WHITE PAPER

Information and Cyber Security Professional Certification

Task Force WG5 I European Human Resources Network for Cyber (EHR4CYBER)

SEPTEMBER 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.
ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg5_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

For the last years, there have been many publications on the expected shortage of security professionals worldwide and in Europe. In addition to the international certification organisation (ISC)² [29], this has been reported by RAND [12] and Plato [11]. The demand for cyber security professionals will increase and that shortage of cyber security professionals creates risks for national and homeland security, people, organisations, and society. According to a report by Frost & Sullivan [30], it is estimated that by 2022 the global cyber security workforce will have a shortage of 1.8 million professionals. This means that it will become more difficult to attract staff to fill open positions. Secondly, it is hard for both employees and employers to assess who has the right qualifications for the open positions. Lastly, recent impacts and developments have broadened the cyber security domains. The European Union Agency for Network and Information Security (ENISA) conducted a study to clarify the EU's position on cyber security definition by releasing a report entitled "Definition of Cyber security – Gaps and overlaps in standardisation" (released on 01.07.2016) [31].

The ENISA document clearly states how cyber security is intertwined with different domains within the term as illustrated in Figure 1 below. The scale of cyber security and its meaning is beyond information security and widespread with five domains listed below including cyber war and cyber defence within military security.

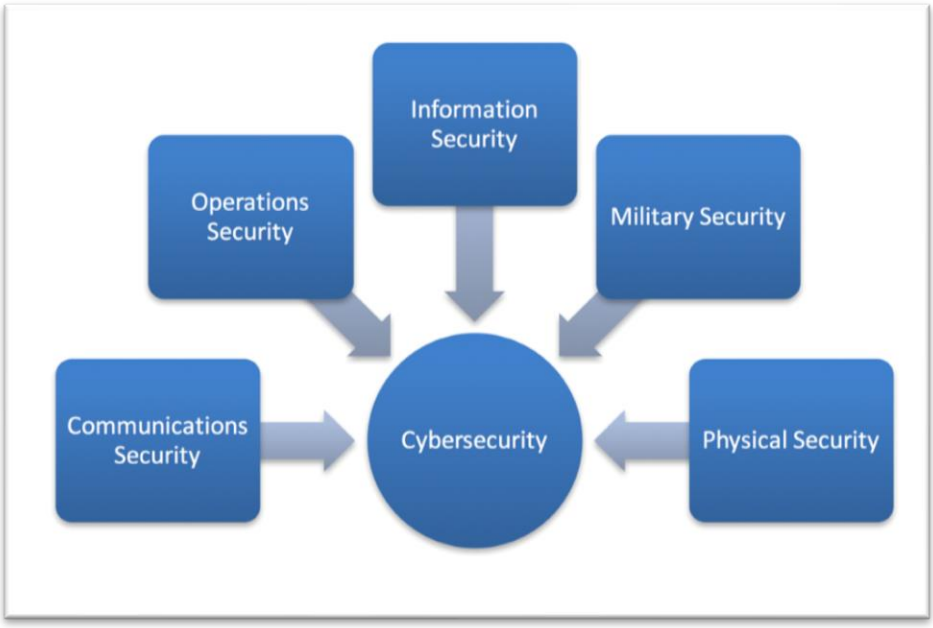

Figure 1 – Cyber Security and its domains [21]

The aforementioned factors will demand reasonable cyber security solutions and certification. In addition to certifying a level of technical and functional expertise required by the security industry. Certification is increasingly necessary nowadays in the perspective of the concept of ***trust***, both internally for the employer itself and for its external clients in terms of quality of service and operational excellence.

Information and cyber security is an immature field of employment; there is, as of yet, only a limited supply of formal training with colleges and universities. Many courses and trainings from various suppliers, including universities and colleges already exist. In some cases, like for cryptography, it has existed even for decades. These trainings do not necessarily lead to a standardised curriculum that would be required for information and cyber security professionals, and over the years the number of functions within information security have also increased, with different function requirements. This is due to the technological developments that have emerged in recent years which have required a different way of adapting the business, including the digital transformation of companies.

This is shown in two conclusions of the PLATO research focused on the Dutch situation:

1. The educational supply regarding cyber security is varied and extensive. Educational programmes are often offered in various locations and there is much variation in types of education or training. At the same time, the supply is not transparent.

2. The match between the demand for cyber security professionals and the supply of these professionals is obstructed by qualitative discrepancies and a lack of transparency.

This makes it hard to assess whether candidates fit the requirements of positions, as shown in Figure 2.

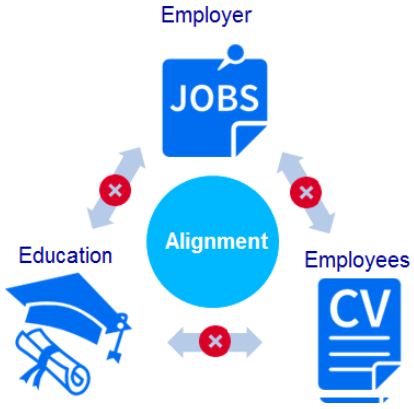

Figure 2 - Missing alignment between education, jobs and resumes

Since the early 1990's, this has generally been solved via professional certifications offered by international professional bodies. One of the first certifications in this area was the (ISC)² Certified Information Systems Security Professional (CISSP). Currently, there is even a magazine dedicated to IT certification programmes (Certification Magazine: http://certmag.com/). Over the years, many certifications have seen the light, which makes it hard to know which certifications are relevant (see Figure 3). In addition to employers and professionals, it is also hard for education institutes to determine where to invest in new training programmes.

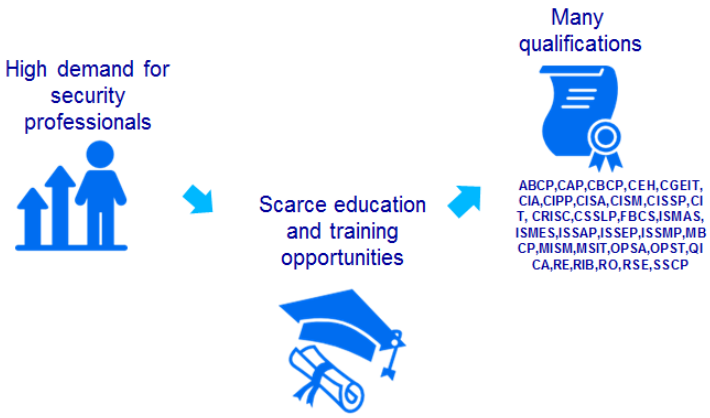

Figure 3 - Many qualifications to choose from

This white paper mainly addresses the established and recognised ***Information and Cyber Security Professional Certification*** schemes that helps to develop human resources. The paper is not meant to be exhaustive but serves to give an overview of several existing certification schemes, both in Europe and internationally, to establish gaps and needed developments for the future. A follow up paper could be envisaged next year which would go deeper into the needs with possible concrete proposals (i.e. the establishment of an EU-wide certification and accreditation scheme as well as a European framework for professional development in cyber security). The white paper does not deal with certification of products and services.

The following sections provide an overview of activities dealing with professional security certification schemes and frameworks, in Europe as well as internationally.

2 Approaches to Certification

The basis for every certification is twofold:

- Proving basic knowledge of a generally accepted body of knowledge.
- Showing the ability to use this knowledge in practice, e.g. demonstrating the competencies and skills involved.

The implementation of the first step is relatively easy and is generally handled via a theoretical examination. This can be a central class-based examination but also via computer-based examination.

Demonstrating the required skills and competencies is the difficult part of certification. This is generally done by showing relevant work experience. For various, relevant certifications like CISA, CISM and CISSP, this is generally a period of 5 years in which the professional needs to work in the field of information and cyber security. The request needs to be endorsed by existing certificate holders.

The advantage of this approach is that it's an easy to implement process, which also scales easily with the number of applicants. There are however a number of consequences of this approach:

- Generally, the certifications are meant for global recognition but are US-centric as they originate from the US. Especially aspects like laws and regulations but also cultural differences between nations don't get a fair treatment.
- The verification of knowledge in the exams is standardised. Training of knowledge of these certifications literally is training for the exams.
- Updates to the body of knowledge takes several years. This means outdated knowledge gets verified.
- It is hard to verify the work experience and whether the required skills and competencies are really at the right level.
- The certifications are binary: you either have the certification or you do not. There are no levels mastering the information security work field.
- Compared to other recognised critical professions in society, the methods are immature.
- Finally, due to among other things the high experience requirements, the certifications are meant for professionals and are not fit to educate young talent at vocational and university level. Because of this, the necessary growth of the cyber security workforce is not stimulated.

As an example, the broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are supposed to be competent in the following 8 domains [26]:

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management

6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Another approach is using validation by reviewers. This is a more complex and time-consuming process, but it enables a validated and consistent level of quality. It not only shows the experience but also proves that the necessary skills and competencies have been acquired. This is done by a portfolio review together with an interview with a group of recognised experts in the field. With this approach, new developments can also be integrated more easily.

A third approach is that the theory part is complemented with a practical assignment. To complete this, professionals need to show that they have acquired the skills and competencies required for the certification. An example of this approach is the Offensive Security Certified Professional (OSCP).

Certification holders are generally required to maintain their certifications by annually demonstrating participation in a set number of continuous professional education activities (CPE), typically around 40 hours per year. This is intended to keep knowledge current in a fast-paced field.

This established market approach to security certifications has a number of shortcomings and limitations.

- Whereas certifications have become a de-facto requirement for many security jobs, the high experience requirement of typically 5 years that is demanded by the key incumbents for market leading certifications provides a barrier to entry for newcomers. One might argue that this works as intended, however it does reinforce existing bottlenecks in view of existing demand.
- As a related problem, certifications for the early phases of a security career are in lower demand than those for the later phases. As career changers contribute significantly to the security workforce, addressing the “entrants” end of the market would enable an early professionalisation and qualification as well as vetting.
- Certification maintenance (normally limited to the submission and auditing of CPE activities), making up a significant portion of certification organisations’ revenue stream, impose a de-facto “certification tax” on security professionals.
- Certifications coexist with academic education offerings in the marketplace without offering the same depth of learning. (A course preparing for certification is equivalent to approximately 1 ECTS credit.) Thus, they can offer a temporary relief for qualification bottlenecks, but they are not a panacea.

2.1 Overview of certifications and providers

There are many certifications related to information and cyber security, though the majority are more related to IT security. In Table 1, an overview of independent certification providers is given (table based upon the information in [7]).

Certifications provider	County	Certificates
(ISC)²	USA	CISSP, SSCP, CCSP, CAP, CSSLP, HCISPP
ISACA	USA	CISA, CISM, CRISC, CGEIT
GIAC	USA	GSLC, GSNA, GISP, GSTRT
CompTIA	USA	CASP, CSA+, Security+
EC-Council	USA	Certified Ethical Hacker (CEH)
EITCI (European Information Technologies Certification Institute)	Belgium (EU)	EITCA/IS
ISECOM (Institute for Security and Open Methodologies)	Spain (EU), USA	OPST, OPSA, OPSE, OWSE, CTA, SAI
Offensive Security		OSCP, OSWP, OSCE, OSEE, OSWE
ANSI, AFNOR, etc.	US, FR, etc.	ISO/IEC 27001 Lead Auditor, Implementor, ISO/IEC 27005 Risk Manager
KÜRT Akadémia / Cyber Institute	HU (EU)	KCEH / MEH (equivalent to CEH in Hungarian)

Table 1 - Overview of Independent security certifications

In general, statistics are not publicly available for all security certifications, but Table 2 provides an overview of number of certificate holders, worldwide and within Europe, for three security-related certifications (https://www.isc2.org/en/About/Member-Counts).

Certificate	Organisation	World wide	Europe	Certificate exists since
CISSP	$(ISC)^2$, US	122 289	17 488	1994
CISA	ISACA, US	61 640	18 880 (incl. Africa)	1978
CISM	ISACA, US	23 220	6 920 (incl. Africa)	2002

Table 2 - Overview of number of people certified for CISSP, CISA and CISM

3 European developments

Within Europe, there is currently no certification framework spanning the whole of the European Union. In some countries, there are activities underway to define job profiles and, in many cases, the European e-Competence Framework is used for this.

3.1 European e-Competence Framework 3.0

The European e-Competence Framework (e-CF, see [2]) provides a reference for 40 competences as applied to the Information and Communication Technology (ICT) field, using a common language for competences, skills, knowledge and proficiency levels that can be understood across Europe.
In 2016, the e-CF became a European standard and was officially published as the European Norm EN 16234-1.
As the first sector-specific implementation of the European Qualifications Framework (EQF), the e-CF fits for applications by ICT service, user and supply organisations, multinationals and SME's, for ICT managers, HR departments and individuals, educational institutions including higher education and private certification providers, social partners, market analysts, policy makers and other organisations in the public and private sectors.
The European ICT Professional Role Profiles do not represent a rigid standard but provide inspiration for the flexible creation of roles as input to job descriptions. Using pre-formatted profiles eliminates the need to start with a 'blank sheet of paper' as they support and shape the construction of tailored ICT Professional Role characteristics.
The e-CF is structured over four dimensions. These dimensions reflect different levels of business and human resource planning requirements in addition to job/work proficiency guidelines. They are specified as follows:

- Dimension 1: The e-CF has 5 e-Competence areas, derived from the ICT business processes PLAN – BUILD – RUN – ENABLE – MANAGE.
- Dimension 2: A set of reference e-Competences for each area, with a generic description for each competence. 40 competences identified in total provide the European generic reference definitions of the framework.
- Dimension 3: Proficiency levels of each e-Competence provide European reference level specifications on e-Competence levels e-1 to e-5, which are related to EQF levels 3-8.
- Dimension 4: Samples of knowledge and skills relate to e-Competences in dimension 2. They are provided to add value and context and are not intended to be exhaustive.

In addition, in the basic version, the e-Competence Framework lists two security related functions:

- IT Security Specialist
- IT Security Manager

3.2 Belgium

The Executive Master's in Information Security Management and the Executive Programme in Cyber Security from Solvay Brussels School of Economics and Management has been certifying professionals since 2001 in various domains of Digital Management and Governance, Risk management and Information and Cyber Security [32].
A cyber security specialisation was announced in 2014 and has been delivered since the academic year 2015, including a full track in Information Security and Cyber Security. While aligning this executive education on bodies of knowledge of various professional certifications, the business school promotes that participants and alumni sit various examinations and add those professional certifications to their résumé. As a result, a majority of their 450 alumni possess one or more certifications such as CISSP, CISM, CISA, CGEIT, CRISC, TOGAF, as well as ISO27001, 27005 and 27034 certifications.
The education is structured around five tracks with three modules each. It is delivered to professionals who typically attend two or more evenings per week for one (Executive Programme) or two years (Executive Master). The body of knowledge is maintained by ITMA asbl, a non-for-profit organisation and a member of ECSO. It is structured based on five Digital Management components that are thought to be essential for technical as well as management profiles in cyber security.

Digital Governance Track	G1 – The CIO Foundation
	G2 – IT Governance Workshop
	G3 – IT Risk and Legal concerns
Digital management Track	M1 – IT Service and Run Management
	M2 – Applications Build and Management
	M3 – IT Sourcing Management
Information Security and Cybersecurity Track	S1 – Information Security Management
	S2 – Information Security Practices
	S3 – Cybersecurity Workshop
Business Agility Track	B1 – Enterprise Strategy and Architecture
	B2 – Business Transformation
	B3 – Digital Agility and Innovation
Activating management Skills Track	A1 – IT Finance and Portfolio Management
	A2 – Soft Skills for IT professionals
	A3 – Building Expert Opinion

Table 3 - Tracks and modules

The education programme has partnered with ISACA since 2007 and recently with PECB Europe, allowing participants to benefit from access to professional certification and bodies of knowledge. It also participated in the foundation of the Belgian Cyber Security Coalition. More than 50 participants are registered on a yearly basis and usually come from Information Security, Cyber Security, Risk, Compliance, Audit IT and Digital professions. Recently, Solvay Brussels School added a short programme in Data Protection.

Education is also delivered on client specific programmes which are delivered to organisations. Various major transformations to the body of knowledge and yearly updates to the specific modules, combined with a case-based and workshop model, allow participants to gain practical expertise beyond basic knowledge of concepts.

3.3 Finland

Finland has adopted training and certification under their nationwide Cyber Security Strategy Implementation Programme. There are three categories of the cyber security certification. The first one targets the working-life professionals and students, while the second focuses on information security auditing of authorities and professionals. Finally, Finland is also encouraging national level cyber security curriculum development from schools to higher education under the Finland Vision 2030 strategies. There is a clear identification of target groups for effective cyber security certification.

- FINCSC – Finnish Cyber Security Certificate
- KATAKRI (Information Security Audit Tool for Authorities)
- National Cyber Security Competence

(1) Professional certification: FINCSC – Finnish Cyber Security Certificate is a certification system for companies and communities to ensure their business continuity.

FINCSC is suitable for diverse organisations regardless of their company form, market size or line of business. With the use of the system organisations confirm their ability to maintain information security and data protection, as well as to provide effective and reliable services for their partners and customers. JYVSECTEC provides versatile and high-quality training in various fields of information and cyber security. The training adds to the personnel's abilities in knowledge and skills to adapt to the constant change of networks and cyber environments. The training develops the personnel's thoughts about observing their own work methods as well as clarifies their attitudes.

(2) Auditing Certification: KATAKRI (Finnish abbreviation of Information Security Audit Tool for Authorities) certification is targeted towards authorities dealing with security products and services. Laurea University of Applied Sciences offers a training programme on KATAKRI (Information Security Audit Tool for Authorities). KATAKRI is a Finnish national security auditing criterion based on several ISMS standards and best practices. The following key competencies are offered and validated with certification:

- KATAKRI aimed to be used when assessing the capability of the organisation to safeguard Classified Information and Issuing a Facility Security Clearance (FSC) for a company.
- An information security management system (ISMS) provides controls to protect organisations' most fundamental assets, data and information
- Security management including administrative and personnel security.
- Physical security including requirements on premises and equipment, deterring unauthorised access, and protection from unauthorised observation and eavesdropping.
- Information assurance including communications, data, system and operations security.

(3) Education programmes & certifications: Finland has implemented a national level cyber security competence development programme from schools to higher education. The curriculum is targeting to meet the standards and learning outcomes of national and international certification programmes. For example, Finnish schools are encouraged to leverage the benefits of the European Union's recommendation on minimum cyber security education for school children. In Finland, the higher education institutes including traditional Universities and University of Applied Science offers graduate, post graduate and professional education programmes (see [22]). While the higher education offers graduates and masters level programme and many times curriculum mapped with professional certification including CISSP, CISM, Security+ and many more. On the one hand, the traditional universities offers more technical-oriented education programmes including masters of engineering (MEng) to masters of sciences (MSc) degrees. For example, University of Jyväskylä, Aalto University, JAMK University of Applied Sciences, University of Turku and South-Eastern Finland University of Applied Sciences. On the other hand, Laurea University of Applied Sciences is offering a comprehensive 60 ECTS module based education in cross-sectoral management and technological solutions for information and cyber security. The curriculum is mapped with the suggestions from industrial partners while designing the cyber security curriculum at Laurea University of Applied Science. The curriculum is directly mapped with the professional certifications including:

- ISACA - Certified Information Security Manager (CISM)
- CompTIA Security+
- (ISC)2 - Certified Information Systems Security Professional (CISSP®),
- Certified Ethical Hacker (CEH)
- CompTIA Cyber security Analyst (CSA+)

Finland is visioning and piloting national level holistic cyber security education mapped with professional certification programmes that other European nations can also benefit greatly in future. The work can benefit EU nations to fill-gap of cyber security professionals.

3.4 France

Within France, ANSSI (Agence nationale de la sécurité des systèmes d'information, the French National Cyber Security Agency) has developed a number of professional labels. Some of them oblige the staff to be qualified (by examination). Currently, ANSSI has labels for:

- PASSI: Audit Providers in SSI
- PRIS: Incident Response

An example for PASSI:
Companies that perform technical or organisational security audits may request to be labelled as PASSI. This implies the demonstration that the auditors have the expected skills (by examination). This label also allows customers to identify companies with qualified auditors and a methodology adapted to the services they propose. The label is granted to the company, but the auditors are individually followed. If auditors disappear, the company loses its label. In addition, these companies must use auditors who have passed the examinations to propose a "PASSI" type of service. There are examinations for the following security domains:

- Architecture
- Configuration
- Source code
- Penetration test

- Organisational and physical security

The principles are the same for PRIS. See for more information [8].
In addition to this, ANSSI provides labels to training organisations. These labels are aimed at training organisations that deliver grades or diplomas like Bachelor, Master, Engineer or Mastères Spécialisé ® for programmes that propose specialised training in security.
Institutions must issue a specific certificate (in addition to the diploma) enabling employers to ensure that graduates have followed the certified training path. Soon, this certificate could be issued on behalf of ANSSI (or by ANSSI). As of now, 41 training courses are labelled. The aim is to reach 50 by the end of 2018.
For more information on the labelling process, see (in English) references [9] and [10].
Finally, in January 2018, ANSSI launched a programme of referencing and labelling short continuous training. The criteria are much lighter than for initial training. It relies:

- Either on the system of professional certifications (for all sectors) set up by the French State and in which ANSSI is involved (for the security part)
- Or on the respect of a specification recognised by ANSSI

Today, only two specifications are available: security for small and medium-size companies and SCADA. A third concerning critical infrastructures is expected to be released soon.

3.5 Germany

The German Federal Office for Information Security (also known as BSI, Bundesamt für Sicherheit in der Informationstechnik) as the national cyber security authority shapes information security in digitisation through prevention, detection and reaction for government, business and society.

The BSI Baseline Protection Manual provides a high-level scheme of security roles, including in particular the role of IT Security Manager (“IT-Sicherheitsbeauftragter”) [27].

A number of professional certification schemes exist specific to the German market. These include:

- German Federal Office for Information Security (BSI) offering BSI Auditor certifications (https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html, in German Language). Focus is mainly on auditors for specific applications and functions related to Common Criteria certification. One exception here is security tester.
- TeleTrusT TISP https://www.teletrust.de/tisp/ is a certification for Information Security professionals, comparable to CISSP, but with more focus on German and European legislation.

3.6 Hungary

Within Hungary, a national certification framework is not currently available. However, there is a specialised certified ethical hacking course offered by Cyber Institute that is a level 5 training according to the European Qualification Framework.

The ethical hacking training curriculum targets national and international participants with a strong emphasis on introduction to cyber security for IT professionals, technical skillset (defensive and proactive), social engineering skillset, professional communication, and strategic thinking. The curriculum offers a comprehensive overview and skillset propagating the cyber security lifecycle (identification, protection, detection, reaction, recovery), enabling participants with practical and up-to-date knowledge that is required to understand and deliver state of the art skills in the field of cyber security.

Also, Hungary addresses the necessity of cyber resilience and awareness on a general (national) level within its “Digital Wellbeing” program, through which the Hungarian government recommends active and particular measures to raise the general cyber security awareness level of end users, basically the non-professional population, along with specific IT and cyber security education offerings.

3.7 Italy

In Italy, the e-CF framework has been used to describe three national profiles, based upon the generic e-CF profile ‘ICT security manager’:

- Information security management system manager
- Digital conservation system security manager
- ICT business continuity manager

This has been done as part of Italian standard - UNI 11621-4 “Unregulated professional activities - ICT professional profiles – Part 4: Information security professional profiles [6]. These profiles are relatively scarcely used and diffused in Italy, where they are valid both for activities organised in a professional body and for non-organisational activities. The standard is new, and it takes a number of years for it to get recognised and used.

It has however highlighted a certain issue, since not-for-business organisations that have existed for a long time, such as ISECOM (Institute for Security and Open Methodologies, http://www.isecom.org), didn’t manage to make the bureaucratic effort needed to get involved in this new standard. The example of ISECOM highlights the limitations well, and possible issues, brought in by the new standard: established back in 2000 and based in Europe (Barcelona, Spain), ISECOM provides the very first penetration testing professional certification courses, recognised all over the world: OPST (OSSTMM Professional Security Tester), OPSA (Professional Security Analyst) and OPSE (Professional Security Expert), all based on the OSSTMM (Open Source Security Testing Methodology Manual), the de-facto standard for running professional penetration tests.

Another example showing the lack of interaction with the e-CF Framework is related to the BC (Business Continuity) and DR (Disaster Recovery) training fields: the BCI (Business Continuity Institute) Italian chapter has a long-standing reputation for the best professional trainings on the topic but, once again, this institute did not work on e-CF Framework compliance or collaboration.

The lack of organisations like ISECOM involved in the standard is definitely emblematic, given that ISECOM certifies more than 800 professional penetration testers in Italy alone, and thousands around Europe and the whole world (the full list of the certified professionals that have authorised their data to be public is available here: http://www.isecom.org/certification/). Moreover, the OSSTMM is the key requirement in public and private tenders for Vulnerability Assessments and Penetration Tests, along with OWASP (Open Web Applications Security Project), which is not recognised either by the standard in Italy.

Therefore, a few certification organisations offer the certification path for those profiles (AICQ-SICEV for example - http://aicqsicev.it/registro-corsi-riconosciuti/) and a few training organisations offer preparation courses recognised by the above-mentioned certification organisations. These courses (ITHUM course for example - http://www.ithum.it/ictsecuritymanager#Corso) are usually short and assume that the candidate has the acquired skill and knowledge from previous courses or experiences, like a Master's at university or other courses. The certification body recognises *some* international certifications, such as:

- CISA Certified Information Systems Auditor (ISACA)
- CISM Certified Information Security Manager (ISACA)
- C|CISO Certified Chief Information Security Officer (EC-Council)
- CRISC – Certified Risk and Information System Control (ISACA)

It is important to underline that in Italy the certification recognises a job profile that should have a set of e-competences, and not each single e-competence of the E-CF framework. On the other hand, it would have been good to distinguish between those certifications provided by Associations (like ISACA) and others provided by private organisations, which do not work, support, or build any international standard or best practices, but whose sole goal is the business side of security trainings.

Recently, AgID (the Italian government agency for the ICT) has started to refer to these profiles in some of its calls (http://www.agid.gov.it/avvisi/avviso-5-2017, http://www.agid.gov.it/avvisi/avviso-6-2017), while the main business associations for the company (Assintel and Assinform) have started to use them in research on the skills market (http://www.assinform.it/pubblicazioni/osservatorio-delle-competenze-digitali.kl).

In Italy, the profiles are helping in the definition of a common language for the labour market of ICT technologies, where a professional figure is often identified with different names, resulting in a disorientation of the demand from operators who are not able to evaluate clearly.
At European level, CEN issued the EN 16234-1 standard in 2016, which incorporates the e-CF, based on the Italian standard UNI 11506: 2013 which then started the path for the standardisation of the profiles by the UNI 11621 standards. So, the route taken in Italy is also used in Europe.

3.8 Switzerland

While the Swiss education market is generally dominated by academic offerings and vocational training and education (VET), most Swiss universities and universities of applied sciences today offer IT and Information Security as part of their IT curricula or as separate post-graduate courses.

As part of the general Swiss vocational education and training system, a federally recognised certificate for *ICT Security Experts* exists, with the first graduates to be released by 2018 [33]. This is planned to be supplemented soon by a more technically oriented *Cyber Security Specialist* certificate [34] (Note: equal to other federally recognised certificates, these certificates require a ca. 2-year education path; they are not the same as “professional certifications”).

No national certification scheme exists, nor is there official recognition for security certifications. Nonetheless, certifications have gained a significant footprint in recent years. Extrapolating from published membership numbers from (ISC)² (https://www.isc2.org/en/About/Member-Counts), Switzerland has more than four times the number of security certifications per capita than neighbouring Germany.

Like other European countries, Switzerland has recently adopted e-CF 3.0 into a national standard (SN EN 16234), which can be expected to have a major impact on a more differentiated recognition and management of security roles.

Extrapolating from published membership numbers of various professional organisations around Switzerland while considering possible overlaps, the number of security professionals can be estimated at around 3000. According to a study by the umbrella organisation for the Swiss IT market, the role of *ICT Security Officer* makes up about only 1% of IT jobs [28] (numbers for ICT specialist roles weren’t published but security skills were amalgamated into other specialist roles).

3.9 The Netherlands

The Dutch Association of Information Security Professionals (PvIB, Platform voor Informatiebeveiliging), together with the organisations of the public-private partnership QIS (Qualification of Information Security professionals), has been working on the Qualification of Information Security Professionals.
The first step in this process was the definition of four Information Security Profiles [5]:

- Chief Information Security Officer
- Information Security Officer
- ICT Security Manager
- ICT Security Specialist

It emerged that employers and trainers distinguish between three different levels of ICT Security Specialist. As a consequence, two further levels were added to the ICT Security Specialist profile. The European e-Competence Framework (e-CF) has been used as a basis for the definition of the Information Security Profiles that will be used in a certification scheme. The description of the PvIB Professional Profiles is based on the European ICT Professional Role Profiles *ICT Security Manager* and *ICT Security Specialist*.
The information security profiles are already used for the definition of internal job descriptions by a number of companies.
For many education profiles, the profiles have been used to define the curriculum for studies in the area of cyber security for young talent:

- Secondary vocational level: network security profile based upon the ICT Security Specialist
- Master’s level: CISO profile and the master’s level for ICT Security Specialist

In addition to this, some commercial training institutes are using the profiles for their own certification level like S-ECO.
The certification scheme for information security professionals is still under development.

3.10 United Kingdom

Within the United Kingdom, the UK National Cyber Security Center (NCSC), as part of GCHQ [1]. provides a certification scheme for cyber security professionals. The Certified Cyber Professional Certification for Cyber Security/IA Professionals is a UK-focused initiative that aims to provide employers with candidates who meet competency and skills requirements for specified roles or responsibilities.

There are six roles:

- Accreditor
- Cyber security/IA auditor
- Cyber security/IA architect
- Security and information risk advisor
- IT security officer family
- Communications security family

These are for the CCP scheme and are not widely used beyond the Government. The most popular roles are audit, architect and risk advisor. The accreditor and communications security roles are very specific to government.

NCSC are currently using the IISP Skills Framework v1. This has been superseded by version 2.2. The skills definitions for these roles dovetail with the disciplines from the IISP Skills Framework (see below). In addition to the professional certifications, the NCSC has certified a number of cyber security degree programmes.

The IISP Skills Framework [3] is a framework available to IISP Members only, it can be summarised as providing nine disciplines:

- A: Information Security Management
- B: Information Risk Management
- C: Implementing Secure Systems
- D: Information Assurance Methodologies, Audit and Testing
- E: Operational Security Management
- F: Incident Management
- G: Business Continuity Management
- H: Information Systems Research

Each of these disciplines contain skills groups. For example:

- Discipline: Information Security Management
    - Skills group: A1 – Governance
        - Example skills: Establishing frameworks to develop and maintain appropriate information security expertise within an organisation

Individuals applying each skill group – e.g. A1 – can achieve a competency level, ranging from 1: Basic knowledge of principles; Level 2: Knowledge and Understanding of basic principles; Level 3: Apply; Level 4: Enable; Level 5: Advise; to Level 6: Initiate, Enable, Ensure – Ex-pert/Lead Practitioner

The UK has recently run a consultation on how to develop the cyber security profession further. As part of that, it considered how to bring more coherence to the landscape of qualification/certifications to make it easier to discern the capabilities of a cyber-security professional and to make it easier for cyber security professionals to navigate their way into and through a career.

4 International developments

4.1 ISO

As part of the 27K stories27000 series, ISO is working on the competence requirements for ISMS professionals. This is done in standard ISO/IEC 27021 - Certification of Information Security Management Professionals [4].
This standard concerns the knowledge, skills and competencies required in respect of the management in information security. This relates to other ISO standards ISO/IEC 27001, 27002, 27005 and 27007 i.e. the management of information security. It is not a personal certification or qualification scheme as such, but in effect serves as a reference for the bodies that run such schemes.

4.2 NIST and the NICE Framework

In addition to its widespread cyber security framework (Identify, Protect, Detect, Respond, Recover), NIST has established a National Initiative for Cybersecurity Education (NICE) [22] which aims to energise and promote a robust network and an ecosystem of cyber security education, training, and workforce development. NICE has also developed a Cybersecurity Workforce Framework [23] which is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role.

The NICE Framework is aimed at a wide-ranging audience:

- Employers, to help assess their cyber security workforce, identify critical gaps in cyber security staffing, and improve position descriptions;
- Current and future cyber security workers, to help explore tasks and work roles and assist with understanding the knowledge, skills, and abilities (KSAs) that are being valued by employers for in-demand cyber security jobs and positions. The NICE Framework also enables staffing specialists and guidance counsellors to use the NICE Framework as a resource to support these employees or job seekers;
- Training and certification providers seeking to help current and future members of the cyber security workforce gain and demonstrate the KSAs;
- Education providers who use the NICE Framework as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and tasks described; and
- Technology providers who can identify cyber security work roles and specific tasks and KSAs associated with the services and hardware/software products they supply.

There are many lessons to be learnt from this NICE Framework if the ambition to move towards a European-wide Education Framework for Cyber, that can map education, knowledge, and skills to competencies and job profiles, is to become a reality.

4.3 ISACA

ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems, including certification, training and education. ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprise. ISACA's certification programmes are globally accepted, and ISACA members have direct access to research, certifications and products that align systems and strategy, as well as support to professional development (through guidance, events, etc.) [24].

4.4 $(ISC)^2$

$(ISC)^2$ or International Information System Security Certification Consortium, founded in 1989, is a non-profit organisation which specialises in training and certifications for cyber security professionals. The most widely known certification offered by $(ISC)^2$ is the Certified Information Systems Security Professional (CISSP) certification.

The CISSP certification was launched in 1994, after the first version of the Common Body of Knowledge had been established in 1992.

$(ISC)^2$ maintains what it calls a Common Body of Knowledge for information security for the following certifications:

- Certified Information Systems Security Professional (CISSP), including:
  - Information Systems Security Architecture Professional (CISSP-ISSAP)
  - Information Systems Security Engineering Professional (CISSP-ISSEP)
  - Information Systems Security Management Professional (CISSP-ISSMP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Authorization Professional (CAP)
- Certified Cloud Security Professional (CCSP)
- Systems Security Certified Practitioner (SSCP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)

All certified $(ISC)^2$ professionals are required to support the $(ISC)^2$ Code of Ethics [35].

4.5 ISECOM

Established back in 2000 and based in Europe (Barcelona, Spain), ISECOM (Institute for Security and Open Methodologies, http://www.isecom.org) provides the very first penetration testing professional certification courses, recognised all over the world: OPST (OSSTMM Professional Security Tester), OPSA (Professional Security Analyst) and OPSE (Professional Security Expert), all based

on the OSSTMM (Open Source Security Testing Methodology Manual), the de-facto standard for running professional penetration tests.

4.6 SANS

The SANS Institute is the largest source for information security training in the world. It provides training programmes to over 165,000 security professionals worldwide and has a large database of information security research. SANS training courses are developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of IT security [25]. SANS also provides access to GIAC Certifications which develops and administers premier, professional information security certifications. More than 30 cyber security certifications align with SANS training and ensure mastery in critical, specialised InfoSec domains.

4.7 Capability Maturity Models

Maturity models establish a systematic basis of measurement for describing the “as is” state of a process. A process’s maturity can then be compared to management’s expectations or contrasted with the maturity of other similar processes for benchmarking purposes. Insights can also be derived from the model for determining improvement options that help a process to satisfy its intended objectives over time.

Clearly, as cybercrime creates continuously and rapidly evolving risks, the tools and techniques to defend and recover must evolve and become mature just as rapidly. Today’s cyber security market still misses a scalable, measurable, but most of all, open and widely accepted maturity model. A methodology that helps organisations and their supply chains to reach the correct maturity level that addresses the specific risk maps of organisations at a reasonable cost.

A good, yet brief explanation of Maturity Models is [13]: *Maturity models establish a systematic basis of measurement for describing the “as is” state of a process. A process’s maturity can then be compared to management’s expectations or contrasted with the maturity of other similar processes for benchmarking purposes. Insights also can be derived from the model for determining improvement options that help a process to satisfy its intended objectives over time*.

CMM and maturity in general is a hot topic in today’s industry, and, recently, also in cyber security processes [14] [15] and eLearning [16] [17]. Even if no unified, formalised, widely accepted standard exists for training on cyber security, there are several private propositions [18].

From a general point of view, A CMM describes process components that lead to better outputs and better outcomes when applied throughout an organisation. A low level of maturity implies a lower probability of success in consistently meeting a specified objective while a higher level of maturity implies a higher probability of success.

Some cyber security related CMMs for example are SANS CMM for Endpoint Security [15] and Cyber Security CMM [14], openSAMM [19], CAMM [20], which also includes the supply-chain. However, there are still no CMM propositions to cover training in cyber security. Usually, CMMs are composed of different elements: (1) levels, (2) components, (3) expectations and (4) supporting tools. A CMM describes process components that lead to better outputs and better outcomes when applied throughout an organisation. A low level of maturity implies a lower probability of success in consistently meeting a specified objective while a higher level of maturity implies a higher probability of success. In terms of training, a high level of maturity means an efficient process to deliver training able to consistently affect the cyber resilience of an enterprise.

5 Conclusions and recommendations

The overview provided in this paper shows:

- As an industry, we're still very dependent on certificates that are US-centric, and which are not based on formal training. It shows knowledge obtained by the certificate holder. This hinders the education of young people and the recognition by employers of competent staff.
- In some European countries, first steps have been taken to set up a certification scheme. In some cases, this includes validating that formal education support these certificates. Uptake of these schemes is still very limited.
- The certification market is dominated by non-European, especially US, companies. A European wide certification scheme including an education framework is lacking.
- Alignment with other international frameworks in this area (like ISO and NIST) is lacking.

Considering the above, the following **recommendations** are made:

1. A comprehensive market study into the age structure and career history of information and cyber security professionals in the European market, training paths and industry demand should be conducted. This would enable better understanding for the actual number and growth of information cyber security professionals, as well as their career development needs and drivers, both upon entering as well as leaving the information and cyber security profession.
2. ECSO should support ENISA and the European standardisation bodies in the development of one European-wide certification scheme and baseline requirements for certification schemes to be met under the purview of public procurement, cyber security and critical infrastructure regulation. As a result, ENISA (or other suitable European body) can offer a European accreditation scheme for cyber security certifications. Leveraging existing market offerings by creating an accreditation scheme for existing cyber security certifications for personnel on a European level, has the potential to drive harmonisation and quality assurance across the board without sacrificing the investment by professionals and businesses in existing certifications.
3. In addition to this and to support the certification scheme, ECSO should coordinate the development of one European-wide education framework for cyber security. This framework needs to support young professionals (via formal education), existing professionals, and professionals joining the cyber security field at a later stage (i.e. after completion of formal education).
4. In the development of the certification scheme as well as the education framework, representatives from existing initiatives at national level should be involved to make this a joint effort.
5. The education framework needs to be internationally recognised and accepted. Cooperation with other parties like NIST (US NICE framework) is recommended.

References

[1] NCSC Certified Professional Scheme, https://www.ncsc.gov.uk/articles/about-certified-professional-scheme

[2] European e-CF framework\: http://www.ecompetences.eu/e-cf-overview/

[3] IISP: https://www.iisp.org/imis15/Default.aspx

[4] ISO: ISO/IEC 27021:2017, Information technology -- Security techniques -- Competence requirements for information security management systems professionals, https://www.iso.org/standard/61003.html

[5] PviB, Job profiles for information security, version 2.0, June 2017, https://www.pvib.nl/kennis-centrum/documenten/job-profiles-information-security-2-0/downloaden

[6] UNI, Italian contribution - UNI 11621-4 “Unregulated professional activities - ICT professional profiles – Part 4: Information security professional profiles, http://store.uni.com/catalogo/index.php/uni-11621-4-2017.html

[7] List of certifications: https://en.wikipedia.org/wiki/List_of_computer_security_certifications

[8] ANSSI, Prestataires de Services de Confiance Qualifiés, http://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/

[9] ANSSI, request for SecNumedu labelling, http://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-f-02_v2.0_dossier_en.pdf (criteria and information request)

[10]ANSSI, commitment convention, http://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-charte_v2-2016-07-22_en.pdf

[11] PLATO, https://www.wodc.nl/binaries/2486-summary_tcm28-73678.pdf

[12] RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

[13] J. Rose, "Selecting, Using, and creating Maturity Models: a tool for assurance and consulting engagements", 2017. [Online]. Available: http://bit.ly/2wyuWPV.

[14] "Cyber Security Capability Maturity Model (CMM) V1.2", Global Cyber Security Capability Centre - University of Oxford, 2014. [Online]. Available: http://bit.ly/2wy3vWo.

[15] G. Hardy, "Behind the Curve? A Maturity Model for Endpoint Security", Sans.org, 2015. [Online]. Available: http://bit.ly/2wy2Q7h.

[16] B. Curtis, W. Hefley and S. Miller, "People Capability Maturity Model", SEI Institute Carnegie Mellon Univ., 1995. [Online]. Available: http://bit.ly/2wy4oOI.

[17] "OPM3® 3rd edition", OPM Experts, LLC, 2013. [Online]. Available: http://www.opmexperts.com/opm3/.

[18] H. Wagenstein, "A capability maturity model for training & education. Chapter one: background and rationale", PMI® Global Congress 2006—North America, 2006 [Online]. Available: http://bit.ly/2wyc9Eh.

[19] OpenSAMM, Software Assurance Model, http://www.opensamm.org/

[20] “Security Think Tank: Measuring security maturity in the supply chain”. Computer security week, http://computerweekly.com/opinion/Security-Think-Tank-Measuring-security-maturity-in-the-supply-chain

[21] P. Rathod and T. Hämäläinen, "A Novel Model for Cybersecurity Economics and Analysis," 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, 2017, pp. 274-279.

[22] National Initiative for Cybersecurity Education (NICE), https://www.nist.gov/itl/applied-cybersecurity/nice
[23] NICE Cybersecurity Workforce Framework, https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
[24] ISACA, Membership, Guidance and Certification for IT Professionals, http://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx
[25] SANS, https://www.sans.org/about/
[26] (ISC)², Official (ISC)² Guide to the CISSP CBK, Fourth Edition
[27] BSI: IT Baseline Protection Manual, role definitions https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKataloge/Inhalt/Rollendefinitionen/rollendefinitionen_node.html (retrieved 2018-08-24)
[28] P. Atzenweiler et al: "Berufe der ICT – 42 Informatik-Berufsbilder und die notwendigen Kompetenzen", SwissICT, © vdf Hochschulverlag AG an der ETH Zürich, 8th edition, 2013, http://berufe-der-ict.vdf-online.ch/post/ICT-Sicherheitsbeauftragter (retrieved 2018-08-24)
[29] (ISC)² Blog, Cybersecurity Workforce Shortage Projected at 1.8 Million By 2022, http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
[30] Frost & Sullivan, Global Information Cyber Security Workforce Study, https://iamcybersafe.org/gisws/
[31] ENISA, 2016, “Definition of Cyber security – Gaps and overlaps in standardisation”, https://www.enisa.europa.eu/publications/definition-of-cybersecurity
[32] Solvay, Digital Transformation & IT Education, solvay.edu/IT
[33] ICT Berufsbildung, ICT Security Expert ED, https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/ict-security-expert-ed/
[34] ICT Berufsbildung, Cyber Security Specialist (EFA), https://www.ict-berufsbildung.ch/themen/projekte/cyber-security-specialist-efa
[35] (ISC)², Code of Ethics, https://www.isc2.org/Ethics
[36] Cyber Security, Study in Finland, Web: https://studyinfo.fi/app/#!/haku/cyber%20security?page=1&facetFilters=teachingLangCode_ffm:EN&tab=los

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91