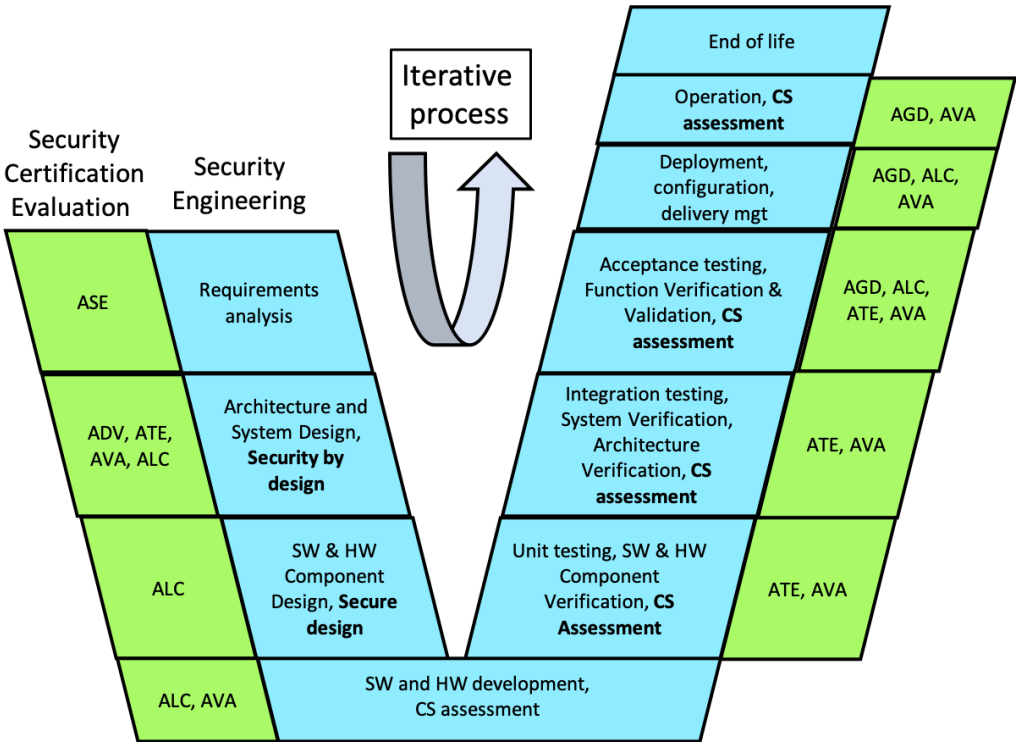

Figure 19: security engineering and Common Criteria certification process

Figure 19, above, suggests how the different steps of the security engineering and certification processes can be put into correspondence. The process descriptions are shown in parallel, to highlight the time dependencies between the steps of a process, and between steps of the security engineering and certification processes. The security engineering process covers both software and hardware development; however, the focus in SPARTA is on software development. The SPARTA assessment framework that is defined in the CAPE research program covers the following phases of the software lifecycle:

- the design phase covering requirements, architecture, design, development, unit testing, integration testing, acceptance testing and deployment,
- the operation phase when a system is running in its target environment
- the end-of-life phase when the system is taken out of operation

The design life cycle is assumed to be iterative. The CAPE research program is developing tools for assessing cybersecurity at the different steps of the security engineering process. The figure suggests that some of the outputs of the assessment tools could be useful as input for the corresponding step in the certification process. For example, once the security requirements for a given system have been defined, they can already be evaluated with respect to the security target or protection profile of the target of evaluation (ASE) (more specifically the ASE REQ security requirements of the Security Target evaluation class (ASE).

4.1.1 Recommendations of standards and frameworks relevant to CAPE

Table 8: Product certification schemes comparison

	ISO 15408 Common Criteria	ANSSI CSPN
EU Cyber Certification Framework	Yes, under way	No
Product level certification	Yes	Yes
Incremental certification possible	Yes	Yes
Can it be certified in different European countries?	Yes	No, only in France
Certification tools available	No (is TOE a tool?)	No (same question)
Process level Certification	?	No
Coverage of certification scheme	Complete	Only technical focus (no architecture, no process, no life-cycle development)
Cost	High	Low
Timeframe Certification	+- 1 year	+- 2 months

The above table compares the two product certification schemes, ISO 15408 Common Criteria and ANSSI CSPN that have been considered in the context of task T5.1. ANSSI CSPN is designed as a lightweight product certification approach and an alternative to ISO 15408 when required confidence levels are lower. It is based on black box testing of the TOE under time constraints, so that evaluation duration is limited. ISO 15408 Common Criteria is a product-oriented cybersecurity certification scheme where users specify security requirements, vendors can provide products that implement the requirements, and evaluation facilities can evaluate the product to determine if the requirements are satisfied.

ISO 15408 has been selected for experimentation in CAPE for several reasons: (1) it covers more SDLC phases than just the testing phases and allows more SPARTA assessment tools to be experimented with, (2) it will likely be part of the EU Cyber Certification Framework and (3) the testing phase will be covered, so that some conclusions on SPARTA tool support for CSPN could also be made.

The following table describes the recommendations for T5.1 from the certification point of view.

Table 9: Recommendations

	Recommendation	Justification
R1	**Incremental certification process**: It is recommended to define a flexible and incremental certification process that can be integrated with the security engineering process (security by design)	Current evaluation schemes are time consuming and costly. More lightweight and flexible certification processes are necessary.
R2	**Continuous integration of certification**: It is recommended to define an implementation of the incremental certification process in the form of continuous integration and deployment	Incremental certification not only implies evaluating only the parts of the TOE that impact requirements defined in the protection profile (PP). It also implies that certification evaluation can be done during the different steps of the security engineering process.

	Recommendation	Justification
		This amounts to integrating the certification process into the security engineering process.
R3	**Assessment tools for certification**: It is recommended to analyse how SPARTA assessment tools can be used to prepare a Common Criteria certification	Some of the assessment tools could produce outputs to prepare for a Common Criteria certification.
R4	**Evaluation tools for certification**: It is recommended to analyse how SPARTA assessment tools can be used by Common Criteria evaluators.	Some of the assessment tools outputs could be used by Common Criteria evaluators during the evaluation process. This could speed up the evaluation process.
R5	**Continuous Monitoring of certification**: It is recommended to analyse which aspects of continuous monitoring of certification could be handled by some of the SPARTA assessment tools.	Once a system has been certified, changes may be made that mean it is no longer compliant. This may not be detected until the next evaluation. The purpose of certification monitoring is to verify that compliance is respected during the operation and evolution of a system. It must be noted that monitoring of compliance will be one of the requirements for the certification scheme to be part of the European cybersecurity certification framework.
R6	**Assessment tools for SME certification**: SME certification schemes also need tool support. It is recommended to analyse if some of the SPARTA assessment tools can be used for parts of SME certification schemes.	SME cybersecurity certification is a growing area of interest. SME's amount for a large part of the European economy: 99% of all companies (93% are micro enterprises of less than 10 people) and 66% of employment in 2017. Often SMEs don't have the resources that larger companies have to address cybersecurity issues. SMEs need lightweight certification schemes and associated tool support.

The status of the above recommendations is described in the tables below.

Table 10: Current status of recommendations R1

Recommendation	Status at M36
R1 Incremental certification process	An incremental Common criteria evaluation process has been proposed in T5.1. It shows how the different Common Criteria evaluation Classes can be integrated with security and safety engineering processes. This work has been continued in T5.4. and reported in two papers of the CyberCert workshop. In [73] the need for flexible and more automated incremental certification was presented as well as a first process definition. In [74] challenges for incremental product certification and a more detailed process description for incremental certification with Common Criteria Is presented. The key idea in this paper is to Compose DevSecOps agile development processes that perform updated with incremental Common Criteria certification processes. First results on a prototype are presented. A prototype was developed for the automotive vertical in T5.4 and is described in D5.4.

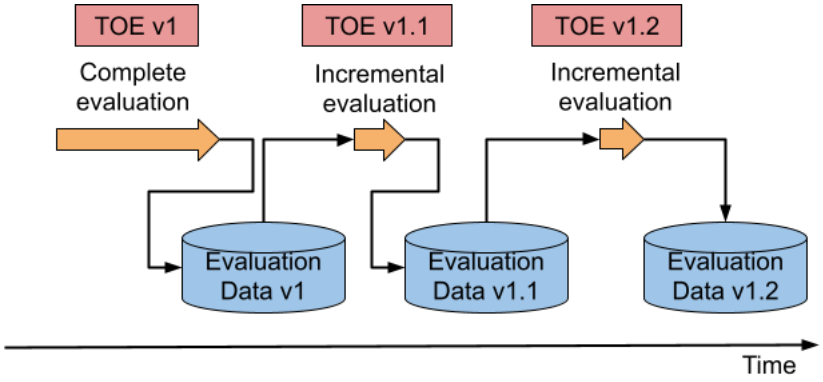

Figure 20: Incremental certification process

Figure 20, from [73], shows the principle of an incremental certification based on two incremental evaluation iterations taken from Figure 19. In the first iteration the Target of Evaluation (TOE) is evaluated with respect to a protection profile (PP) and evaluation results are saved as “Evaluation data v1”. Later, the TOE is modified in version v1.1 and some of the changes impact security requirements defined in the PP. The TOE v1.1 must be re-evaluated with respect to PP. The evaluation is incremental because only the parts of the TOE that impact some PP requirements are re-evaluated. The results are stored as “Evaluation data v1.1”. Later, the TOE is modified again into version v1.2, and the incremental evaluation process is applied again to produce results stored as “Evaluation data v1.2”.

In [74] several key ideas regarding incremental certification are introduced. The main purpose of incremental certification is to ensure continuity of certification. Critical applications and infrastructures are connected and they are being updated on a more frequent basis. To ensure continuity of certification, updates must be analysed to verify the impact on certified cybersecurity properties. Impacted properties need to be re-certified. A lightweight and flexible incremental certification process that can be integrated with DevSecOps practices to automate as much as possible evidence gathering and certification activities is proposed. The approach is illustrated on the Common Criteria product certification scheme and a firewall update on an automotive case study.

Dealing with certification and product evolution: Since the 1980s, there has been a growing need to submit IT products to security certifications in order to assess, impartially, the cybersecurity posture of a product. At that time the Department of Defence (DoD) developed the Trusted Cyber Security Assessment Criteria, also known as the ”Orange Book” which described how to perform a security certification for IT systems, to ensure reliability on security enforcing measures deployed to protect information with a particular interest in personal data. In the 1990s the European Security Standard named ”Information Technology Security Evaluation Criteria (ITSEC)” was issued, followed at the turn of the 2000s by the Common Criteria for Information Technology Security Evaluation standard (now in its version 3.1 revision 5). The security certification aims to assess the effectiveness of security countermeasures implementations (Target of Evaluation - TOE) by analysing a defined threat scenario, evaluating the robustness of the mechanisms implemented within a defined operating environment. The strength of a security certification therefore lies in the fact that a third party (Evaluation Laboratory) guarantees an impartial examination of the evidences produced by the developer. Evaluation laboratories need to be accredited by certification authority before they can perform evaluations. Finally, an authority called the Certification Body supervises the certification and issues the certification. In a more static world, modelled by a more static development process, this approach guarantees a good confidence on the implementation effectiveness of the security

mechanisms. Today, in a world where the products are constantly evolving, due for example to the continuous need for technological updates or the release of vulnerability patches there is the need to face challenges of guaranteeing the maintenance of the security certification in view of the changes occurred.

Current practices of incremental certification with Common Criteria: the need to shape security certifications to the continuous evolution of IT products was therefore addressed by Common Criteria within the so-called Common Criteria Assurance Continuity. Assurance continuity aims to define a mutually recognized approach within the Common Criteria for the maintenance and re-evaluation of certified products. The assurance continuity defines a process for carrying out an impact analysis intended to assess the level of changes that have occurred to a certified product. These changes are categorized into minor and major, with the result of having to carry out a number of different evaluation activities in terms of effort and time on the certified product under evaluation, up to the need for a new certification. The assurance continuity activities involve all the players who take part in a Common Criteria certification, starting with the sponsors and developers, passing through the Evaluation Laboratory and finally the Certification Body. The standard therefore provides a methodological approach to carrying out the impact analysis while not defining specific supporting tools or methodologies.

Requirements for flexible incremental certification processes: It is therefore important to identify requirements that make the incremental certification process more flexible, even if well structured, in order to have advantages in terms of time and cost. The first requirement that we can consider, is to adopt a structured security development process which would allow to guarantee a greater assurance of the certified product since the earliest stages of requirement definition. At the same time, an agile process must be put in place to support the certification in all phases of the life cycle, considering also the very important maintenance phase (patch management and improvement). To this extent, methods and technologies such as DevSecOps can greatly help in reducing costs and times by supporting the developer in the process of creating and maintaining a certified product, in carrying out Assurance Continuity activities and in the production of the Impact Analysis Report. The evidences of certification could be partially produced by means of DevSecOps' automatic tools, by allowing a reduction of costs and times. This would allow the developer to take into account the impacts of the changes in progress to the certified product and maintained simpler during the entire life-cycle development. Moreover, the evaluator can assess more quickly the impacts and can obtain the necessary evidences for the maintenance of the certification. From the point of view of the evaluator, a good development process (including the maintenance phase) would also ensure faster access to the evidences necessary for the evaluation of an impact analysis. One example of efficiency improvement could be related to the management of minor changes. In a structured semi automatized process, changes not affecting the Target of Evaluation could be evaluated faster. The assurance of the DevSecOps process could be verified by the evaluation laboratory during the Common Criteria evaluation of the product in order to ensure its effectiveness for the production of certification evidences (also when modified for the assurance continuity). Please note that this would greatly help concurrent evaluations as well (i.e. evaluations conducted during product development).

Modelling certification processes: Common criteria certification defines a process that includes the following classes:

- ASE (Security Target Evaluation): this class deals with the evaluation of the consistency of the Security Target which also contains the definition of the security requirements of the TOE.

- ADV (Development): this class deals with the evaluation of the six families of requirements for structuring and representing the security functionality realized by the TOE at various levels and varying forms of abstraction that the developer must produce during the product development phase.
- AGD (Guidance Documentation): this class takes care of the evaluation of the manuals that are delivered to the customer.
- ALC (Life-cycle support): this class evaluates all aspects of the management of the TOE during its life cycle; it includes maintaining the certification via security patch management.
- ATE (Tests): it is the class that takes into consideration all the tests that demonstrate that security functionalities operate according to their design descriptions.
- AVA (Vulnerability Assessment): this class takes care of vulnerability assessment activity to analyse vulnerabilities in the development and operation of the TOE.

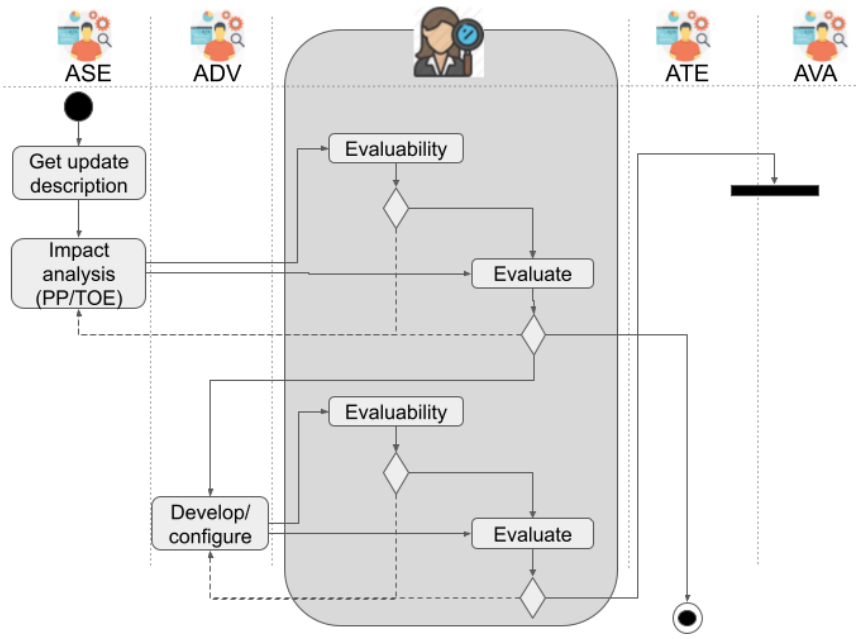

Figure 21: Certification process activity diagram

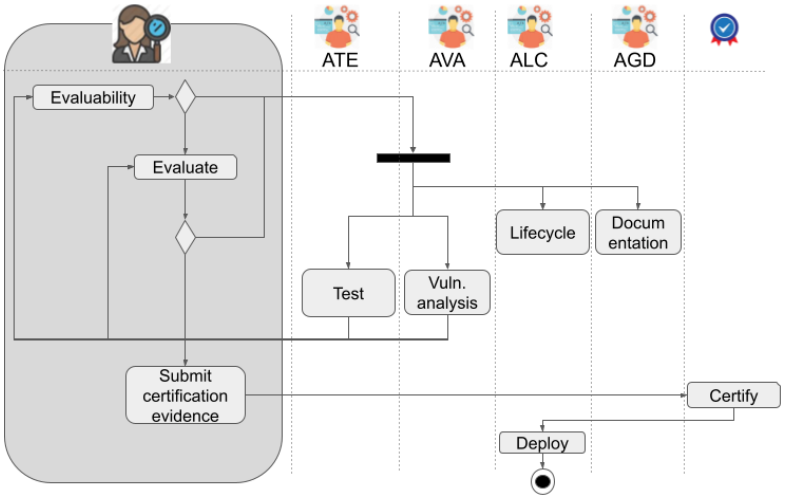

Figure 22: Certification process activity diagram

Figure 21 and Figure 22 show an activity diagram that models the incremental certification activities of the product owner, the Common Criteria evaluator and the accreditation body, i.e. that delivers the official certification. The pattern of interaction for each class is the following:

- The product owner carries out normal security engineering activities and produces certification evidence for the evaluator;
- Once the certification evidence is available, the evaluator is notified and performs an evaluability check. In the evaluability check the evaluator verifies that the necessary evidence is available;
- If the evaluability check is positive, then the evaluator performs the evaluation on the available evidence.

In Figure 21 the incremental certification process is triggered by the arrival of a new version of the software. Within the ASE class a description of the update is made and impact analysis can start. The goal of impact analysis is to determine if incremental certification is necessary. Once impact analysis evidence has been created, the evaluator makes the evaluability check. If it is positive, then the evaluation of impact analysis evidence starts. If the evaluability check is negative then impact analysis must continue until it produces the required evidence. If the evaluation of impact analysis ASE evidence is positive, then incremental certification then moves to the ADV class with the same type of pattern of evaluation. If the ASE evaluation is negative, then impact analysis must continue until the necessary evidence is created. During the development phase certification evidence is produced and once the developer considers the evidence as complete, the evaluator starts the evaluability check. If the evaluability check is positive, i.e. all the required evidence is available, the evaluator starts the evaluation of the ADV evidence. If the evaluation is positive, then evaluation of ATE testing and AVA vulnerability evidence can start.

Figure 22 shows the incremental certification process for the other Common Criteria classes. The same pattern of evaluability and evaluation applies to the ATE, AVA, ALC and AGD classes (the two latter are not shown). Once the evaluator has validated the evidence from all classes, he submits it to the accreditation body that reviews the evidence and delivers the certification for the product

or service with respect to the security requirements specified in the protection profile (PP) or target of evaluation (TOE).

The main aim of modelling the incremental certification process is to compose it with different development process models so that certification activities are integrated with the development process and can reuse development artifacts, and thus reducing as much as possible the certification overhead.

Table 11: Recommendation status R2

Recommendation	Status at M36
R2 Continuous integration of certification	An implementation of the SPARTA framework in the form of continuous integration and deployment has been proposed in D5.1. D5.2 proposed to implement continuous integration and deployment in the form of a DevSecOps process. A DevSecOps process was defined for each of the CAPE verticals and includes the required tools . In D5.4 a demonstrator of a CI/CD process model is presented.

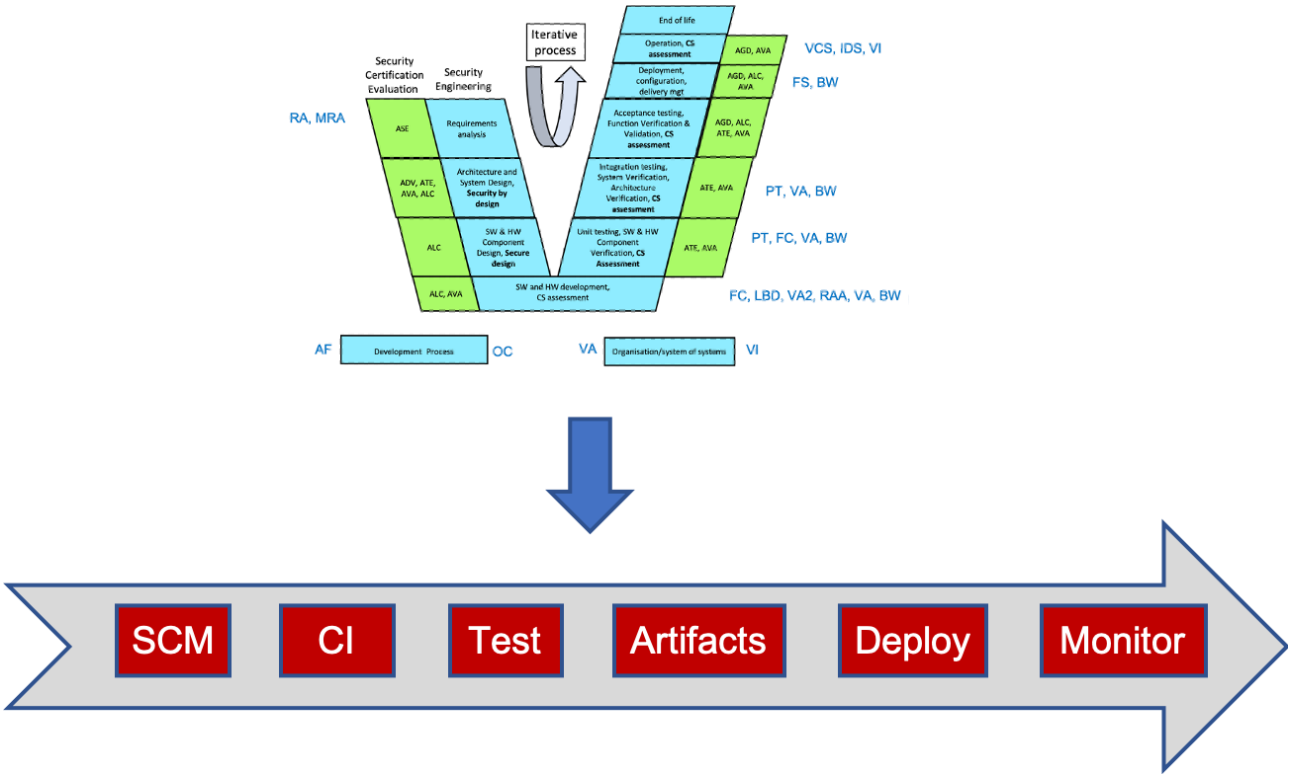

Figure 23: Continuous integration of certification evaluation.

Figure 23, above, suggests that the different steps of the common criteria certification evaluation process could be implemented into a DevSecOps process where assessment tools as well as certification evaluation activities are performed. Currently several CAPE demonstrations scenarios are considering using a continuous integration and deployment approach.

In [74] DevSecOps practices are summarized and modelled for the purpose of integrating certification evaluation processes. In recent years, the need to improve software delivery in terms of speed and quality has given rise to a set of practices that combine continuous build, testing, integration, delivery, ... The DevOps approach, closely related to Agile software development method, integrates software development (”Dev”) and operations (”Ops”) processes to ensure that new features are added to a software solution in the shortest time possible, and with a high level of quality. This approach emphasizes the importance of communication between the involved parties, including the whole production chain (developers, system administrators, network team, ...), to break the classic ”silos” of specialists. DevOps relies on the ”CAMS” (Culture, Automation, Measurement, Sharing) characteristics and on a ”shift to the left” where aspects such as resilience or security are taken into account as soon as possible in the software development life cycle. DevOps is focused on producing quality code, quickly and reliably. The security problematic is not directly addressed in this approach and DevSecOps is aiming at complementing DevOps with security procedures to ensure continuous security assessment.

DevSecOps is an agile development process that is ideally suited for making system updates to complex systems. In order to make incremental certification activities more flexible, they need to be integrated into the update development process.

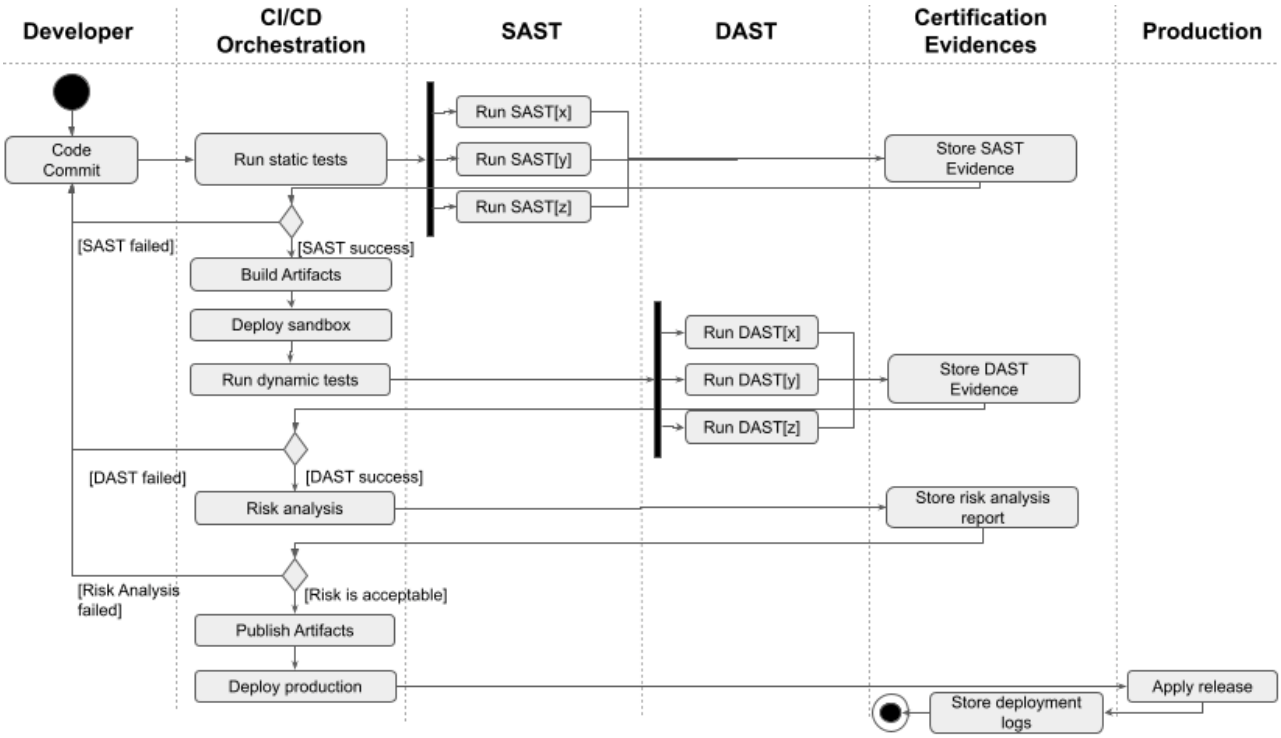

Figure 24: DevSecOps process activity diagram - code, build, test, release, deploy

Modeling DevSecOps processes: Figure 24 shows a sample activity diagram of DevSecOps activities in the context of continuous integration and deployment on a autonomous rover. Each step provides results (logs, reports, ...) that can be used as certification evidence. The sequence reads as follows:

- Upon modifying the software, the developer commits the modifications to a code repository. If any of the subsequent steps fail, the process restarts from here with modifications to the code and configuration.
- Static security tests such as source code or dependency analysis are run on the source code.
- The Static Analysis Results Interchange Format (SARIF) and the Static Analysis Server Protocol (SASP) can facilitate the integration of the SAST output with other tools.
- If static tests succeed, artifacts are built, deployed into a sandbox and dynamic security tests (DAST) are applied to the environment: vulnerability analysis, penetration testing, etc.
- If dynamic tests are successful, a risk analysis can be performed on the system. It will take as input the various outputs of the previous steps (vulnerability analysis report, code analysis report, etc.) and produce an updated risk for the software version being released. If the risk is not acceptable, steps must be taken to mitigate it, for example by improving security monitoring or enforcing stricter security rules.
- The packaged application is published in an artifact repository and deployed to the production environment.

Composing incremental certification and DevSecOps processes: Figure 25 shows the composition of the incremental certification process model with the DevSecOps process model for the impact analysis part of the process. The two processes evolve in parallel but interact in the following

general manner: the DevSecOps process produces evidence for the certification process, and the certification process will authorize the deployment if incremental certification is required. The incremental certification process is triggered by a change request to update the deployed

system with a new version of a component. The change request triggers the beginning of the impact analysis in the certification process. In the DevSecOps process the change request triggers the code commit of the source code and the start of static analysis activities. Part of the static analysis results are stored as certification evidence for the impact analysis activity. The arrow between the ”Store SAST Evidence” activity and the ”Impact analysis” activity will trigger the checks on the certification evidence: when all impact analysis certification evidence is available, the evaluability check by the evaluator can start.

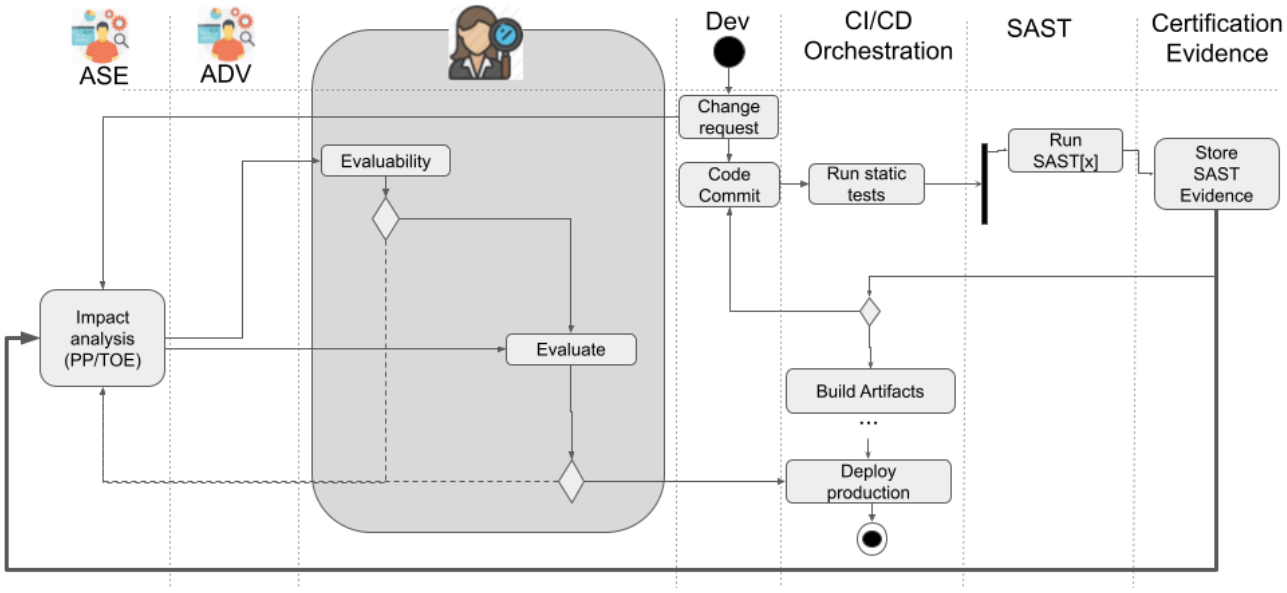

Figure 25: Composed certification and DevSecOps activity diagram impact analysis

This composed process is illustrated on a concrete firewall update example: the example shows how the impact analysis evidence is analysed to determine if incremental certification of a automotive platooning system is required. The ”Store SAST Evidence” will produce the evidence that will be used by the ”Impact analysis” activity to produce traceability evidence to requirements. The same type of interaction between the certification and DevSecOps processes occur for all Common Criteria classes, but this is not described in In [74] and left for future work. With the automation of security testing, DevSecOps already provides some foundation for automating certification. For example, static and dynamic security tests produce reports in an automated way, those reports can be used as certification evidence in an automated certification process. Development documents such as architecture, design, specifications, security model, ... are usually produced by hand, which can limit automation of the DevSecOps and certification activities. Solutions for improving the integration of those evidences in a continuous process include the use of model-based approaches to generate the evidences: infrastructure as code for the architecture, Business Process Model and Notation, etc.

Table 12: Recommendation status R3

Recommendation	Status at M36
R3 Assessment tools for certification	The CAPE assessment tools are used in the two verticals following different CI/CD approaches. OpenCert is the only CAPE assessment tool designed for performing certification evaluations. The approach that has been taken to facilitate certification evaluation is to integrate results relevant for certification evaluation produced by CAPE assessment tools in the OpenCert tool.

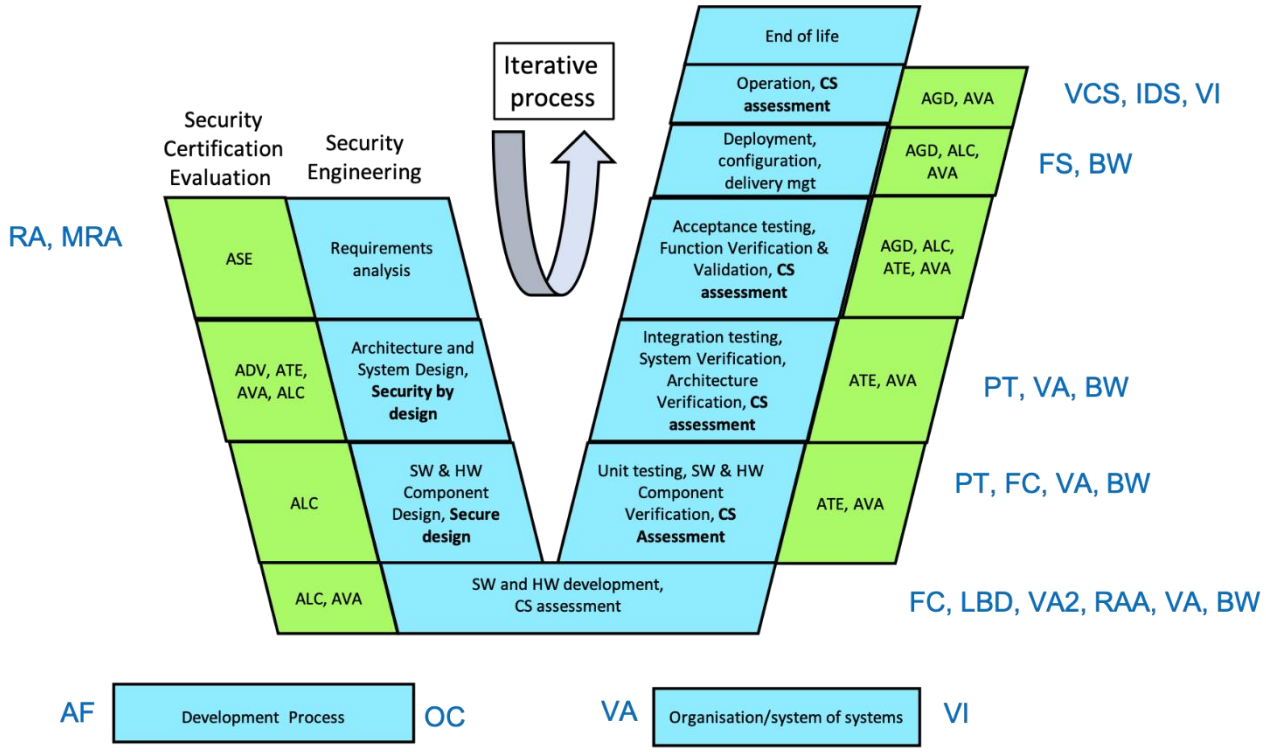

Figure 26: SPARTA Assessment tools and Certification Process

Based on Figure 23 of D5.1, Figure 26 (above) shows the Common Criteria certification evaluation process phases, the corresponding security engineering process phases and the SPARTA assessment tools that can be used in each of the phases. Most of the assessment tools have been designed to be used for cybersecurity assessment during the security engineering process. They have not been explicitly designed for certification purposes. Only the OpenCert tool has been designed for certification evaluation.

Some of the other assessment tool outputs could be used for certification purposes. The table below summarizes potential use of SPARTA assessment tool outputs.

Table 13: SPARTA assessment tool outputs

Security engineering, Common Criteria Classes	SPARTA assessment tools	Possible use for certification
Requirements analysis; ASE	RA, MRA	Can outputs from risk assessment of RA and MRA be used for the ASE assurance class, covering Conformance claims, Extended components definition, Security objectives for the operational environment, security requirements?
SW and HW development, CS assessment; ALC, AVA	FC, LBD, VA2, RAA, VA, BW	Can outputs from code analysis (FC), detection of logic bombs (LBD), Vulnerability assessment (VA, VA2), risk assessment, sandboxes (BW), be used for Life-cycle support/TOE coverage (ALC) and vulnerability assessment (AVA).

Security engineering, Common Criteria Classes	SPARTA assessment tools	Possible use for certification
Unit testing, SW & HW Component Verification, CS Assessment; ATE, AVA	PT, FC, VA, BW	Can outputs from penetration testing (PT), code analysis (FC), vulnerability analysis (VA) or sandboxes (BW) be used for independent unit testing ATE or component vulnerability evaluation AVA?
Integration testing, System Verification, Architecture Verification, CS assessment ; ATE, AVA	PT, VA, BW	Can outputs from penetration testing (PT), vulnerability analysis (VA) or sandboxes (BW) be used for independent integration testing ATE system vulnerability evaluation AVA?
Deployment, configuration, delivery management; AGD, ALC, AVA	FS, BW	Can outputs from virtual machine attacks assessment (FS) or sandboxes (BW) be used for assessing operational user guidance (AGD), lifecycle support (ALC) or Vulnerability assessment (AVA)?
Operation, CS assessment; AGD, AVA	VCS, IDS, VI	How can outputs from run-time monitoring (VCS), intrusion detection (IDS), or visual analysis of cybersecurity information (VI) be used for assessing operational user guidance (AGD) or Vulnerability assessment (AVA)?

Where the tool abbreviations (described in D5.1) are the following RA = Risk assessment (NeSSoS), SB= Sabotage, VA = Vulnerability assessment, FC = Frama-C, PT = Penetration testing, OC = OpenCert, VI = Visual investigation of security information, AF = Autofocus, MRA = model risk assessment for cyberphysical interconnected infrastructures, FS = Foreshadow-VMM Assessment Tool, VCS = VaCSInE, VA2 = Vulnerability assessment, LBD = Logic Bomb Detection, RAAs = Risk Assessment of Android app, IDS = IDS and SIEM assessment tool, BW = “Buildwatch” - A sandbox to monitor development processes.

Currently Autofocus modelling is being used in T5.2 to define a protection profile for the automotive vertical in a purely manual manner.

Table 14: Recommendation status R4

Recommendation	Status at M36
R4 Evaluation tools for certification	Currently OpenCert is the only tool designed for evidence management, assurance case specification, and part of compliance management. The OpenCert tool is demonstrated on the automotive case study and is reported in D5.4.

OpenCert provides evidence management, assurance case specification, and part of compliance management. It supports the management of knowledge about standards (e.g. IEC 61508, DO-178C, ISO 26262, EN 50128/50126/50129, and IEC 62443, among others). Adding support for

Common Criteria to OpenCert was not planned in 2021. However, evaluation data produced during the DevSecOps process was stored and reused during evaluation. This work is reported in the annex of D5.45

Table 15: Recommendation status R5

Recommendation	Status at M36
R5 Continuous Monitoring of certification	Very few tools from the SPARTA assessment framework described in D5.1 cover the deployment and execution phase of the security engineering process. The VaCSInE deployment and monitoring tool was used for monitoring certification.

In the context of task 11.1 SPARTA participated in the Continuous Audit Metrics Working group of the Cloud Security Alliance (CSA). The CSA is defining a "Continuous Certification" scheme. In the context of this effort, the working group is defining security attributes and metrics associated with the control objectives defined within the Cloud Control Matrix (CCM). The aim is to define a catalogue of security attributes and metrics for continuous auditing.

This approach to monitoring certification was investigated in T11.1 and the CAPE tasks. The prototype VaCSInE tool is designed to orchestrate the security response and was illustrated in a CAPE demonstrator by deploying and updating a certified firewall on the rovers to protect them. The monitoring was based on OpenSCAP vulnerability scans, Ansible automation and GitLab-CI. The Impact Analysis Report (see Appendix G of D5.4) describes the security remediation.

Table 16: Recommendation status R6

Recommendation	Status at M36
R6 Assessment tools for SME certification	D11.1 reports on several SME initiatives in Europe. We are currently analysing some of them to understand their needs in terms of assessment tool support.

The table below shows an initial analysis of which SPARTA tools, described in detail in section 3.1 of deliverable D5.1, could be useful for SME certification:

Table 17: SPARTA tools for SME certification

SPARTA Assessment Tools	Potential Use for SME certification
RA = Risk assessment (NeSSoS)	Yes, good for high level assessment for SME's
SB = Sabotage	No, too specialised
VA = Vulnerability assessment	Vulnerability analysis as a service for SME
FC = Frama-C	Too Restrictive, only useful for SME's specialised in C development
PT = Penetration testing	Unknown
OC = OpenCert	Only useful for SME's specialised in Cyber Physical System. Could be useful to manage compliance data if

SPARTA Assessment Tools	Potential Use for SME certification
	OpenCert is extended to support specific certification schemes.
VI = Visual investigation of security information	No, dedicated to large software organisation
AF3 = Autofocus	No, very specific. It is a tool for model-based development of embedded systems
MRA = model risk assessment for cyberphysical interconnected infrastructures	No, too complex
FS = Foreshadow-VMM Assessment Tool	No
VCS = VaCSInE	Yes, it can help SME's involved in security and DevSecOps
VA2 = Vulnerability assessment	It can help SME's involved in C and Java development
LBD = Logic Bomb Detection	It can help SME's involved in app development on Android
RAAs = Risk Assessment of Android app	It can help SME's involved in app development on Android
IDS=IDS and SIEM assessment tool	It can help SME's involved in Network security and Pentest
BW = "Buildwatch" - A sandbox to monitor development processes	It can help SME's involved in application security
PS = package scanner	useful for SME's specialised in Python development

4.1.2 Convergence of security and safety - techniques and specifications study (CAPE Task 5.2)

This task of CAPE focuses on the techniques and specifications for integration of security and safety in the *Connected & Cooperative Car Cybersecurity* context.

Table 18: Certification schemes and standards for Task 5.2

	ISO/IEC 15408 Common Criteria	ISO 26262 Road vehicles — Functional safety	SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	ISO/SAE 21434 Road vehicles — Cybersecurity engineering
EU Cyber Security Certification Framework	Yes (planned)	No	No, those are guidelines	No
Cybersecurity	Yes	(Yes)	Yes	Yes
Safety	No	Yes	No	
Product or services level Certification scheme	Yes	No	Yes	Yes
Process level Certification scheme	No	Yes, certifies personnel only	No	No
Certification facility easily available	Yes	Yes	No	No

The above table summarises the certification schemes and standards that have been considered in the context of task T5.2 that focuses on the automotive vertical. The table includes ISO 26262, which is a safety standard for functional safety of on-board automotive electrical and electronic systems. There is some ongoing work to include some cybersecurity aspects. SAE J3061 provides guidelines for security engineering of modern vehicles and refers to ISO 26262. ISO/SAE 21434 specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning of road vehicle electrical and electronic systems. It is still in draft status. The main challenge from the certification point of view in task T5.2 is to understand how ISO 26262/SAE J3061 and ISO/IEC 15408 certification can be performed.

Table 19: Convergence of safety and security task recommendations

Recommendation	Justification
R7 Common Criteria Certification experimentation: It is recommended to apply the incremental certification approach to Common Criteria on at least one of the SPARTA verticals	Common Criteria is the first certification scheme that has been selected for inclusion in the EU cybersecurity framework. The ENISA “Transposition of the SOGIS-MRA certification framework” working group is working on this. From the SPARTA perspective the assessment

Recommendation	Justification
	tools may be used in support of Common Criteria certification.
R8 Cybersecurity and safety co-design: It is recommended to carry out a partial certification evaluation with ISO 26262/SAE J3061 and Common Criteria. The aim is to understand if a Common Criteria evaluation could complement/improve ISO 26262/SAE J3061 certification.	ISO 26262 is a safety standard for the automotive sector. SAE J3061 is a cybersecurity guidebook for cyber-physical vehicle systems that refers to ISO 26262. ISO/IEC 15408 Common Criteria could complement SAE J3061.
R9 Incremental cybersecurity certification experimentation: It is recommended to experiment with incremental certification, on at least two iterations of the release process.	Incremental certification is an important approach to making certification more flexible and efficient. Experimenting incremental certification on the automotive vertical could provide valuable insights on the application of incremental certification.
R10 Cybersecurity and safety co-certification experimentation: currently certification of safety and security are performed separately. It is recommended to experiment with safety and cybersecurity design and how certification could be performed.	There are several classes of approaches to safety-cybersecurity co-design. Each one of them places constraints on how incremental certification can be carried out.
R11 Cybersecurity assessment tools for certification experimentation: it is recommended to experiment with some of the SPARTA assessment tools that can be used by evaluators	Providing certification evaluators with tools to support the evaluation process is key to automating part of the process and making it more efficient.
R12 Integration of certification activities into continuous integration experimentation	In SPARTA the incremental certification could be integrated into the continuous integration DeSecOps approach for the assessment tools. Integrating certification evaluation activities into the DevSecOps process could contribute to making certification evaluation more flexible and efficient.
R13 Sharing of certification evaluation data: It is recommended to analyse how Common Criteria incremental certification can be performed by different evaluation facilities in Europe.	This is an important topic in T11.3 that aims to understand how incremental product certification can be performed by different evaluation facilities. This means that evaluation evidence needs to be produced in a standard format so that other evaluation facilities may perform incremental certification

Table 20: Recommendation statuses R7, R8

Recommendation	Status at M36
R7 Common Criteria Certification experimentation	Common Criteria has been selected as the cybersecurity certification scheme for the automotive vertical. The case study defined a protection profile for the platooning functionality of the automotive vertical. This protection profile was extended for incremental certification of a certified firewall on the rovers. The extended certification profile is available in the D5.4 annex.
R8 Cybersecurity and safety co-design and certification	The automotive vertical is being analysed following the ISO 26262 safety standard, the SAE J3061 Cyber Security Guidebook For Cyber-Physical Vehicle Systems and ISO/IEC 15408 Common Criteria.

In the context of task T5.2 a hazard analysis was carried out. The SAE J3061 Cyber Security guidelines were considered in the analysis process. In parallel the first steps of a Common Criteria ISO/IEC 15408 Common Criteria have been followed: a protection profile for the automotive vertical was defined and is available in the D5.4 annex.

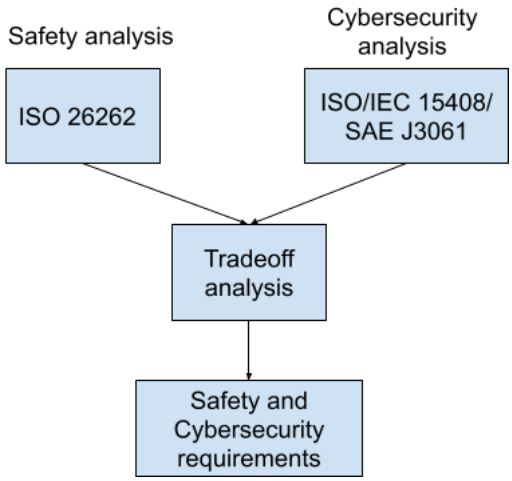

Figure 27: Safety and cybersecurity trade-off analysis

Figure 27, above, shows the approach that has been taken in the automotive vertical: safety analysis and cybersecurity analysis are being performed in parallel, i.e. there is no common safety and security model. A trade-off analysis was then be carried out to determine which trade-offs between safety and security needed to be taken.

Co-certification aspects between safety and security were not analysed further due to the complexity of the task. However OpenCert used to manage the safety and security assessment evidence. It was used to store evidences for the evaluation process, such as the ATE and AVA documents, and to generate the necessary argumentations to justify the assessment by using the previous stored evidences and explanations.

Table 21: Recommendation statuses R9 to R12

Recommendation	Status at M36
R9 Incremental cybersecurity certification experimentation	In Task T5.2 the automotive vertical is following a process to prepare for ISO/IEC 15408 Common Criteria certification. A protection profile (= generalised requirements for a class of systems) has been created to define the requirements on the automotive vertical, and was extended for experimenting with incremental certification (see the appendix of D5.4 for the protection profile definition) . It is also planned to have two iterations. The vertical is currently in the first iteration.
R10 Cybersecurity and safety co-certification	In task T5.2 safety and cybersecurity design are being performed separately, with trade-off analysis being performed after. Certification evaluation will only be carried out after trade-off analysis. Due to the complexity of safety/security co-certification, more emphasis was given to certification of cybersecurity in the automotive domain.
R11 Cybersecurity assessment tools for certification experimentation	In task T5.2 and T5.4 OpenCert was used to store development evidence for certification of the automotive vertical. OpenCert can be used to manage some of the ISO26262 data. Certification evaluation activities were carried out in T5.4 based on evidence stored in OpenCert.
R12 Integration of certification activities into continuous integration experimentation	Some of the automotive demonstration scenarios have expressed interest in using a continuous integration approach. In D5.4 several demonstration scenarios for assessing Connected and Cooperative Car Cybersecurity (CCCC) experimented with certification with a continuos integration approach using the OpenCert tool to store certification evidence.

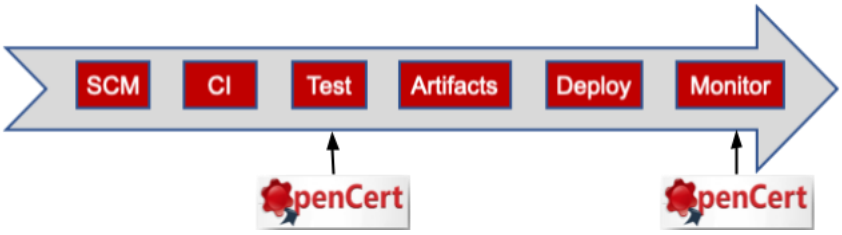

Figure 28: integration of OpenCert tool into continuous integration and deployment process

Figure 28, above, shows a possible integration of the OpenCert tool into the continuous integration and deployment process. Results from the testing phase could be compared to test specifications defined in OpenCert for compliance and saved as part of evidence and compliance management. OpenCert could also be used for compliance management during the monitoring phase. Use of OpenCert in the automotive vertical is under consideration.

Table 22: Recommendation status R13

Recommendation	Status at M36
R13 Sharing of certification evaluation data	The concept of sharing evaluation certification data between evaluation facilities is being analysed in task T11.3 and will be reported in D11.3. It is recommended to experiment with incremental certification in T5.2 to better understand how evaluation data must be structured. This concept defined in D11.3 was too complex to investigate in the CAPE research program. No CAPE demonstration contains any demonstration of sharing of certification evidence.

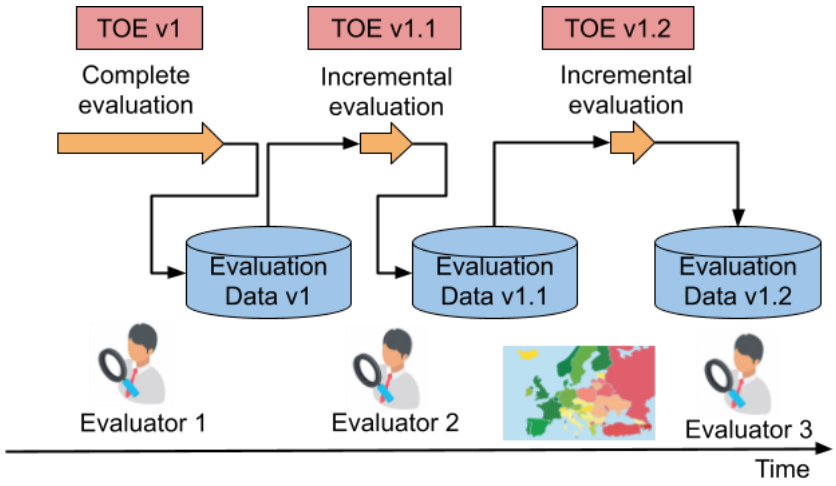

Figure 29: Incremental certification process - different evaluation organisations

Figure 29, above, sketches the incremental certification process for Common Criteria across different evaluation organisations. The figure shows a target of evaluation (TOE) evolves in time from v1 to v1.1 and v1.2. TOE v1 is the subject of a complete certification of the TOE with respect to a protection profile (PP). The first evaluation is performed by an evaluation organisation “evaluator 1” and evaluation data is stored as “Evaluation Data v1” in a standard and shareable format between organisations. The TOE then evolves to v1.1 and some changes are made to requirements of the PP. Some of the changes made to the TOE impact some of the requirements in the PP. The TOE needs to be certified again with respect to the impacted requirements of the PP. This is the subject of an incremental evaluation on TOE v1.1 performed by evaluator “Evaluator 2”. “Evaluator 2” could be an evaluation facility located in a different country than the first evaluation. It produces new evaluation data stored as “Evaluation Data v1.1”.

In task 5.2 two development iterations are planned. The first iteration is an opportunity to understand which certification data needs to be stored for future incremental evaluations. And the second iteration is an opportunity to experiment with incremental certification.

4.1.3 Risk Discovery, Assessment and Management for Complex Systems of Systems (CAPE Task 5.3)

Table 23: Certification schemes and standards for Task5.3

	ISA/IEC 62443	ISO 27034
Process certification	Multilateral certification system	Multi-part standard
Domain	Industrial automation and control systems	Integrate security into systems development life cycle (applications)
Organisation	Yes	Yes
Methodology	Yes	No
System development	Yes	Yes
Security profile	Yes	No

The above table compares two process-oriented certification schemes and standards. ISO 27034 has been selected as the most interesting process-oriented standard to analyse in T11.4 and T5.3. In T11.4 ISO 27034 is being analysed to determine how it can be applied to a cloud computing software development lifecycle.

Table 24: Task 5.3 recommendations

Recommendation	Justification
R14 Software development process-oriented certification: Analyse how these certification schemes/standards can certify agile software development processes.	Many software development projects are carried out in an agile manner where software products are released very frequently. Product cybersecurity certification approaches are not well adapted to frequent product releases. Process cybersecurity certification is an interesting alternative.
R15 DevSecOps process certification: How can these standards be implemented into a continuous integration and development process	Many agile software development projects now follow a DevSecOps continuous integration and deployment approach. It is possible to constrain the DevSecOps process to achieve process cybersecurity certification. This would lead to efficient process certification.

Table 25: Recommendation status R14

Recommendation	Status at M36
R14 Software development process-oriented certification	ISA/IEC 62443 and ISO 27034 are being analysed in task 11.4 to determine if they can be applied to Cloud software development lifecycle where new releases are deployed daily and by the hour. These results will be communicated to task T5.3 to decide how it could be applied. An analysis was performed on how the CAPE tools could support different process elements identified in D11.2. This is reported in D5.4.

Task 5.3 is currently planning a demonstration on the automotive vertical that focuses on the platooning functionality and not the cloud aspects of platooning. To illustrate process-oriented cybersecurity certification it is recommended to demonstrate it on the cloud part of the vertical where there is a rapid cycle of software product releases and deployment. ISO 27034 provides guidance on specifying, designing, selecting, and implementing information security controls through a set of processes integrated throughout an organization's systems development life cycles. For example, the application security control of ISO 27034 aims to prevent SQL injection by binding program variables in SQL statements. This control could be integrated into one the SPARTA verticals development process by tasking one of the SPARTA assessment tools to verify that all program variables are bounded. This is one of the verifications that can be made by the SPARTA Frama-C source code analyser.

Table 26: Recommendation status R15

Recommendation	Status at M36
R15 DevSecOps process certification	Task T5.3 is interested in using continuous integration and deployment to demonstrate results. If a continuous integration approach is followed, then some aspects of process cybersecurity certification could be experimented such as implementing some security controls in the DevSecOps process. This recommendation was too complex to be addressed in T5.3.

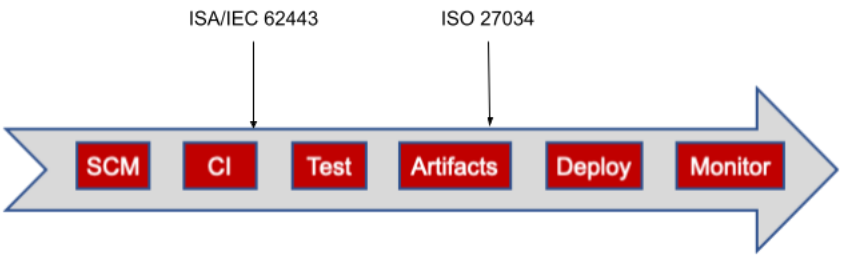

Figure 30: DevSecOps process certification

Currently there are no standards that define security for DevOps. ISO/IEC 27034-1 is more general and is a standard for the secure development lifecycle. Figure 30, above, suggests how a DevSecOps process could be constrained to comply with ISA/IEC 62443 or ISO 27034. This could

be experimented with in a task 5.3 continuous integration and deployment process. For example, the ISO 27034 security control for detecting unbound program variables in SQL statements mentioned above, could be verified by Frama-C in the DevSecOps process: Frama-C could be invoked during the testing phase of the DevSecOps process.

4.2 WP6 HAII-T – High-assurance intelligent infrastructure toolkit

IoT-connected devices are transforming infrastructure and making it evolve towards a true Intelligent Infrastructure. However, an intelligent and connected infrastructure must be protected from vulnerability that enables attackers to steal or affect sensitive data, personal data or control devices remotely. The HAII-T research program aims to consider security and resilience requirements in future II systems from the outset rather than being an add-on.

Discussions between HAII-T and WP11 have triggered interest in the topic in several activities in the HAII-T programme (WP6 tasks). Certification activities have been discussed and their use is being considered as future work.

The future EU cybersecurity framework has identified the area of IoT as a priority for identifying and preparing cybersecurity standards for the EU cybersecurity certification framework. Intelligent infrastructures cover a large variety of infrastructures with many existing standards, e.g. critical infrastructures. The work in HAII-T could be used to recommend new security controls for high assurance intelligent infrastructures.

4.2.1 Standards and framework relevant to HAII-T

The HAII-T research program is focusing on building a foundation for secure-by-design Intelligent Infrastructures and is working on IOT, Fog and clouds environments.

The general approach followed when discussing with participants of the program was to perform a risk assessment in order to establish which is the Target of the Evaluation by examining what needs protection, from which type of attack. Some general recommendations regarding cybersecurity certification standards that have been discussed are:

- The Industrial Internet of Things Security Framework [51] could be a good starting point for building secure IOT components.
- For all cloud related matters, the Security Trust Assurance and Risk (STAR) [52] provides a good balance of controls regarding security and privacy for cloud activities.

Table 27: Short comparison of the schemes

Criteria	The Industrial Internet of Things Security Framework	Security Trust Assurance and Risk
Issuer	Industrial Internet Consortium	Cloud Security Alliance
Scope	Product and process	Product and process

Criteria	The Industrial Internet of Things Security Framework	Security Trust Assurance and Risk
Type of companies or individuals	Large and small organisations, Operator, integrator	Large and small organisations, public entities
Technology areas covered	Risk management, Communication, Cryptography, Endpoint, Monitoring, configuration	Risk management, Communication, Cryptography, Endpoint, Monitoring, configuration, people skills, identity and access management, business continuity...
Different levels of certification	No	Yes, 1 (self-assessment to, soon, 3 (continuous monitoring)
Workload	Several weeks to several months	Several weeks to a year, depending of the chosen level

In term of their focus and activities in this research program and how they can introduce cybersecurity certification initiatives, the approach was a bit different for each of the tasks:

In **WP6 Task 2 -** the main focus was on Industrial Internet of Things Security Framework and Cloud certification;

In **WP6 Task 3** - Secure Orchestration for the Intelligent infrastructure, the KPI indicators for Certification criteria was investigated, cloud certification and initiatives. For the Intelligent Infrastructures and legacy issues, checking the security capacities of the old components, formal verification (network protocols) and how to maintain the security properties during operations and implementations

WP6 Task 4 - Resilience-by-design of Intelligent Infrastructures, which is based on fault and intrusion detection and tolerance the focus was different based on the nature of II systems and the implemented mechanisms for resilience. Each mechanism was encouraged to investigate relevant framework and certification standards.

WP6 Task 5 - Privacy enhancing mechanisms and tools, such as the GDPR compliance tool that uses BPMN model and performs checks on a process for GDPR compliance. The discussion was focused on introducing in the tool certification criteria or alternatively integrating the tool with a certification process. The discussions in this task were the most advanced and performed an analysis of integrating a cybersecurity certification process. Thus, this analysis is described in more detail in the following paragraph.

4.2.2 Analysis of adoption of cybersecurity initiatives and integration of the GDPR certification tool with the cybersecurity certification processes

The GDPR compliance tool, DPO Tool (dpotool.cs.ut.ee), uses “the BPMN notation to model a business process for evaluating the compliance level with the GDPR regulations. The users of the tool are asked a series of questions to identify GDPR-focused characteristics and attributes of the relevant elements in the process. This information is used to instantiate a compliance model of the GDPR, which is used to refine the process model and determine potential violations of the GDPR”[75]. After a careful examination of the tool and discussion with the development team some overlapping between the two processes have been identified as well as the need of integrating privacy and GDPR aspects, which became evident in incremental certification.

Discussion on common criteria and implication of GDPR in complex systems updates, the pilot parking service was identified as a good candidate use case to do a proof of concept.

Following the analysis of the GDPR validation and the incremental certification processes the focus was on how can GDPR validation be part of a DevSecOps continuous integration testing and deployment lifecycle that includes Cybersecurity certification and GDPR compliance testing. How we can integrate the DPO Tool and possibly other tools for GDPR validation with the CI/CD workflow. The diagram below (see Figure 31) summarises the result of this discussion.

The idea is that as with the cybersecurity certification, there will be two types of tests for GDPR compliance. The "static" ones (SAST in the diagram) that will test the BPMN model that the system analyst provides. The result of this test is recorded in the evidences registry and if it is passed it is published to the system developer and operators. If the tests fail the analysts receives feedback to modify accordingly the model. The "dynamic" tests (DAST) are applied to the deployed and running components of the system (such as the database or the service API). The results of this GDPR compliance testing are again stored in the evidences registry but this time the developer is notified for any compliance issues discovered.

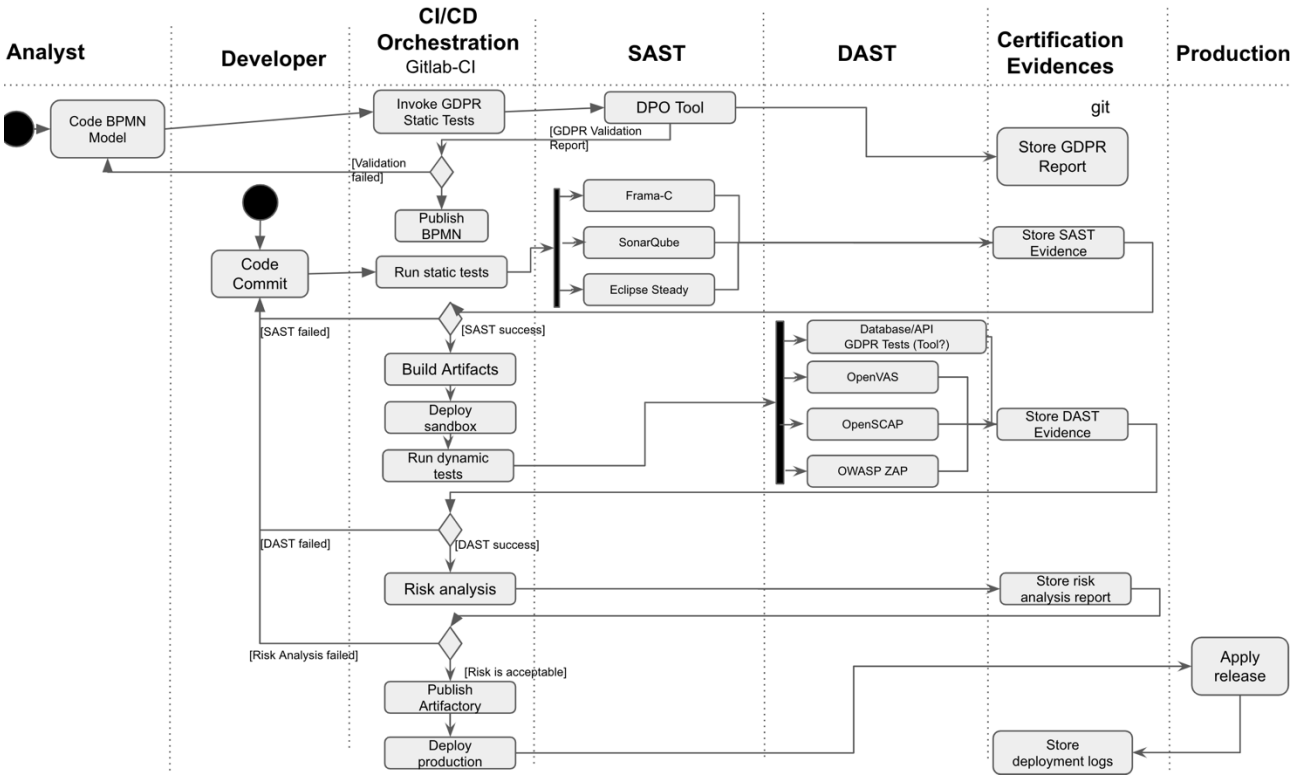

Figure 31: CI/CD Activity Diagram of certification with GDPR Compliance validation

Chapter 5 Collaboration with other European Pilot Projects

Contacts with the other pilots projects were taken during the M1-M12 period. Information was exchanged as regarding the project specific activities. It was difficult to have a structured collaboration, so a joint workshop approach was taken as a more flexible way to collaborate and have discussions on cybersecurity certification topics.

5.1 Summary of CyberCert 2020

CyberCert 2020 (First International Workshop on lightweight and Incremental Cybersecurity Certification, https://www.cetic.be/cybercert2020) was organised by SPARTA on September 7 2020 as an all digital workshop of the 5th IEEE European Symposium on Security and Privacy.

The topics of interest were selected to cover a broad set of topics relevant to cybersecurity certification and initiate collaborations: Integration of security engineering and certification processes, and incremental certification, lightweight certification schemes, e.g. for SME, Assessment tools for products, services and processes, Analysis of security and privacy issues in Certification, Models for authentication and privacy management related to certification, Audit and accountability related to certification, Policy models and policy management related to certification and Dynamic security techniques and certification.

The program committee was composed of SPARTA participants exclusively:

Name	Organisation
Florent Kirchner	CEA
Andrea Morgagni	LEONARDO
Volkmar Lotz	SAP
Tiziano Inzerilli	ISCOM
Pascal Bisson	THALES
Fabio Martinelli	CNR
Jeremy Grandclaudon	CETIC
Nicolò Maunero	CINI

Out of the 5 accepted papers, 2 were submitted by CyberSec4Europe partners and 2 by SPARTA partners. None of the papers reported on cross-pilot collaboration results. The agenda was the following:

Time	Title	Authors and affiliation
14 :00-14 :30	Introduction to workshop and EU cyber security act	Philippe Massonet – workshop chair
Governance and certification		
14 :30-15 :00	How to stop crashing more than twice: A Clean-Slate Governance Approach to IT Security Certification	Tobias Fiebig – TU Delft
15 :00-15 :30	From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium	Christophe Ponsard, Philippe Massonet, Jeremy Grandclaudon – CETIC Research Centre Nicolas Point – Multitel
15 :30-15 :45	Coffee break	
Product and process level certification		
15 :45-16 :15	Towards Incremental Safety and Security Requirements Co-Certification	Andrea Morgagni – LEONARDO Cybersecurity Philippe Massonet, Sébastien Dupont, Jeremy Grandclaudon – CETIC Research Center
16 :15-16 :45	Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach	Volkmar Lotz – SAP Security Research
16 :45-17 :15	JCMathLib:Wrapper Cryptographic Library for Transparent and Certifiable JavaCard Applets	Vasilios Mavroudis – University College London, Petr Svenda – Masaryk University
17 :15	Conclusions and end of the workshop	Philippe Massonet – workshop chair – workshop chair

5.2 Summary of CyberCert 2021

After the successful organisation of the CyberCert 2020 workshop, SPARTA and CyberSec4Europe agreed to co-chair a new edition of CyberCert and to invite the other pilot projects to the program Committee.

CyberCert 2021 was organised on September 6, 2021 as an all-digital workshop of the sixth IEEE EuroS&P 2021 conference. The topics of interest were similar to the previous version.

The workshop co-chairs were Philippe Massonet (CETIC, Belgium) and Tobias Fiebig (TU Delft, Netherlands). Representatives of the four pilot projects were invited to the program committee:

Name	Organisation
Thibaud Antignac	CEA, France
Volkmar Lotz	SAP, France
Artsiom Yautsiukhin	CNR, Italy
Nicolò Maunero	CINI/Politecnico di Torino, Italy
Kai Rannenberg	Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany
Chatzopoulou Argyro	TÜV TRUST IT GmbH, TÜV Austria Group, Germany
Liina Kamm	Cybernetica AS, Estonia
Vashek Matyas	Masaryk University, Czechia
Douglas Wiemer	Rhea Group, Belgium
Barbara Carminati	University of Insubria, Italy

Out of the 4 accepted papers, 2 were submitted by by SPARTA partners, 1 by CyberSec4Europe and CONCORDIA. The paper “Towards Cybersecurity MOOC Certification” reported on CyberSec4Europe and CONCORDIA cross-pilot collaboration results. An invited talk was given by Eric VETILLARD from ENISA. The agenda was the following:

Time	Title	Authors and affiliation
12:00 - 12:05	CyberCert Opening Remarks	Philippe Massonet (CETIC), Tobias Fiebig (TU Delft) – workshop co-chairs
12:05-12-30	Challenges in building cybersecurity certification schemes and how it interacts with research and standardization	Eric VETILLARD – ENISA
12:30 - 12:50	Towards Cybersecurity MOOC Certification	Matthias Beckerle, Argyro Chatzopoulou, and Simone Fischer-Hübner
12:50 - 13:10	Incremental Common Criteria Certification Processes using DevSecOps Practices	Philippe Massonet, Sébastien Dupont, Guillaume Ginis, Christophe Ponsard, Mirko

		Malacario, Claudio Porretti and Nicolò Maunero
12:10 - 13:20	MEDINA: Security framework for cloud service providers to achieve a continuous audit-based certification	Leire Orue-Echevarria Arrieta, Christian Banse, Juncal Alonso Ibarra, Luna Garcia Jesus, Fabio Martinelli and Artsiom Yautsiukhin
13:20 - 13:30	Questions and Answers, CyberCert Closing Remarks	Philippe Massonet (CETIC) Tobias Fiebig (TU Delft)

5.3 Further Collaboration

The CyberCert workshops provided an opportunity for the pilot projects to present their cybersecurity certification related research and activities. This allowed SPARTA to promote the collaboration work between CAPE and WP11 in the form of two research papers. The workshop format provided a opportunity for loose collaboration. However, collaboration between the four pilots projects on the topic of certification should be more structured in the future context of the European Cybersecurity Competence Centre (ECCC). The organisation of common workshops is certainly a good approach. However, the topics of interest were very diverse reflecting internal research interests of the different projects.

Since the entry into force of the Cybersecurity Act in 2019 a process has been defined for creating new certifications schemes. This is the responsibility of the Commission and ENISA. However, research on how to efficiently support the CyberAct certification framework could be organised within the ECCC and the competence network.

Chapter 6 Conclusions and Future Work

6.1 Recommendations and evolution of cybersecurity certification

Certification in cybersecurity, no matter the field, is now more than ever a necessity in order to build a safe and efficient cyber-world. However, cybersecurity certification is not a panacea that will resolve all cybersecurity issues.

But cybersecurity certification needs to be as much as possible an added value to products, processes, or services and not something that will create an entry barrier or distort competition.

It is also important not to forget the smaller actors such a SME's in designing "monster" schemes, necessitating large investment of time and money that will exclude smaller companies and can be a hindrance even for larger companies.

When developing a new certification scheme, it should:

- Be more agile in the cybersecurity certification processes,
- Provide an incremental certification process,
- Integrate cybersecurity certification process with security and privacy by design,
- Implement a better integration of safety and security standards (OT vs IT → OT & IT),
- Cover continuous monitoring of cybersecurity.

Small and medium enterprises

Regarding SME's, there is now a strong trend toward dedicated cybersecurity certification in several Member States. It is now time that the European Union take a closer look at all these schemes and initiatives and try to push a European SME's certification. It can be the beginning of a great cybersecurity journey for a company: to start with a scheme adapted for a SME, preparing it to meet the broader requirement of a scheme issued for the EU Cyber Act.

Composability approach

"Until a few years ago, security certification only applied to a limited number of products and processes. Schemes have been defined for each product or process category, which often became more and more complex over time, together with the ecosystem's own complexity.

Where a single evaluation initially applied to a complete device, it was first split into a hardware evaluation and a software evaluation, performed by different stakeholders. As the complexity of software kept growing, the software itself was separated into generic platforms and vertical applications.

Similar splits now appear in many fields, as complexity grows. Cloud-based systems, IoT deployments in factories or in cities, or even cars, are now so complex that a global certification can only be achieved by assembling certifications of components. Composition is the generic name for this assembly process [61].

It's becoming urgent to start looking at this issue. We are using more and more building blocks, software, and hardware, to create complex products. How to decide the security value of each

component's certification? And the way schemes produce security evidence is not the same so how can we compare them and their relative value?

This will be a growing field as we will certify more and more parts involved in complex products. Some actors such as ECSO and their partners are already looking at this and we should follow closely any new development.

6.2 Conclusion

Even if the certification landscape is heavily fragmented, measures are being taken in order to create a common ground for the creation of future certification scheme in Europe (EU Cyber Act). Current priority areas for European wide certifications schemes are IoT, industrial systems, and Cloud Computing. The current favourable context for cybersecurity certification in Europe is an opportunity for SPARTA to show that some of its results, and notably the assessment tools developed in the CAPE program, can be useful in a certification context.

The D11.1 deliverable provides an overview of the European security certification landscape, identifies relevant cybersecurity schemes and associated standards and provides concrete recommendations about integrating cybersecurity certification activities into the SPARTA research programs. A broader list of cybersecurity frameworks, best practices and standards is available in the Annex.

The D11.5 deliverable updates D11.1 with a summary of results from the recommendations for the CAPE research program, a summary of collaboration with the HAIIT research program on integrating GDPR requirements verification in an incremental evaluation process, and reporting on collaboration with the other pilot projects on the topic of cybersecurity certification of products/services, processes or people.

Chapter 7 Annex

7.1 SMEs

7.1.1 Comparison and analysis of SME's Cybersecurity Initiatives

It is critical to protect our SMEs because they are known to play a key role in the worldwide economy. In European countries they employ two thirds of the workforce and generate about 60% of the total added value [62]. Moreover, SMEs are a lot more fragile than bigger companies. Although the impact is lower in absolute value as shown in Figure 28, it is very high when compared to their revenues and it will also have a higher detection time, meaning a higher impact. According to J. Leclair [63], in case of attack, most SMEs will not get a second chance: about 60% of companies go out of business within six months after an attack.

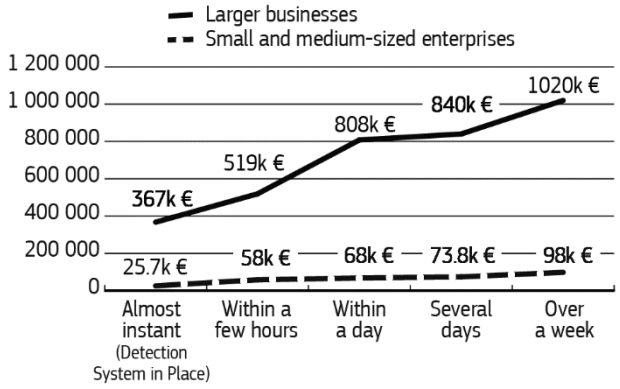

Figure 32: Financial impact of cyber breaches according to detection time [63]

Public authorities have also identified the need to help and even to force SMEs to become more mature in the way they address cyber security threats. At European level, many organisations such as ENISA, SME Alliance, the European Commission, European Cybersecurity Organisation (ECSO) are active in this area. At national or even regional scale, the need to support SMEs to face cyber security challenges has given birth to several initiatives aiming at defining and deploying specific labelling schemes. Those are usually operated by a network of third-party expert companies, supported by specific public funding that are also setting up the rules to operate in such a network. For example, the Cyber Essentials is supported by cyber security vouchers in United Kingdom [64]. Of course, such a work should not be done in isolation as stressed by Digital Europe [65]. It should be as much as possible aligned with strategic directions defined at the European level or in international standards. It should also learn from similar on-going work carried out in other countries.

According to the European SME Definition (2015), three criteria are taken into account:

- The staff headcount;
- The annual turnover;
- The annual balance sheet total;

The category of micro, small and medium-sized enterprises consists of enterprises which (as described in Figure 29):

- employ fewer than 250 persons; and
- have either an annual turnover not exceeding EUR 50 million or an annual balance sheet total not exceeding EUR 43 million

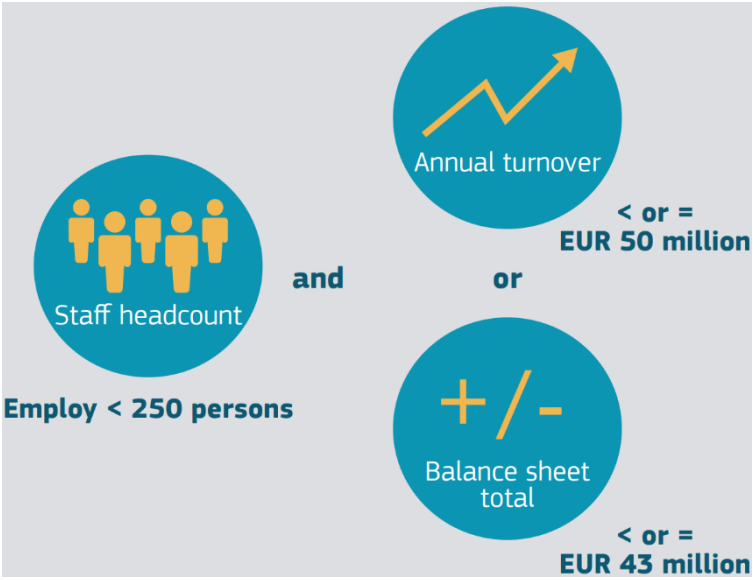

Figure 33: Three criteria [66]

- **"Micro-enterprises** are defined as enterprises that employ fewer than 10 persons and whose annual turnover or annual balance sheet total does not exceed EUR 2 million.
- **Small enterprises** are defined as enterprises that employ fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million.
- **Medium-sized enterprises** are defined as enterprises that employ fewer than 250 persons and either have an annual turnover that does not exceed EUR 50 million, or an annual balance sheet not exceeding EUR 43 million (as described in Figure 33)."[67]

Enterprise category	Headcount: annual work unit (AWU)	Annual turnover	or	Annual balance sheet total
Medium-sized	< 250	≤EUR 50 million	or	≤ EUR 43 million
Small	< 50	≤EUR 10 million	or	≤ EUR 10 million
Micro	< 10	≤EUR 2 million	or	≤ EUR 2 million

Figure 34: Three sizes of enterprises [67]

7.1.2 Selection of the SME's Cybersecurity Initiatives

Several European countries already possessed or are working on a dedicated solution for the cybersecurity of their SME's and their certification. We have chosen to present four of them in this document in order to give a broad overview of the existing initiatives. This is obviously a small sample and there are still many others schemes to consider. There is not yet a representation from Eastern Europe but some countries, like Poland with their PPHS cybersecurity standard, have projects ongoing.

We will present the schemes emanating from the following countries:

United Kingdom and Cyber Essentials:

This scheme is very successful in the UK and widely adopted by the companies, it is currently under modification after more than five years of exploitation.

Italy and their national framework:

Since 2015, they have developed a complete framework based on NIST for their critical infrastructures but also their companies, including the SME's, providing them with a holistic solution.

Belgium with Keep It Secure and Cyberfundamentals

We (CETIC) have created Keep It Secure (KIS) with the Walloon region (ADN) and participated in the elaboration in the Cyberfundamentals. The last one should include a certification component, missing otherwise in Belgium for SME's.

Finland and FINCSC

This is a recent scheme dedicated toward SME's and allowing companies to become official assessment bodies in order to spread FINCSC.

7.2 National cybersecurity schemes

7.2.1 United Kingdom

7.2.1.1 Cyber Essentials

Cyber Essentials is a UK government scheme launched in 2014 to encourage organisations to adopt good practices in information security. It includes an assurance framework and a simple set of security controls to protect information from threats coming from the Internet. It was developed in collaboration with industry organisations combining expertise in Information Security (ISF), SMEs (IASME) and standardisation (BSI).

There are five main controls, respectively covering: boundary firewalls/internet gateways, secure configuration, access control, malware protection and patch management.

Cyber Essential is organised in two levels of certification which must be renewed yearly. The first level is a basic level based on a self-assessment which is independently verified.

The second" Plus" level provides higher assurance through certifying the external testing of the organisation's cyber security. Certifying bodies are licensed (either for the basic or both levels) by five Accreditation Bodies which are currently appointed by UK government. The certifying bodies must demonstrate appropriate levels of quality assurance processes, security controls, and security assessment methodologies. They must also sign a code of conduct and provide technical competent and qualified staff to be mandated. To support SMEs in adhering to the approach, the UK government has deployed a specific voucher scheme including coaching, documentation, and certification.

It was quite successful: more than 30.000 Cyber Essentials and Cyber Essentials Plus certifications have been issued by over 200 Certification Bodies since the launch [68]. Once certified, the SME can also advertise about the fact it takes cyber security seriously boosting its reputation and providing a competitive selling point.

The scheme is constantly evolving but after consultations with several organisations and individuals, they will make several large modifications starting after Mars 2020.

Here some of some of the changes:

- Introducing a "minimum criteria" for certification bodies and assessors,
- Registered certification marks,
- Continuous collaboration and improvement,
    - Introduction of advisory services,
    - Measuring benefit,
    - Feedback on controls,
    - Levels of confidence,
    - Scope of certification,
    - Automation.

7.2.2 Italy

7.2.2.1 National Cyber Security Framework

In times of ever-increasing dependence on digital solutions in an increasingly interconnected world, it has become apparent that society has become more vulnerable. The current technological revolution and its global effects imply the need in Italy and elsewhere to tackle common opportunities and challenges through a systemic approach that must include public institutions, companies, academia and individual citizens.

A common, general challenge when it comes to cybersecurity is creating a clear legal framework and institutional architecture, so as to identify all entities responsible for cybersecurity issues. Italy made tremendous advances in creating a cybersecurity ecosystem and a new cybersecurity governance/strategy in the belief that a transparent and protected environment can contribute to creating a positive business environment favourable to the birth and development of new companies and investments in innovation.

This last point, innovation is key to the development of a healthy cyber-economy. New investments play a key role in activating a cyber-ecosystem, allowing research worldwide to be transformed into business opportunities. In general, a set of organic actions is needed to strengthen existing skills, intercept new talent and create new career paths needed to meet the technological challenges posed by cybersecurity and to improve the relationships between academia and private companies.

Joint efforts of all cybersecurity players must aim to build strong and resilient capabilities, particularly in specific sectors of cyberspace.

Priority areas to develop cybersecurity know-how are connected to defence and national security issues, critical networks providing essential services to end users and the protection of national businesses.

When it comes to ICT, cybersecurity is also fundamental to the protection of citizen rights. We live in an era where state surveillance powers are expanded, where global internet giants collect and record data on our behaviour, holding a knowledge of our most intimate beliefs and conduct, which can allow others to manipulate (such as in the case of the well- known “fake news” phenomenon) and intimidate us.

Cybersecurity is growingly focusing also on the financial sector, in which cyber-attacks pursue three specific goals: organize large-scale theft of financial data, temporary impairment of banking and insurance services, and violation of the integrity of data present within the banking system.

Italian companies are end-users of sophisticated solutions for cyber-protection, and at the same time, producers and exporters of advanced technologies, which position Italy among the most important players in the world cyber market.

7.2.2.2 Italian Cybersecurity Architecture

In 2017 and 2018, Italy streamlined and strengthened its cybersecurity structure in order to boost its cyber capabilities.

The Security Intelligence Department (DIS) is at the centre of the Italian cybersecurity ecosystem’s governance, acting as:

- Supporting body for the Prime Minister and the Inter-Ministerial Committee for the Security of the Republic (CISR) on cyber issues

- Chair of the Cybersecurity Management Board (NSC), an interagency and intergovernmental operational body within the DIS tasked with cyber crisis prevention, preparation and management (see Figure 31)
- European Point of Contact under the Network and Information Security (NIS) directive (see Figure 32)

The NSC is responsible for promoting Italy's participation in cyber activities (such as Cyber Europe organized by ENISA, the European Network and Information Security Agency) and other initiatives aimed at increasing national cybersecurity. NSC also contributed to the creation of the National Laboratory for Artificial Intelligence and Intelligent System and the Italian Industry Plan 4.0 Funding Program launched by the Ministry of Economic Development.

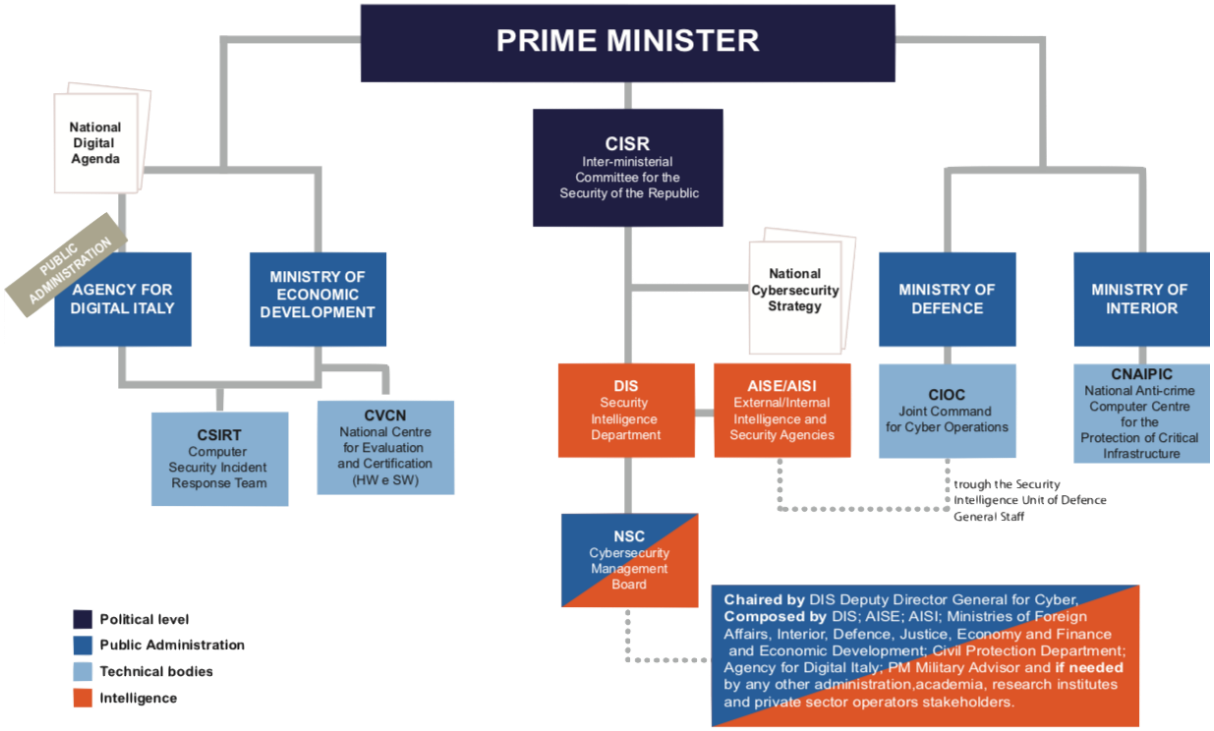

Figure 35: Italian Cybersecurity Architecture

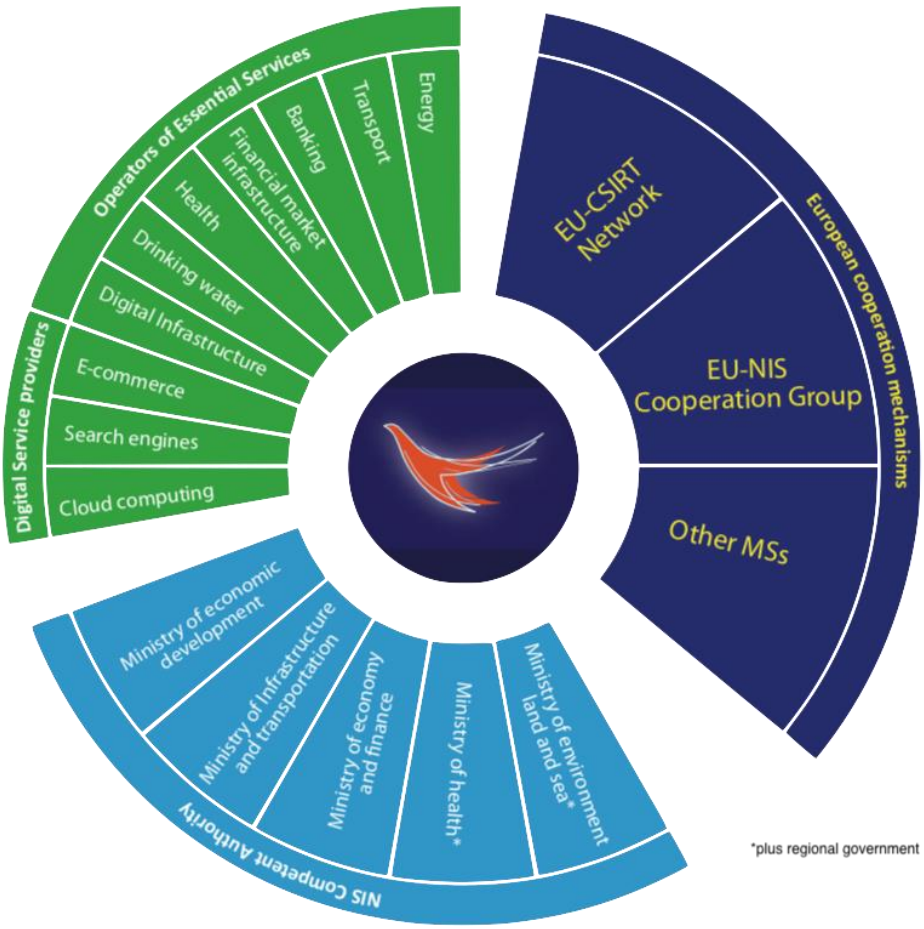

Figure 36: European Points of Contact under the NIS directive

7.2.2.3 The Italian Strategy

The Italian strategy provides guidelines for collaboration among both private and public stakeholders, as well as with academia and research. These guidelines aim to:

- Strengthen Italian critical infrastructures and other strategic players' defence capabilities;
- Improve cyber actors' technological, operational, and analytic capabilities;
- Boost public-private cooperation;
- Foster cybersecurity culture;
- Support international cooperation.

7.2.2.4 Cybersecurity Promotion

The Italian national strategy for cybersecurity promotes the integration and a synergistic approach between cyber security companies with different expertise with two main objectives. First, to develop new means and solutions at the national level to tackle cyber challenges. Second, create national "champions" to be able to compete at the highest international level. In this context, the Ministry of Foreign Affairs and International Cooperation together with other competent institutions, facilitates the development of a cyber supply chain, promoting national and international Business to Business

(BtoB), Business to Government (BtoG), and Government to Government (GtoG) cooperation agreements, and contributing to exporting Italian capabilities and strategic know-how globally.

Italian Economic Diplomacy is involved in supporting cybersecurity companies that are approaching foreign markets, thanks to the work of the wide network of Embassies and Consulates around the world. Each year, the Steering Committee for international promotion of Italian companies, co-chaired by the Minister of Foreign Affairs and International Cooperation and the Minister of Economic Development, sets Italy's priorities for bilateral commercial relations with other Countries. This activity includes the definition of target markets and export sectors, the organization of training activities for entrepreneurs, facilitating financial support for export strategies, monitoring opportunities in international markets and organizing dedicated systemic missions to enter emerging and innovative markets abroad, including the cyber security market.

The Ministry of Foreign Affairs and International Cooperation in cooperation with the Security Intelligence Department and the Ministry of Defence, has organized systemic missions in Washington, London, and many other relevant markets in order to foster the international promotion of national companies specialized in cybersecurity related fields, such as fintech, defence, energy and ICT.

7.2.2.5 The Ministry of Defence and The Italian Open Lab Experience

In the past few years, the Italian Government implemented specific initiatives to support companies, in particular Small and Medium Enterprises (SMEs) and start-ups, in their digitization and technological progress.

In 2019, the Ministry of Defence launched a program to support companies in the sectors of innovation and cybersecurity. This initiative, called Italian Open Lab, represents a new model of interaction between public institutions, private stakeholders and citizens. Its goal is to achieve, through structured brainstorming sessions, an improvement in the business environment to enable an increasing competitiveness of this sector in Italy and abroad.

Italian Open Lab seminars concern different subjects, such as network security and defence of critical infrastructures, with particular attention to the promotion of Italian strategic know-how and production capacity on cybersecurity.

7.2.2.6 The Italian Trade Agency and Cybersecurity

The Italian Trade Agency (ITA) is the Governmental agency that supports business development of Italian companies abroad and promotes the attraction of foreign investments in Italy. With a motivated and modern organization and a widespread network of overseas offices, it provides information, assistance, consulting, promotion and training to Italian small and medium-sized businesses. Using the most modern multi-channel promotion and communication tools, it acts to assert the excellence of Made in Italy in the world.

ITA's promotional strategy and activity for the cybersecurity sector have significantly increased over the past few years as a result of a careful analysis and understanding that includes the needs of the start-up world. ITA pays continuous attention to the evolution of this domain (including Fintech and blockchain) in international markets and in specific sub-sectors; it organized and participated in events in the USA and UK and is planning promotional actions in the most developed countries when it comes to IT security.

Promotional initiatives include participation at major international events, invitation of foreign delegations to Italy at specialized fairs and forums, and organization of workshops, seminars and

B2B initiatives in specific markets on particular topics identified by the ITA's Innovation Desks in London, Los Angeles, Mumbai, Singapore, Moscow and Paris. ITA regularly involves Italian Universities, accelerators and incubators in selecting Italian start-ups with innovative cybersecurity software and hardware solutions.

7.2.2.7 Research and Innovation

The Italian strategy on cybersecurity considers research a pillar for a reliable cyberspace. Universities, research centres, innovative start-ups and other Italian players involved in the development of cybersecurity technologies interact with public institutions and private companies to ensure the development of resilient capabilities and let Italy take a primary role as an attractive and competitive player in cybersecurity.

Established in 1989 under the supervision of the Ministry for Education, University and Research, CINI (National Interuniversity Consortium for Informatics) is a consortium of Italian universities that involves 1,300+ professors of both Computer Science and Computer Engineering from 45 public universities. It also supports joint research activities with universities, institutes of higher education, research institutions, industries, and public administrations. Finally, CINI facilitates access and participation in R&D projects, scientific activities and technology transfer.

The Italian Innovation Network

Italy has equipped itself with an efficient and functional innovation ecosystem in order to create and manage an integrated research program on the main technological drivers and to develop services and applications for businesses, institutions and citizens.

The Italian innovation network aims at seizing and exploiting the opportunities offered by digitization and to ensure the country's medium- and long- term competitiveness.

In order to support investments in digitization, the system integrates public and private subjects' networks, which are functional and complementary, so as to experiment and test digital innovations for the market: Competence Centres (CC), Digital Innovation Hubs (DIH) and National Technological Clusters (TC).

Digital Innovation Hub

In line with the European strategy on industrial digitization, the Government promotes the Digital Innovation Hub (DIH) network at the regional level as a gateway for companies to access digital transformation. Its purpose is to set up competence centres, technology experts, suppliers, end-users of technological solutions and investors to support the access of enterprises to the EU market. DIHs are the contact point among companies, research institutions and both public and private investors at regional level.

National Technology Clusters

To boost innovation processes and increase Country's industrial competitiveness through a more effective integration between national and regional policies on research and innovation, Italy has promoted the development of 12 National Technology Cluster The clusters are formed by companies, universities, research institutions, technology districts, start-up incubators and other stakeholders in the field of innovation.

In the framework of the National Smart Strategy, according to EU guidelines, each Cluster is focused on a specific technology field: aerospace, agri-food, green chemistry, intelligent factory, transport, life sciences, technologies for living environments, technologies for smart communities, cultural heritage, design, creativity and Made in Italy, sea economy and energy.

The aim of each Cluster is to develop represent structural collaboration platform for enterprises and R&D entities that help enhance research and technology transfer to the business system.

Competence Centre

The Competence Centres (CCs) are public-private partnership centres, vertically specialized in the technological fields of industry 4.0 to facilitate technology transfer to Italian companies. The centres offer training and support activities in the implementation of innovative projects, industrial research and experimental development of new technologically advanced products and services.

Two of these Competence Centres are focused on wide-ranging cybersecurity:

- Cyber 4.0, the Competence Centre of central Italy, is dedicated to data security and focused on solutions for the strategic sectors of automotive, space and healthcare.
- Start 4.0 is the Competence Centre for Security and Optimization of Strategic Infrastructures, based in Genoa. This CC focuses on enabling technological application of Industry 4.0 (IoT, blockchain, big data) in the field of security (security, safety and cyber), on the application domains of infrastructures for transport (including ports), energy and water and production systems.

7.2.2.8 Economic Trends

Implementing effective cybersecurity measures is particularly difficult today since cybercriminals are becoming more experienced in their attacks. The number of cyber-crimes and targeted attacks are rising rapidly, leading to a considerable growth in demand for services and security solutions. Nevertheless, cybersecurity can also be an opportunity. There will be 1.5 million cybersecurity job openings by 2019, and by 2025 the demand for cybersecurity professionals will increase to approximately 6 million globally [69].

7.2.3 Belgium

7.2.3.1 Cyber & SMEs

“Belgium can be considered an SME country par excellence, both in terms of employment as in added value. SMEs account for 69,3% of total employment and 62,4% of added value (€134,1 billion). In total, SMEs generate 1.978.527 jobs.

Unfortunately, 1% of Belgium's annual gross national product (4,5 billion EUR) is lost due to cybercrime. A computer virus blocks access to data or to the entire business process, the online shop is no longer available due to the work of a hacker, or all credit card details of the customers become public by an innocent click on a link, with many legal and trust problems as a result: Cyber incidents can seriously harm companies.

The main known breaches are caused by phishing, malware, human error, theft or loss of data. The intent is often vandalism, political, financial or ideological motives or damaging a competitor.

Cybercrime is not just a problem for large companies but affects increasingly SMEs, including self-employed workers. According to the CCB, no less than 60% of SMEs are targeted by cyberattacks.

As a result, almost two out of three Belgian companies (65%) experienced economic losses in the past two years due to Cybercrime. In 9% of the cases, this involved more than 10.000 EUR. A survey conducted by UNIZO in 2017 showed that three out of ten entrepreneurs became victims of phishing in the past year and one out of ten entrepreneurs was hacked.

Cybercrime not only causes damage but can also result in additional sanctions, for instance, where the GDPR is applied. After all, this law obliges companies to better protect the data of individuals. A leak of personal data can therefore lead to high fines.

Cybercrime and complex European legislation form an increasing challenge for the SME environment. Unlike large organizations, most SMEs do not have their own cyber security teams (CSIRTs). Cybercriminals who want to gain financial advantage or seek to damage companies tend to target the smaller and less secured ones. Today, corporate security - with classic areas of activity like fire protection, protection against burglary, theft, and sabotage - needs to be complemented by the aspect of information security.

Comprehensive security measures involve know-how and considerable effort, leaving SMEs often depend on measures taken by an external IT provider to ensure a solid level of security. However, it is often difficult for SMEs to evaluate which products and measures offer a higher level of security or which are just not worth the cost.

In September 2017, UNIZO interviewed 475 entrepreneurs about cyber security. The majority (56%) takes limited measures (firewall, antivirus, etc.). One fifth uses external IT partners, but 10% of these companies are not aware of the measures taken by the IT provider. Compared to 2016 this study also noticed a decrease in the use of IT codes of conduct, such as clear agreements on the use of social media, (mobile) devices, and passwords, which is a worrying evolution.

European directives, digital developments and challenges make information security a crucial issue for all SMEs. After all, economic growth and prosperity are created by entrepreneurship in a secure environment. Recently, the demand for support has become louder and louder, in order to improve cyber security and to provide more clarity. Both companies and their suppliers are looking for methods to support their efforts.

This trend can also be seen in other Member States, where some have already taken appropriate initiatives. The United Kingdom issued a certification for SMEs in 2017. Around 30.000 self-assessments and certificates have since been used by the business community. The GDPR was the main reason for the increase in applications. In Germany there is the VDS-certificate for SMEs, which cooperates with insurance companies. Finland is currently also preparing their SME certification.

The above aspects have led a team of public-private actors in Belgium to explore a pathway to allow Belgian SMEs to check, improve, and assess their information security status [70].

7.2.3.2 Keep IT Secure

In Belgium, the effort is currently structuring at the two levels depicted in the figure 33:

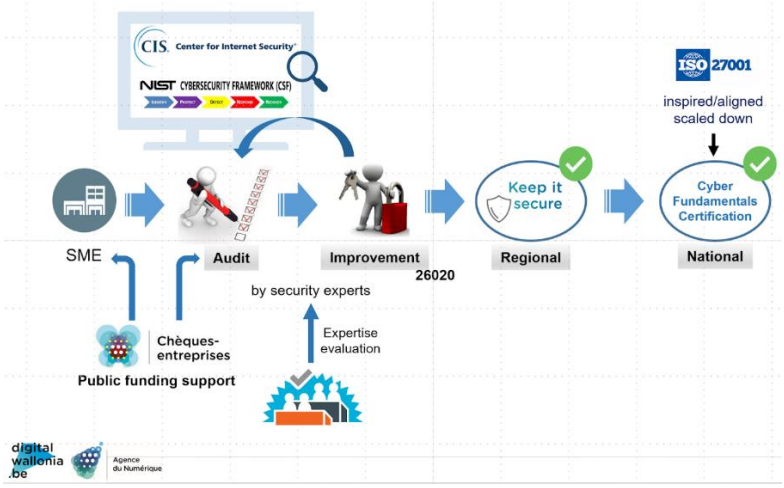

Figure 37: Cybersecurity process in Belgium

The regional level is responsible for the non-certifying audits which aims at ensuring SMEs have identified key cybersecurity risks and have taken adequate measures to manage them. They are helped in this task by validated cybersecurity experts. In Wallonia, the driving initiative is called "Keep IT Secure" and is led by Digital Wallonia [70]. Expertise is validated by an advisory board which checks that experts master cybersecurity fundamentals and can conduct assessment and improvement activities with SMEs. A funding scheme is also available through specific cybersecurity vouchers that will only support the intervention of validated experts.

The national level is concerned about providing certification based on a light certification scheme inspired by ISO27K. It under development by Centre for Cybersecurity Belgium which is also supporting awareness actions such as cybersecurity guide for SME [71].

Keep IT Secured emerged after a long maturing period started in 2017 and involving public authorities, research centres, a local cybersecurity cluster and end-user SMEs through specific awareness-raising events. During our elaboration process, we have also been inspired by other European initiatives as described by C. Ponsard.

Unlike other domains where posterior control is possible, the sensitive dimension of cybersecurity requires ensuring, prior to any service, that service providers are qualified experts w.r.t their ability to:

- identify and manage risks related to the various types of information held by the company especially in the SME context,
- implement adequate protection mechanisms for the various types of systems that contain and manage information.

the following key abilities are required and need to be checked:

- general purpose expertise in cybersecurity and reference frameworks,
- ability to embrace all SME-specific cybersecurity issues,
- ability to carry out organisational and technical audits, according to a well-established, methodology that may be their own.

The criteria are based on international standards and inspired by European labels. These include the NIST Cybersecurity Framework, the 20 key criteria of the Centre for Internet Security (CIS), similar approaches undertaken in other countries (eg. CyberEssentials in Great Britain). These criteria cover the main steps of a cybersecurity risk management approach: identification - protection - detection - response - recovery. The precise methodology is left to the discretion of the auditor but to consider the 20 key criteria of the CIS. The criteria are also only significant in their contextualisation in relation to the risks incurred. The capability to perform risk assessment is also evaluated during the interview process based on case studies where basic risks and then more complex risks are progressively injected.

General Interview Process

The interviews are carried out individually, even if several experts from the same organisation are reviewed. It is led by two specialists from the cybersecurity expert advice centre and lasts for a maximum of two hours. After having welcomed and explained the KIS framework, the expert is asked to give an overview of his professional training and experience. KIS does not impose a methodology on the provider but checks the coverage of fundamentals that guarantee a good mastery of cybersecurity within SMEs. To do this, a few concrete scenarios are presented and serve as support for a dynamic discussion to evaluate the following aspects:

- Identification of risks in relation to the context of the SME,
- Main strategies from prevention to recovery using NIST CSF at top level,
- Use of basic controls, based on a detailed checklist inspired from CIS20 but structured around NIST CSF.

Checklist

The checklist is organised as a spreadsheet divided in seven main tabs. First an overview tab for filling the administrative and evaluation information, then a help task explaining the global structure and then five tabs corresponding to the five NIST CSF categories. Those tabs are easy to fill using click control and have room for comments. While an assessor is asking a question, the other is filling and checking to prepare more questions on issues that have not yet been covered by expressing them in the scope of the supporting cases. An interesting way to use it is to upload it on a collaborative platform so it can be filled collaboratively. So, the sheet can efficiently help to both drive and control the interview and allow the interview to hop from a topic to another while keeping track of everything. As an example, the Identify tab is depicted in Figure 34. Each tab is composed of a main categories and then more detailed section with checks organised by levels: basic, intermediate and advanced. As the interview progressed basic checks are first covered and the progressively more complex ones, but the discussion can also go more quickly deeper in detail on some topics and already cover intermediate and advanced topics. The coverage of all advanced topics is also not mandatory and left to the interviewers.

	A	B	C	D	E
1	**Identify**				
2					
3	This feature focuses on how the organization perceives its risks relating to IT. it includes to understand the context of the company, critical resources, etc ...				
4		**Spontaneous**	**Questionned**	**Sufficient**	**Problems**
5	**Categories:**				
6	*Presence of a computer inventory?*	☑	☐	☐	☐
7	*The company's business is clear*	☐	☐	☑	☐
8	*Vulnerable resources are identified*	☑	☐	☐	☐
9	*Security policy in place?*	☑	☐	☐	☐
10	*The risks to the company are identified*	☐	☐	☐	☑
11					
12	Basic				
13	Presence of a computer inventory?	☑	☐	☐	☐
14	The company's business is clear	☐	☑	☐	☐
15	Vulnerable resources are identified	☑	☐	☐	☐
16	Security policy in place?	☑	☐	☐	☐
17	The risks to the company are identified	☐	☑	☐	☐
18	#VALUE!				
19	Intermediate				
20	The risk management process in place	☑	☐	☐	☐
21	The company's risk level is determined	☑	☐	☐	☐
22	Having a detailed software inventory	☑	☐	☐	☐
23	The sources of information on cyber security are identified and	☐	☐	☐	☐

Figure 38: Excerpt of the ”Identify” tab of the assessment spreadsheet

Supporting scenarios

Scenarios are not described in detail here for evident reasons but are composed of two main cases: one very basic, focus on a SME with basic needs of IT infrastructure and one more specialised in order to be able to ensure a wide coverage. Each case is explored with a raising level of threats. The first case is typically inspired from a traditional domain with a limited IT support: basic network, few workstations, configuration close to domestic use. It then develops the scope of the business activities to increase its dependencies on information technology through on-line orders, transactions, more complex networks, remote access, etc. A complementary case is also used to explore more specific problems such as high availability and sensitive information, e.g. in health or logistics.

7.2.3.3 Cyberfundamentals

The Cyber Fundamentals Initiative aims to support SMEs to arm themselves - in a simple and cost-efficient way - against increasing cybercrime that threatens their turnover, profitability and reputation. Moreover, through this initiative SME will be able to rely more correctly on their external ICT services, to facilitate the implementation of the European regulations, and to keep and enhance the trust of their customers.

This initiative is specifically designed for small and medium-sized companies and aims to ensure a minimum level of security without overburdening the companies organizationally or financially. The recommended measures can be implemented by the company's own specialized staff (IT department or IT security responsible) **or their IT professional or service company**. The Cyber Fundamentals make it possible to check whether a company has minimum protection against basic threats from cyberspace (network, firewall, VPN access, mobile devices, web servers, e-mail & password use, etc.).

The Cyber Fundamentals contain minimum requirements for the security of ICT, a series of basic technical controls, relevant information on the organizational and technical implementation of information security. These minimum requirements will help organizations to protect themselves against common online security threats, but they also offer opportunities to gain consumer trust.

The aim is to support and encourage SMEs to raise their level of cyber security through a defined path that CCB (2016). Cyber Security Guide for SME is fast, simple and cost-effective to implement. In addition, it will make it easy for SMEs to check whether the cyber-measures they have already applied are sufficient. The Cyber Fundamentals will help to address different compliance requirements, such as the GDPR, but it will also help to reduce the risk of becoming a victim of the most common cyberattacks.

While the CCB and Cyber Security Coalition have initiated the development of the Cyber Fundamentals a huge coalition of professional and governmental organization joined forces all centered around a common vision to make our SMEs cybersecure.

Principles

The Cyber Fundamentals aim to support SMEs in building achievable cyber security. It will contain many basic components of the ISO 27001, albeit with an important focus on cyber security and a specific focus on:

Current and effective measures, which are generally accepted as minimum measures, an average company can implement, within acceptable budgets, which can achieve the best possible results, and are measurable.

The initiative will be phased, each corresponding to a maturity level with complementary and incremental deliverables all on a voluntary basis.

Phase - 1 – "Self-Awareness": development of a **self-assessment questionnaire** on measures required to ensure protection against a wide variety of the most common cyberattacks. The self-assessment process is designed to be lightweight and easy to follow through several steps. This questionnaire focuses on internet-connected devices (both company devices and personal devices) which contains company data (both company information and operational information) and which can be attacked with the help of widespread, easily accessible tools by attackers with limited or average knowledge.

Phase - 2 - "Cyber Fundamentals Self-declaration": Based on the priorities of the company and at the pace they feel appropriate the identified defects, issues will be remediated through their internal resources or by a cyber security or IT professional.

Successful completion of this process, meaning remediation of the remaining issues, and a cosignatory by a recognized cyber security professional will allow the company, on a voluntary basis, to apply for a "Cyber Fundamentals label". The voluntary list of "labelled" companies will be kept on a website.

Optional Phase 3 (still ongoing discussion) – "Cyber Fundamentals Certification": After implementation of Phase 1, 2 and a positive assessment of the program a certification recognized by the National accreditation body (BELAC) can be initiated.

The measures required will remain the same, but this time the verification will be carried out independently by a certification body. The self-declaration will be validated by an onsite audit.

Technical requirements

In terms of content, the Cyber Fundamentals will include the following themes: password management, the configuration of firewalls, account management and the presence of policies in the event of incidents.

The initiative will consider the Cyber Security Act, certification initiatives of Germany, France, Great Britain, and Finland.

On a yearly basis the content of the technical requirement will be reassessed.

SMEs can be sure - through the Cyber Fundamentals - that the right tools, processes, and knowledge have been applied to protect themselves and their customers' data from the most common cyberattacks.

The Cyber Fundamentals program should be seen as supportive and encouraging. After all, a strong SME playing field in Belgium in the field of cyber security guarantees a strong Belgian economy. A measurable and recognizable way for SMEs to demonstrate their active engagement to making their environment safe for their customers is necessary for the continuation of an even competition with foreign companies.

7.2.4 Finland

The country published in November 2019 the updated version of their Cyber Security Strategy. This an improvement from the 2013 version and is linked to the Security Strategy of the Society. That strategy and its implementations are also part of the EU Cyber Security Strategy.

The goal is to support the development of accessible and reliable digital services and business development. This is the beginning of the National Cyber Security Development Programme. A new management coordination model supports the preparation of the development programme, taking into account the planning and cooperation for cyber security for public administration and the business community. The programme will improve the cyber security situation picture and integrate planning with other activities, such as economic planning.

The strategy is built on 3 strategic Guidelines [72]:

- Development of international cooperation – protection of the cyber environment without borders
    - “Finland strives to secure its cyber environment while enjoying active support internationally and through EU cooperation
    - International cooperation is vital for Finland’s cyber security as it benefits Finland to closely cooperate with international actors multilaterally, regionally and bilaterally. This is true for cooperation and dialogue on both technical and political levels”
- Better coordination of cyber security management - planning and preparedness
    - “The overall state of national cyber security will improve through a development programme and by promoting cooperation in planning and monitoring.
    - So far, the implementation programmes of the 2013 cyber security strategy have been based solely on proposals from actors committed to its development and the partly sectoral work of the competent authorities. Effective cyber security planning requires

that the necessary financial resources and cooperation are considered with sufficient precision in each administrative branch. This will be improved by a cyber security development programme extending beyond government terms; this will replace the earlier implementation programme. The programme will concretise national cyber security policies and clarify the overall picture of cyber security projects, research and development programmes."

- Development of cybersecurity competence- everyday skills and top skills as cyber security safeguards
    - "National cyber security competence will be ensured by identifying requirements and strengthening education and research
    - Finnish society needs cyber security competence both in public administration and in the business community. National cyber security will be built in cooperation among the authorities, the business community, organisations and citizens, when everyone can contribute to our shared cyber security. Each individual is therefore an important cyber security actor who can improve cyber security through his or her actions on a daily basis and thus impact his or her own cyber security and that of others. At the national level, it must be ensured that everyone has sufficient capacity to operate safely in a digital environment."

7.2.4.1 FINCSC

To support the implementation of the Finnish National Cyber Security Strategy, they have developed a cost-effective certification mechanism for business of all sizes, the Finnish Cyber Security Certificate or FINCSC, with the public and private sector actors. It is dedicated to ensure the business continuity and a proper data protection for Finnish companies.

They are working on two main pillars:

First, the knowledge development where they are developing and improving the cyber security knowledge and understanding in society and the requirement management in order to setup a "common criteria" for organizations for managing cybersecurity.

During the certification process, the organization's activities are evaluated against a fixed set of criteria.

They are looking into the computing environment, the processes and practices but also how the personnel is dealing with IT operations.

By example, they evaluate the followings parts:

- **Processes**
    - Policies and practices,
    - Work instructions.
- **Personnel**
    - Users,
    - Administrators.
- **Technology**
    - Premises,
    - Storage units,
    - Data erasure solutions.

- **Facilities**
  - End devices,
  - Intermediary devices,
  - Storage devices,
  - Software and applications.
- **Out of scope**
  - Internet,
  - Service providers,
  - Public services.

The mechanism is maintained by cyber security research, development and training center JYVSECTEC depending from JAMK University. JYVSECTEC works in close cooperation with the assessment bodies and advisory board. The advisory is composed from representatives coming from the business side and the public administration.

FINCSC provides three services for Finnish companies:

The FINCSC certification

It is based on an online self-assessment questionnaire and checks the adequacy of the organization's security controls and privacy practices. After completion, the questionnaire is examined by the assessment body and if found satisfactory, the company is certified for 1 year.

The FINCSC PLUS certification

The "basic" certification is required to ask for the PLUS certification. On top of the questionnaire, the company must prepare an on-site audit and collect concrete evidences. An external assessment body will then organise the audit itself and performs physical inspections, personal interviews...

If the audit is successful, the company is then certified for a three-years period.

Becoming an assessment body

To deliver FINCSC certification, a valid FINSCSC certificate is required and the company will need to demonstrate the organization's qualifications to provide certification services. The process includes multiple verifications and trainings. Authorization is applied separately for each certification level.

7.2.5 Comparative analysis

Table 28: Comparison of SME-oriented approaches

Name	Type	Country	Organisation	SME	Controls	Tools	Scheme	Maturity	Since
Cyber Essentials	Label	UK	Gov.	Yes	5 mains areas	Online self assessment	Accreditation and certification	2 levels	2013
Italian Framework	Frame-ework	Italy	CINI	Yes	Based on CSF 11 guidelines	Unknown	N/A	4 levels	2015

Name	Type	Country	Organisation	SME	Controls	Tools	Scheme	Maturity	Since
KIS	Label	Belgium	ADN	Yes	Based on NIST + CIS 20	Ongoing development	Accreditation	1 level	2018
Cyber fundamentals	Label	Belgium	CCB	Yes	Based on ISO 27001	Ongoing development	Accreditation and soon certification	2 levels	2019
FINCSC	Certifi-cation	Finland	JYVSECTEC	Yes	Unknown	Self assessment questionnaire	Accreditation and certification	2 levels	2019

The existence of multiple cybersecurity certification for SME initiatives in different European counties shows that this is a topic of interest. After all companies employing fewer than 250 people represented 99 % of all enterprises and 66.3% of total employment in the EU for 2015 according to Eurostat. Helping SME to protect themselves sufficiently will clearly have an impact on limiting the socio-economic consequences of cybersecurity attacks and will contribute to the general level of protection of companies in the EU.

While SME are free to use the most relevant cybersecurity standards relevant to their activities, they seldom have adequate means to protect themselves. For example, while they may have a team of IT system administrators, they may not have dedicated cybersecurity experts. While this is true in general for SME it is even more acute for very small businesses that occupy between 6 and 20 employees. Therefore, SME specific initiatives, that may rely on existing cybersecurity standards, are needed to help SME understand the threats they are facing and how to address the high impact cybersecurity risks.

The above comparison shows that the different European SME initiatives are all different and complement each other. While several countries have started SME initiatives and others have not, the latter could benefit from the experiences gained by countries that have already started. In the context of the EU cybersecurity act and the cybersecurity certification framework, cybersecurity certification for SME is clearly an area that would benefit from convergence at European level. A European wide standard should be very progressive and voluntary to allow SME to improve their protection levels at their pace and not view it as a burden. A flexible European wide certification standard for SME would allow countries that have not yet taken SME initiatives to benefit from experience in other countries.

7.3 Compilation of existing standards [44]

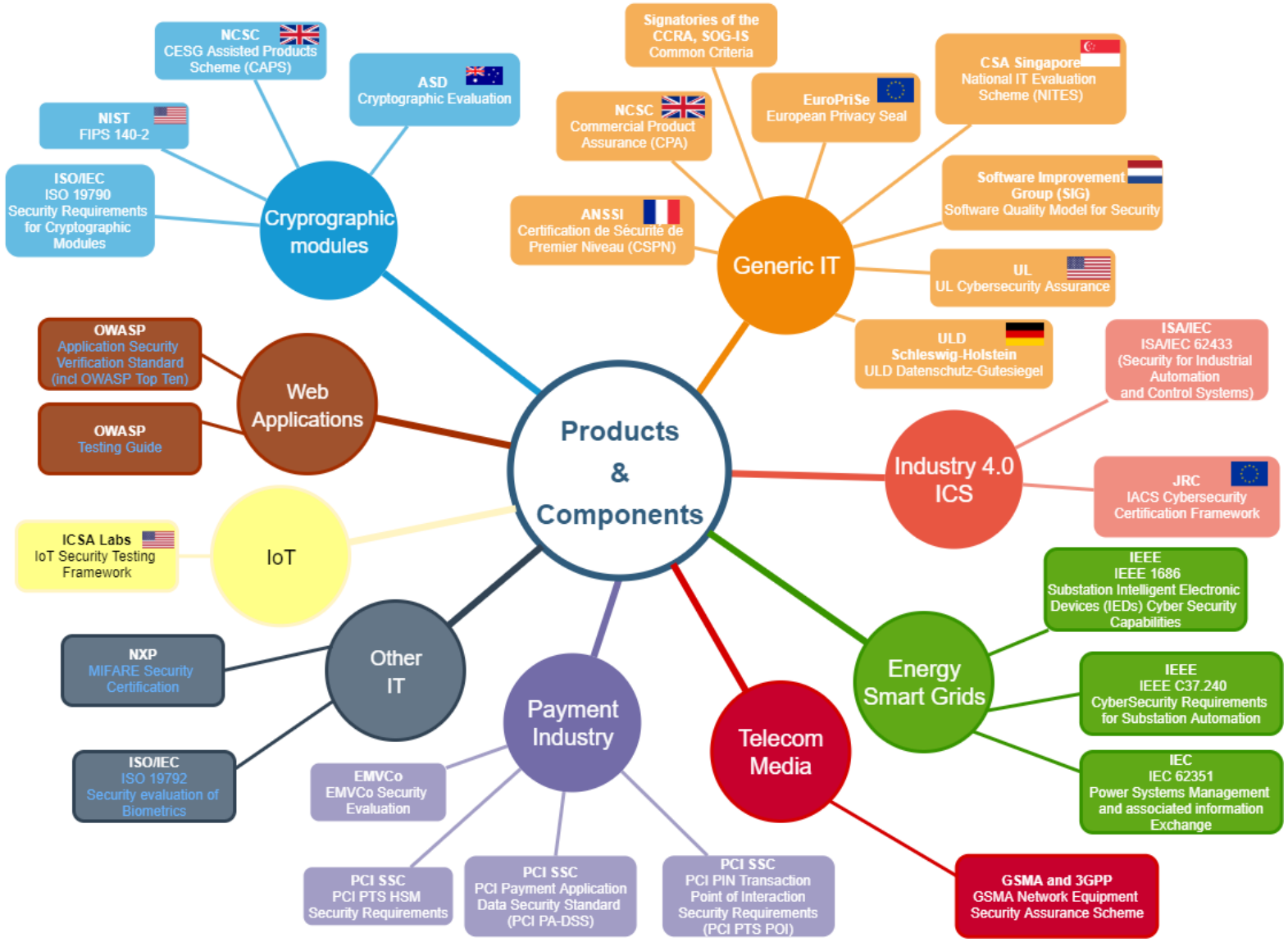

Figure 39: Standards and Frameworks - Products and Components

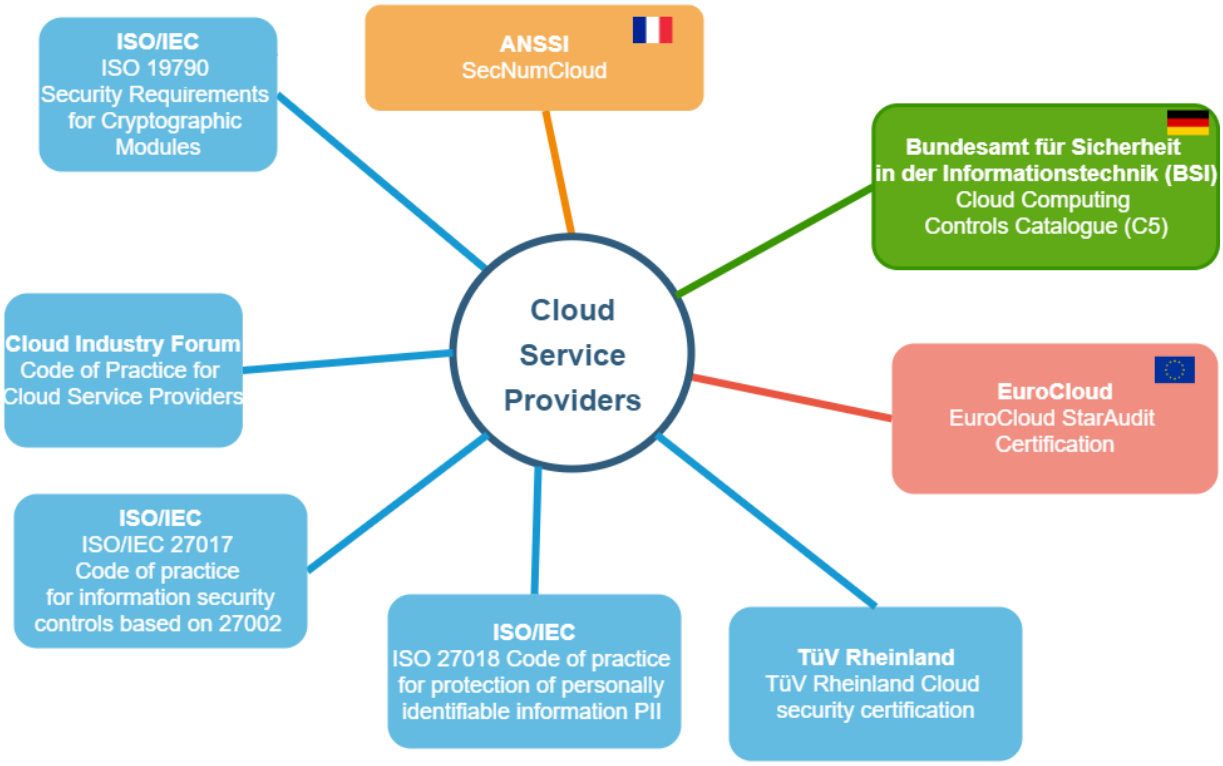

Figure 40: Standards and frameworks for Cloud Service Providers

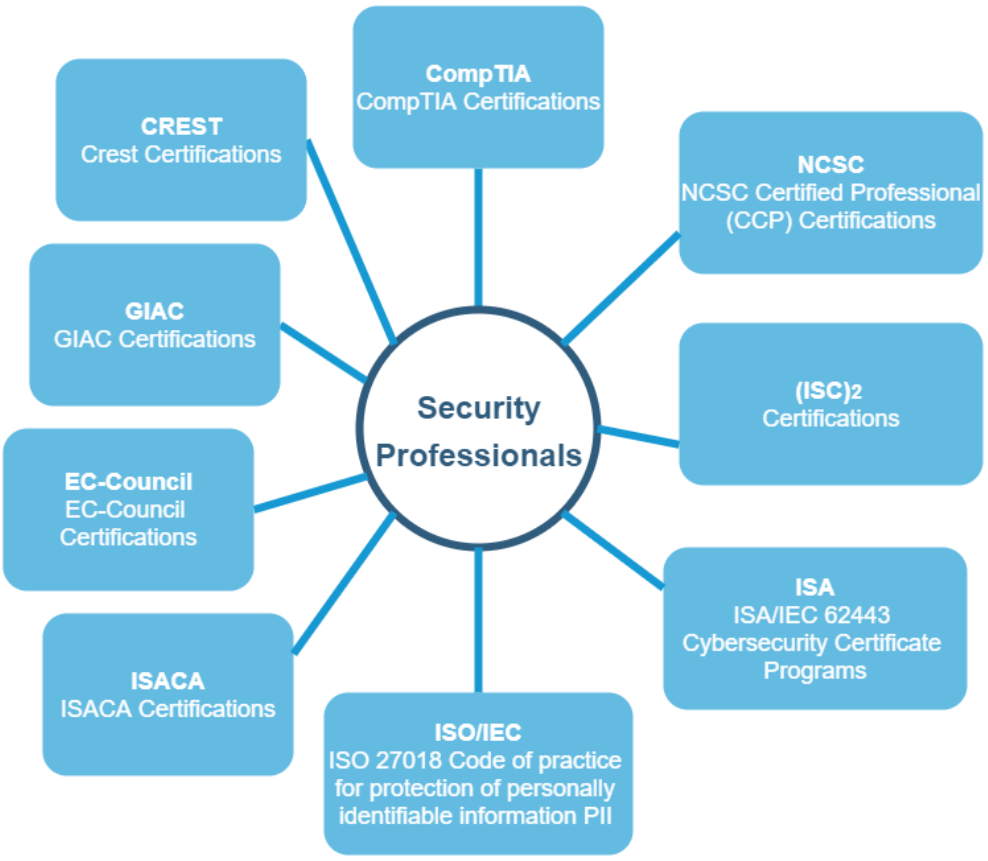

Figure 41: Standards and certifications for security professionals

Figure 42: Standards and frameworks for Services providers and organisations

Chapter 8 List of Abbreviations

Abbreviation	Translation
ADN	Agence Du Numérique
AI	Artificial intelligence
ANSI	Agence nationale de la sécurité des systèmes d'information
ASE	Security Target Evaluation
BSI	Federal Office for Information Security
BTOB	Business to Business
BtoG	Business to Government
GDPR	Government to Government
CAIQ	Consensus Assessments Initiative Questionnaire
CB	Certification/Validation Bodies
CC	Common Criteria
CCB	Centre for Cyber security Belgium
CCM	Cloud Controls Matrix
CCRA	The Common Criteria Recognition Arrangement
CE	Conformité européenne
CEM	Common Methodology for Information Technology Security Evaluation
CIS	Center of Internet Security
CINI	National Interuniversity Consortium for Informatics
CISR	Ministerial Committee for the Security of the Republic
cPP	collaborative Protection Profiles
CSA	Cloud Security Alliance
CSIRT	Computer emergency response team
CSPCERT WG	European Cloud Service Provider Certification Working Group
DDOS	Distributed Denial of Service attack
DG CONNECT	Directorate General- for Communications Networks, Content and Technology
DIH	Digital Innovation Hub
DIS	Security Intelligence Department
EAL	Evaluation Assurance Level
ECCG	European Cybersecurity Certification Group
ECCS	European Cybersecurity Certification Schemes

Abbreviation	Translation
ENISA	European Union Agency for Cybersecurity
EU	European Union
FINCSC	Finnish Cyber Security Certificate
GDPR	General Data Protection Regulation
GtoG	Government to Government
IACS	Industrial Automation and Control Systems
ICCF	IACS Cybersecurity Certification Framework
ICCS	IACS Cybersecurity Certification Schemes
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IECEE	IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
IIC	Industrial Internet Consortium
IIoT	Industrial IoT
IIRA	Industrial Internet of Things Reference Architecture
IISF	Industrial Internet of Things Security Framework
IOT	Internet of Things
ISA	International Standards on Auditing
ISMS	information security management system
ISO	International Organization for Standardization
IT	Information Technology
ITA	Italian Trade Agency
ITSEC	Information Technology Security Evaluation Criteria
ITSEFs	IT Security Evaluation Facility
JYVSECTEC	Jyväskylä Security Technology
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NLF	New Legislative Framework
NSC	Chair of the Cybersecurity Management Board
OT	Operation Technology
PP	Protection Profile
PPHS	Polish Platform for Homeland Security
RIHA	Administration system for the state information system
SAE	Society of Automotive Engineers

Abbreviation	Translation
SANS	SysAdmin, Audit, Network and Security
SARs	*Assurance* Requirements
SME	Small and medium-sized enterprises
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
STAR program	Security Trust Assurance and Risk
TC	Technological Clusters
TOE	Target of Evaluation
UK	United Kingdom
UNIZO	De Unie van Zelfstandige Ondernemers
US	United States
WP	Work Package

Chapter 9 Bibliography

1. Degryse, Christophe, Digitalisation of the Economy and its Impact on Labour Markets (February 10, 2016). ETUI Research Paper - Working Paper 2016.02.
2. Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6,2019,
3. Jesper Zerlang, GDPR: a milestone in convergence for cyber-security and compliance, Network Security, Volume 2017, Issue 6, 2017
4. Pupillo, Lorenzo, EU Cybersecurity and the Paradox of Progress (February 19, 2018). CEPS Policy Insight, No 2018/06, February 2018.
5. Hiscox Cyber readiness report 2019 https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF. Last access: November 2019
6. Hybrid and cybersecurity threats and the European Union's financial system https://bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf. Last access: November 2019
7. SBS position on cybersecurity solutions and certification for SME users and providers of critical services https://www.sbs-sme.eu/sites/default/files/publications/SBS%20PP%20on%20cybersecurity%20solutions%20and%20certification.pdf. Last access: November 2019
8. Questions and Answers: Directive on Security Network and Information systems, the first EU-wide legislation on cybersecurity https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651. Last access: November 2019
9. Review of Cyber Hygiene practices https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport. Last access: November 2019
10. GAME OVER? EUROPE'S CYBER PROBLEM https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem. Last access: November 2019
11. I. Øverland, E. Scholl, K. Westphal, K. Yafimava '*The Case for Energy Risk Mitigation and Connectivity"* (2016) p.2 https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C26_wep_et_al.pdf Last access: May 2020
12. The EU Cybersecurity Act https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act. Last access: November 2019
13. The Directive on security of network and information systems (NIS Directive) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. Last access: December 2019
14. EU data protection rules https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en. Last Access: November 2019
15. EC Cloud Strategy https://ec.europa.eu/info/sites/info/files/ec_cloud_strategy.pdf Last access: December 2019
16. B. Larrumbide Martinez and L. Orue-Echevarria "*Recommendations for the implementation of the CSP Certification scheme*" (2019) p.9
17. https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view Last access: May 2020
18. Cybersecurity certification: lifting the EU into the cloud https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud Last access: December 2019
19. 2017 roundup of internet of things forecasts https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internetof-things-forecasts/#6d8a4f551480. Last access: December 2019
20. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ Last access: December 2019
21. Explosive IoT Growth Slowed by 'Early Adopter Paradox' https://press.f-secure.com/2018/10/24/explosive-iot-growth-slowed-by-early-adopter-paradox/ Last access: November 2019

22. IoT Security Flaw Leaves 496 Million Devices Vulnerable At Businesses: Report https://www.crn.com/news/internet-ofthings/300106806/iot-security-flaw-leaves-496-million-devices-vulnerable-at-businesses-report.html Last access: December 2019
23. Frost and Sullivan "Cyber Security in the Era of Industrial IoT" (2017) p.3 Last access: November 2019
24. The Merging of Cybersecurity and Operational Technology https://cybersecurity.isaca.org/csx-resources/the-merging-of-cybersecurity-and-operational-technology Last access: December 2019
25. IACS Cybersecurity Certification Framework https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs Last access: November 2019
26. European Cybersecurity Certification Group National Initiatives 1st Informal meeting 12 July 2019
27. ENISA AND CYBERSECURITY CERTIFICATION FRAMEWORK https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61590 Last access: November 2019
28. The EU Cybersecurity Act https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act Last access: November 2019
29. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN Last Access: November 2019
30. Jose Ruiz, Analysis and comparison of lightweight evaluation Methodologies https://www.standict.eu/sites/default/files/Input%20jtsec%20-%20Analysis%20and%20comparison%20of%20lightweight%20evaluation%20methodologies.pdf Last access May 2020
31. Building a DevSecOps Culture - from a Technical Perspective https://tech.gsa.gov/guides/building_devsecops_culture/ Last access: May 2020
32. N. Tomas, J. Li and H. Huang, "An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, 2019, pp. 1-8,
33. Christophe Ponsard, Gautier Dallons, Philippe Massonet: Goal-Oriented Co-Engineering of Security and Safety Requirements in Cyber-Physical Systems. SAFECOMP Workshops 2016: 334-345
34. AMASS: Assurance and Certification of CPS. https://www.amass-ecsel.eu/ Last access : May 2020
35. AQUAS: Aggregated Quality Assurance for Systems. https://aquas-project.eu/ Last access : May 2020
36. Cobit 5 principles https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/lessons-learned-while-combining-cobit-5-and-itil Last access: May 2020
37. Cobit 5 Enablers https://cobit.nl/ Last access: May 2020
38. ECSO (2017), Position paper: Initial position on the EU cybersecurity package. http://www.ecs-org.eu/documents/uploads/ecsoposition-paper-on-cybersecurity-package.pdf Last access December 2019
39. European Commission (2015), Cybersecurity industry. https://ec.europa.eu/digital-single-market/en/cybersecurity-industry Last access May 2020
40. International Organization for Standardization https://www.iso.org/deliverables-all.html Last access May 2020
41. C. Warren Axelrod. The creation and certification of software cybersecurity standards. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, 1-6.
42. Christophe Paul W. Witherell, Sudarsan Rachuri, Anantha Narayanan Narayanan, Jae H. Lee, "FACTS: A Framework for Analysis, Comparison, and Test of Standards. NIST Interagency/Internal Report (NISTIR) - 7935, 05/2013. https://doi.org/10.6028/NIST.IR.7935
43. Christophe Ponsard, Gautier Dallons, Philippe Massonet: Goal-Oriented Co-Engineering of Security and Safety Requirements in Cyber-Physical Systems. SAFECOMP Workshops 2016: 334-345 Last access: May 2020
44. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT https://www.iso.org/isoiec-27001-information-security.html Last access November 2019
45. STATE OF THE ART SYLLABUS Overview of existing Cybersecurity standards and certification schemes v2 https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf Last access: November 2019
46. ISO /IEC 27001 - Worldwide total https://www.iso27001security.com/html/27001.html Last access: November 2019
47. Framework for Improving Critical Infrastructure Cybersecurity https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf Last access: November 2019

48. NIST: Cybersecurity Framework. https://www.nist.gov/cyberframework (2014) Last access: November 2019
49. Center for Internet Security https://www.cisecurity.org/ Last access: November 2019
50. CIS: CIS Controls V7.1 https://www.cisecurity.org/controls/ (2019) Last access November 2019
51. Industrial Internet of Things Security Framework https://www.iiconsortium.org/IISF.htm Last access: November 2019
52. The STAR program https://cloudsecurityalliance.org/star/ Last access: November 2019
53. STAR Open Certification Framework https://cloudsecurityalliance.org/star/levels/ Last access: November 2019
54. ISKE : IT-GRUNDSCHUTZ in ESTIONIA https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag_2010/ISKE.pdf?__blob=publicationFile Last access: November 2019
55. Three-level IT Baseline Security System ISKE https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html Last access: November 2019
56. Estonian Security System Overview https://www.ria.ee/sites/default/files/content-editors/ISKE/iske_eng.pdf Last access: November 2019
57. BSI-Standards https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html Last acces: November 2019
58. A. Barber « Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard" (2018) P.7-8
59. UNECE ISO-SAE 21434 Road vehicles – Cybersecurity Engineering General Overview https://wiki.unece.org/download/attachments/44269802/TFCS-05-12%20%28OICA-CLEPA%29%20Overview%20on%20ISO-SAE%20activities%20regarding%20Cyber%20Security.pdf?api=v2 Last access: November 2019
60. Status of the various work products in the ISA/IEC 62443 https://www.isa.org/isa99/ Last access: November 2019
61. European Cyber Security Certification Composability approach WG1 – Standardisation, certification, labelling and supply chain management September 2019 Last access: November 2019
62. Annual Report on European SMEs 2014 / 2015 https://publications.europa.eu/en/publication-detail/-/publication/7c9fbfe0-e044-11e5-8fea-01aa75ed71a1 Last access: November 2019
63. J. Leclair "*House Hearing, 114th Congress - Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks*" (2015) p.60-62
64. Kaspersky Lab: Measuring Financial Impact of IT Security on Businesses (2016) Last access: November 2019
65. UK Government: CyberEssentials https://www.cyberaware.gov.uk/cyberessentials Last access: November 2019
66. Alex Whalen: Digital Europe's views on cybersecurity certification and labelling schemes. http://bit.ly/2m3dyLV(2017) Last access December 2019
67. SME Definition - user guide 2015 https://ec.europa.eu/docsroom/documents/15582/attachments/1/translations Last access: December 2019
68. Cyber essentials https://www.cyberessentials.ncsc.gov.uk/blog-post/the-bare-essentials Last access: December 2019, Bure valley Group, 2019
69. CCB (internal report)
70. Digital Wallonia (2018). Keep IT Secure. https://www.digitalwallonia.be/keepitsecure. Last access: November 2019
71. CCB (2016). Cyber Security Guide for SME. http://www.ccb.belgium.be/en/guide-sme. Last access: November 2019
72. Cyber Security Strategy 2019 https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf Last access : November 2019
73. Morgagni Andrea, Massonet Philippe, Dupont Sbastien, Grandclaudon Jeremy: Towards Incremental Safety and Security Requirements Co-Certification. EuroS&P Workshops 2020: 79-84
74. Sébastien Dupont, Guillaume Ginis, Mirko Malacario, Claudio Porretti, Nicolò Maunero, Christophe Ponsard, Philippe Massonet:

Incremental Common Criteria Certification Processes using DevSecOps Practices. EuroS&P Workshops 2021: 12-2
75. Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, see https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf, last accessed January 2022
76. DPO tool for evaluating a business processes, see dpotool.cs.ut.ee. Last access: January 2022
77. prEN 17640 Fixed-time cybersecurity evaluation methodology for ICT products, see https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/04-05-banon, last accessed: January 2022