Cyber Security Certification Programmes

Eleni-Constantina Davri[*], Eleni Darra[*], Isidoros Monogioudis[*], Athanasios Grigoriadis[*], Christos Iliou[†], Notis Mengidis[†], Theodora Tsikrika[†], Stefanos Vrochidis[†], Adamantini Peratikou[‡], Helen Gibson[§], Damir Haskovic[‖], Dimitrios Kavallieros[*#], Evangelos Chaskos[#], Peng Zhao[¶], Stavros Shiaeles[¶], Nick Savage[¶], Babak Akhgar[§], Xavier Bellekens[⁑], Mohamed Amine Ben Farah[⁑]

[*]Center for Security Studies, KEMEA, Athens, Greece: {n.davri, e.darra, i.monogioudis, a.grigoriadis, d.kavallieros}@kemea-research.gr
[†]Information Technologies Institute, CERTH, Thessaloniki, Greece: {iliouchristos, nmengidis, theodora.tsikrika, stefanos}@iti.gr
[‡]Open University of Cyprus, OUC, Nicosia, Cyprus: adamantini.peratikou@ouc.ac.cy
[§]CENTRIC, Sheffield Hallam University, Sheffield, UK: {h.gibson, B.Akhgar}@shu.ac.uk
[‖]MINDS & SPARKS GmbH, Wien, Austria: damir.haskovic@mindsandsparks.org
[#]University of Peloponnese, Tripolis, Greece: {d.kavallieros, e.chaskos}@uop.gr
[¶]University of Portsmouth, Portsmouth, UK: {peng.zhao, stavros.shiaeles, nick.savage}@port.ac.uk
[⁑]University of Glasgow, Glasgow, UK {xavier.bellekens, mohamed.ben-farah}@strath.ac.uk

***Abstract*—Although a large and fast-growing workforce for qualified cybersecurity professionals exists, developing a cybersecurity certification framework has to overcome many challenges. Towards this end, an extended review of the cybersecurity certifications offered currently on the market from 9 major issuing companies is conducted. Moreover, the guidelines for the definition of a cybersecurity certification framework as they are provided from the recent Cyber Security Act and framework of ENISA, NIST and ISO/IEC 17024 are covered. A vast comparison among the presented cybersecurity certifications is given, based not only on the cybersecurity domain covered but also the required level of candidate's experience. A proposed certification program has been also analyzed based on the learning pathways and the knowledge areas described in FORESIGHT.**

Keywords—Cybersecurity, certifications, education, certification frameworks

I. Introduction

The demand for cyber security certification programs has been increased the last years as the need for cyber security professionals is mandatory in almost all organizations. It is estimated that by 2022 the global cyber security workforce will have more than 1.8 million professionals. This means that the workforce environment will become even more demanding, and it will become quite attractive for candidates to fill open positions. Nowadays, it is quite hard for both employees and employers to assess who has the right qualifications for each position. Additionally, all the security domains have been broadened to a wide range of solutions and certificates in terms of quality of service and operational excellence [1].

This paper provides a review of the certifications issued by nine organizations. These certifications were reviewed during the process of identifying the most suitable certification framework for the FORESIGHT H2020 project [2]. Thus, only the certifications that are related with the project's Knowledge Areas have been included in this paper (Section II). The selection of these organizations was made based on the request of employers have regarding certifications (e.g., in job finding sites). All selected organizations are product vendor neutral, well establish and accepted by private and public bodies as proof of knowledge on specific domains of the great area of cybersecurity. Furthermore, a review of three certification frameworks is provided (Section III), depicting the fundamentals of a certification framework.

II. Background

Certifications should verify the knowledge and expertise of the trainees while combine professional training. To achieve that a certification must identify the area of the certification, the objectives, exam-based verification, prerequisites to take the exam or even to be able to register for attendance, identification of sustainability criteria (e.g., how many Continues Education Units (CEUs) needed for renewal) and the respective curriculum. Efforts have been made the last years to develop deferent certification and training models. Authors in [2] proposed a theoretical model regarding professional certifications based on four main steps: i) demand identification of industry and workforce, ii) professional competencies and knowledge, skills and abilities (KSAs), iii) certification domains and objectives and finally iv) education, training curriculum and outcomes.

The approach presented in [4] provides a harmonized integrated and automated approach for the certification in IoT. Additionally, this approach is based on two building blocks: security risk assessment and testing. In particular, the proposal makes use of the main notions from the European Telecommunications Standards Institute (ETSI) risk-based security assessment and testing methodologies, by proposing an instantiation through specific technologies and tools. An improvement of this paper is presented in [5] where a security certification methodology has been designed for IoT to empower different stakeholders with the ability to assess security solutions for large-scale IoT deployments in an automated way. The certification approach represents an instantiation of the Risk-based Security Assessment and Testing methodologies presented by ETSI based on the ISO31000 and ISO29119, and it is built on top of different technologies and approaches for security testing and risk assessment adapted to the IoT landscape. The paper presented in [6] attempts to explore the use of professional certifications as helpful input to shaping and maintaining a cybersecurity curriculum. Authors offer a literature analysis that shows how changes made to professional certifications ((ISC)^2, ISACA, EC Council) are applicable and relevant to maintaining a cybersecurity curriculum. They also provide a case study involving an undergraduate cybersecurity program in a mid-sized university in the United States. In [7] it is examined the nature of the challenge, presenting evidence of the reported skills shortages, and then proceeding to examine the different forms of qualification that are available, and how security practitioners and employers may usefully identify the options that are best suited to their needs. Authors in [8] present the Skills Framework that provides a means to map the landscape and understand where the various qualifications and certifications fit in. For the individual, it offers a means of understanding their own skill base, rating their familiarity and experience of the different groups against the six skill levels that can be involved.

III. Existing Certification Programmes

FORESIGHT curricula will focus in seven Knowledge Areas: i) Security Fundamentals, ii) Web Security, iii) Network security, iv) Software Security, v) IoT and Cloud Security, vi) Digital Forensics and vii) Malware Analysis. All knowledge can be categorized as declarative (factual), procedural (understanding what to do with factual knowledge) and contextual (understanding the "why" of the knowledge). The curricula framework details how knowledge can be taken from larger knowledge areas and broken into smaller subjects. Each subject will have aspects of learning that is declarative, procedural and contextual depending on the pathway being followed.

Verification of expertise in the aforementioned domains is provided through academic education, work experience and certifications. This paper will review certifications available in the market from many organizations through a process of testing skills and knowledge. Among the various organizations, such as (ISC)^2, CompTIA, ISACA, GIAC common practices are used for the certification process. For example, to participate in exams issuing certification, prerequisites are imposed by the issuing organization. Exam preparation is available also by the organizations with different training modes provided (e.g., self-paced, online training, instructorless and more). Specific guidelines per organization are followed for the exam process like duration, Continues Education Units earned or need to renew the certification, etc.

A. International Information System Security Certification Consortium (ISC)^2

The (ISC)^2 was established in the United States in 1989 and has over 150,000 certified members worldwide across the information security sector [9].

CISSP, targets to security professionals looking to certify their knowledge over a range of different cybersecurity domains. For security professionals who have already been CISSP-certified, and they wish to demonstrate their expertise, CISSP-ISSAP (Information Systems Security Architecture Professional) is offered as a follow-on course. The offered certification for IT administrators, network security practitioners and candidates responsible for an organization's systems operation security is SSCP (Systems Security Certified Practitioner). For experienced cloud security professionals of at least five years' experience in IT and three years in information security, CCSP (Certified Cloud Security Professional) is provided. Information security and information assurance practitioner with roles focusing on security assessment, authorization and continuous monitoring is the target participant group of CAP (Certified Authorization Professional) certification. Professionals working in software development who need to incorporate security practices into the software development lifecycle, the ideal certification is CSSLP (Certified Secure Software Lifecycle Professional).

B. Computing Technology Industry Association (CompTIA)

CompTIA was established in 1982 as a non-profit association. It is estimated that until now more that 2 million people have received certification from CompTIA [10].

Network+ is an entry level certification focused on network security, cloud computing and virtualization techniques. CompTIA Security+ covers network security concepts, threats and vulnerabilities, access control, identity management and cryptography. CySA+ certification covers the use of system threat-detection tools, as well as the use of data and behavioral analytics to secure applications and systems from risks, threats and other vulnerabilities. CASP+ certification is the only performance-based, hands-on certification currently available from CompTIA. PenTest+ certification verifies that successful candidates have the knowledge and skills required to plan and scope a security assessment, understand legal and compliance requirements, perform vulnerability scanning and penetration testing and finally report and communicate the results.

C. Information Systems Audit and Control Association (ISACA)

ISACA was established in 1969 and is a non-profit association of about 1.400.00 professionals across 180 countries. ISACA certification exams are computer-based. [11].

The CISA (Certified Information Systems Auditor) certification focuses on auditing, controlling, monitoring, and assessing an organization's information technology and business systems. CISM (Certified Information Security Manager) indicates expertise in information security governance, program development and management, incident and risk management. CGEIT (Certified in the Governance of Enterprise IT) certification assess, design, implement and manage enterprise IT governance systems. CRIST certification (Certified in Risk and Information Systems Control) is designed for those experienced in the management of IT risk and the design, implementation, monitoring, and maintenance of IS controls. ISACA's CDPSE (Certified Data Privacy Solutions Engineer) is about architecture, and lifecycle of data privacy at a technical level. The required experience for entering is three or more years in data privacy governance, privacy architecture, and/or data lifecycle work.

D. Global Information Assurance Certification (GIAC)

Under the scope of General Cyber Security, the certification GIAC Security Essentials (GSEC) validates the knowledge of a medium experienced practitioner on information security and demonstrates his qualification for hands-on IT security tasks [12].

In Incident Response domain, GCIH (GIAC Certified Incident Handler) certification validates a practitioner's ability to detect, respond, and resolve computer security. GCED (GIAC Certified Enterprise Defender) builds on the security skills measured by the GIAC Security Essentials certification. For intermediate experienced under the Incident Response domain again, GICSP (Global Industrial Cyber Security Professional) is provided. GICSP bridges together IT, engineering and cyber security. In Security Analysis domain, GIAC provides GCIA (GIAC Certified Intrusion Analyst) certification, that validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. GCIA certifies the needed skills to configure and monitor intrusion detection systems, and to read, interpret, and analyse network traffic and related log files. GRID (GIAC Response and Industrial Defense) aims to demonstrate professionals' performance on Active Defense strategies to an Industrial Control System (ICS) network and systems. In Penetration Testing domain for experienced audience, GPEN (GIAC Penetration Tester) certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies. The GWAPT (GIAC Web Application Penetration Tester) tries to secure organizations through penetration testing and a thorough understanding of web application security issues. A Penetration Testing certification is GXPN (GIAC Exploit Researcher and Advanced Penetration Tester) trying to find and mitigate significant security flaws in systems and networks. Under the domain of Malware Analysis, the GREM (GIAC Reverse Engineering Malware) certification is designed for experts who exploit reverse-engineer malicious software in the context of forensic investigations, incident response, and Windows system administration. In the scope of Digital Forensics, GCFE (GIAC Certified Forensics Examiner) certification validates emphasizes on core skills required to collect and analyze data from Windows computer systems. GCFA (GIAC Certified Forensic Analyst) certifies experts on how to conduct formal incident investigations and handle advanced incident handling scenarios, including internal and external data breach intrusions, advanced persistent threats, anti-forensic techniques used by attackers, and complex digital forensic cases. Under Network and Software Security domain, GCDA (GIAC Certified Detection Analyst) certifies experienced individuals not only wielding tools such as Security Information and Event Management (SIEM), but also on turning attacker strengths into attacker weaknesses.

E. International Council of Electronic Commerce (EC-Council)

International Council of Electronic Commerce (EC-Council) is an organization that provides support to IT professionals by offering training, certification and educational services in cybersecurity. It was founded in 2001 after the 9/11 attack. As of 2010 the US government department of defense requires all network defenders to pass the certification offered by EC-Council named CEH [13]. CSCU (Certified Secure Computer User) belongs to Security and Networking domain and certifies fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, etc. CND (Certified Network Defender) helps IT Professionals to be more active in the digital business assets protection, detection, and cyber threats response. Under the domain of Information Security, CEH (Certified Ethical Hacker) certification and CEH Practical prove that someone is Master in hacking. ECSA follows a generic kill chain methodology through methodologies covering different pen testing requirements across different verticals. LPT-Master (Licensed Penetration Tester Master) introduces the most advanced penetration testing techniques and is built on backbone of the Advanced Penetration Testing Cyber Range. Another specialist-level certification is the ECIH (EC-Council Certified Security Specialist) trains Incident and Response Handlers on effectively handling of post data consequences. In Forensics domain, CHFI (Computer Hacking Forensic Investigator) certifies professionals on hacking attacks discovery and on properly extracting evidence to report. In Disaster Recovery domain, the EDRP (EC-Council Disaster Recovery Professional) certifies the knowledge around business integrity and continuity after a disaster. To enrich knowledge in cryptography, ECES (EC-Council Certified Encryption Specialist) is provided offering practical application in encryption, VPNs, and cryptographic algorithms. Another hands-on certification for training advanced software development professionals is CASE JAVA/.NET (Certified Application Security Engineer). CTIA (Certified Threat Intelligence Analyst) certification is about building effective threat intelligence. CSA (Certified SOC Analyst) attest certification is designed to Tier 1 and Tier 2 SOC analysts in performing entry- and intermediate-level operations. Another certificate for fundamentals level of the information security, network security and computer forensics is the ECSS (EC-Council Certified Security Specialist).

F. Offensive Security

Offensive Security stared operating in 2007 and is an American international company working in information security, penetration testing and digital forensics. Operating from around 2007, the company created open-source projects, advanced security courses, ExploitDB and the Kali Linux distribution [14]. Especially for penetration testing, there are many certifications provided by Offensive Security for experienced candidates.

OSCP (Offensive Security Certified Professional) certification verifies the ability of a candidate to conduct a penetration test in real world environment within 24 hours. There is OSWP (Offensive Security Wireless Professional) certification focusing on wireless network penetration testing whereas another certification, OSEE (Offensive Security Exploitation Expert) verifies candidates vulnerability assessment skills. The certification focuses on bypassing security mechanisms that are designed to block attacks and covers evasion and breach techniques in greater depth is the OSEP (Offensive Security Experienced Penetration). OSED (Offensive Security Exploit Developer) certification exploits development and reverse engineering techniques in Offensive Security's isolated VPN networks. Finally, the OSWE (Offensive Security Web Expert) certification focuses on white box web app pentest methods through live exploitation of vulnerabilities.

G. CREST

CREST was established in the UK in 2006. Subsequently, CREST International was incorporated in 2015 to act as an umbrella organization for the CREST chapters in Australasia, Hong Kong, Singapore, the UK and USA [15].

CREST offers the CPSA (CREST Practitioner Security Analyst) certification that provides insights of operating systems and common network services. CRT (the CREST Registered penetration Tester) certifies a candidate's ability to carry out basic vulnerability assessment and penetration testing tasks. Assessment of a network for flaws and vulnerabilities at the network and operating system layer is offered by the CCT Inf. (Certified Infrastructure Tester) certification. Regarding web application testing at a medium to high level is provided by the CCT App (CREST Certified web Application Tester) certification. Certification in the wireless communications security domain is offered by the CCWS (CREST Certified Wireless Specialist) module.

Attack simulation is another certification domain covered by CCSAS (CREST Certified Simulated Attack Specialist) and CCSAM (CREST Certified Simulated Attack Manager), focusing on simulated attacks and the exploitation of vulnerabilities. In the domain of security analysis CREST offers a pathway of three certifications, the CPIA (CREST Practitioner Intrusion Analyst), the CRIA (CREST Registered Intrusion Analyst) and the CCNIA (CREST Certified Network Intrusion Analyst) focused in i) network intrusion, ii) host intrusion and iii) malware reverse engineering. Additionally, CCHIA (CREST Certified Host Intrusion Analyst), certifies in the assessment of a Windows host for indications of malware and related forensic artefacts. The CCMRE (CREST Certified Malware Reverse Engineer) focuses on reverse engineer of malwares. The CCIM (CREST Certified Threat Intelligence Manager) qualifies a candidates' competency on incident response and on assessing and handling incident scenarios. Finally, the CRTSA (CREST Registered Technical Security Architect) certification is focused in developing systems architects in secure manner.

H. Mile2

Mile2 provides Information Security training and consulting services that exceed military, government, private sector and institutional specifications [16].

Mile2 provides two certifications for entry level regarding organizational cyber awareness, the C)SA1 (Cyber Security Awareness 1) and the C)SA2 (Cyber Security Awareness 2). C)SP+ (Certified Security Principles+) is provided to verify technical knowledge skills implementation.

In the domain of Cyber Crime and Fraud Investigators, C)DFE (Certified Digital Forensics Examiner) targets in electronic discovery and advanced investigation techniques. The C)PEH (Certified Professional Ethical Hacker) certification is about the functionality of malware and destructive viruses. The Mile2's C)VA (Certified Vulnerability Assessor) certification provides training on the tools an IT engineer needs to review an Information System (medium level). Preventing, detecting and responding to attacks is provided by the C)IHE (Certified Incident Handling Engineer).

The C)NFE provides training for digital and network forensic. Vulnerability identification and exploitation training is provided in the C)PTE (Certified Penetration Testing Engineer) certification. IS20 Security Controls certification covers proven general controls and methodologies that are used to execute and analyze the Top Twenty Most Critical Security Controls. The C)SWAE (Certified Secure Web Application Engineer) certification targets in identification and defense against security vulnerabilities in software applications.

I. eLearnSecurity (eLS)

eLearnSecurity is an information technology security organization that provides cybersecurity education. It is based on a distance and online learning model. eLearnSecurity develops and provides proprietary certifications with a practical focus through scenario-based exams [17].

A certification on penetration testing and information security for entry level individuals is the eJPT (eLearnSecurity Junior Penetration Tester). For experienced penetration testers, the eCPPT (eLearnSecurity Certified Professional Penetration Tester) certification is provided. Assessing a cyber security professional's web application penetration testing skill is given through eWPT (eLearnSecurity Web Application Penetration Tester). The eMAPT (eLearnSecurity Mobile Application Penetration Tester) certification is focused on mobile application security knowledge. The most advanced pen testing certification, with an actual penetration test on a corporate network is eCPTX (eLearnSecurity Certified Penetration Tester eXtreme) certification. Focused on Incident Handling & Response knowledge the eCIR (eLearnSecurity Certified Incident Responder) certification is provided. eCXD (eLearnSecurity Certified eXploit Developer) tests capabilities on Windows and Linux exploit development and software vulnerability identification. The eNDP (eLearnSecurity Network Defense Professional) certification provides proof of hands-on skills through a comprehensive practical exam. Reverse engineers who passing a practical examination can be certified by eCRE (eLearnSecurity Certified Reverse Engineer). Finally, an expert-level certification issued to cyber security professionals after passing a practical examination and proving their threat hunting and threat identification capabilities is the eCTHP (eLearnSecurity's Certified Threat Hunting Professional).

Each knowledge area is made up of subjects, which follow on from each other and cover the fact, processes and context of that subjects. Different levels for the same subject can be made by altering the ratio of fact, process and context (beginner level has a focus on fact and less focus on context – advanced level has a high focus on context). Each knowledge area of the FORESIGHT curriculum (except security fundamentals) offers opportunities to focus on fact, process and context. Table 1 provides a comparison of all these certifications in terms of knowledge area and level of expertise. The level of expertise is divided in three (3) levels, Beginner (B), Intermediate (I), Advanced (A). The three levels of expertise will be discussed in detail in Section V.

Table 1: Cyber Security Certifications Map

Issuing Company	Certification	Security Fundamentals	Network Security	Software Security	Digital Forensics	IoT & Cloud Security	Web Security	Malware Analysis	L/E
(ISC)^2	CISSP	✓		✓		✓	✓		A
	CISSP-ISSAP	✓	✓	✓		✓			A
	CISSP-ISSEP	✓	✓	✓					A
	SSCP	✓	✓	✓	✓			✓	A
	CCSP				✓				A
	CAP		✓	✓					A
	CSSLP		✓	✓					A
CompTIA	CompTIA A+	✓							B
	CompTIA Network+		✓			✓			I
	CompTIA Security+		✓	✓		✓	✓		I
	CompTIA CySA+		✓	✓		✓	✓		A
	CompTIA CASP+		✓	✓	✓	✓	✓	✓	A
	CompTIA PenTest+	✓	✓	✓	✓	✓	✓		I
ISACA	CISA	✓							I
	CISM	✓							I
	CGEIT	✓							I
	CRISC	✓							I
	CDPSE		✓	✓		✓	✓		I
GIAC	GSEC	✓	✓			✓			I
	GCIH		✓		✓			✓	A
	GCED		✓		✓			✓	A
	GICSP	✓	✓	✓		✓		✓	I
	GCIA		✓		✓				A
	GCFA				✓				A
	GRID				✓			✓	A
	GPEN		✓	✓					A
	GWAPT						✓		A
	GXPN		✓	✓				✓	A
	GREM							✓	A
	GCFE				✓				I
	GCDA		✓	✓					A
EC-Council	CSCU		✓	✓			✓		B
	CND		✓			✓			I
	CEH/CEH Practical		✓	✓		✓	✓	✓	A
	ECSA			✓		✓	✓		A
	LPT-Master			✓		✓	✓	✓	A
	ECIH			✓	✓			✓	A
	CHFI				✓				A
	EDRP	✓							I
	ECES		✓			✓			A
	CASE JAVA/.NET			✓	✓	✓	✓		A
	CTIA			✓				✓	A
	CSA attest	✓							B
	ECSS	✓							B
Offensive Security	OSCP	✓	✓	✓			✓		A
	OSWP	✓	✓						A
	OSEE			✓					A
	OSEP	✓		✓			✓		A
	OSED			✓				✓	A
	OSWE						✓	✓	A
CREST	CPSA	✓	✓				✓		B
	CRT	✓	✓				✓		I

IV. CERTIFICATION FRAMEWORK

The EU cybersecurity certification plays a vital role in the increase of trust and security in products and services. Several security certification schemes for ICT products exist in Europe but without a common framework that will apply and be valid in EU by all Member States. The reason for a common certification framework is the alignment of all MSs with a set of rules, technical requirements, standards and procedures. This common framework will certify that ICT products and services will comply with specified requirements.

A. ENISA/Cyber Security Act

Based on the Regulation (EU) 2019/881 (Cybersecurity Act), the important task is that one of cybersecurity certification. The purpose of the EU cybersecurity certification framework under Cyber Security Act is to establish and maintain the trust and security on ICT digital products, services and processes. As set out in Cybersecurity Act, the EU cybersecurity certification framework lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognized and used in all Member States. Each certification scheme will specify one or more level(s) of assurance (basic, substantial or high), based on the level of risk associated with the envisioned use of the product, service or process [18], [19].

The role of the certification framework is to provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. Additionally, the certification framework will indicate that ICT products and services comply with specified requirements. In particular, each European certification scheme should specify: a) the categories of products and services covered, b) the cybersecurity requirements, for example by reference to standards or technical specifications, c) the type of evaluation (e.g., self-assessment or third-party evaluation), and d) the intended level of assurance (e.g., basic, substantial and/or high).

B. National Institute of Standards and Technology (NIST)

The NIST Framework for Improving Critical Infrastructure Cyber Security was published in response to the US Presidential Executive Order 13636 and is aimed at improving the security operations and governance of public and private organizations. The framework is supplementing the Cybersecurity Enhancement Act (CEA) of 2014 and will continue evolving according to the CEA [20].

The framework is organized in three distinct parts, the framework core, the implementation tiers and the framework profiles. The core is a set of cybersecurity activities, references and outcomes that are similar across CI. The core further supplements the implementation tiers and the profile. The implementations tier provides context on an organization's view on cybersecurity and the processes currently in place to manage risks. The profiles correspond to individual organization profiles allowing to map business activities, missions, requirements, risk tolerances and resources. The Framework is based around five function areas each containing a variety of categories, sub-categories and informative references.

- **Functions**: organize cybersecurity activities at the highest level of abstraction. Including, Identify, Protect, Detect, Respond and Recover. These aid an organization focus on priorities.
- **Categories**: provide subdivision of a function into a group of cybersecurity outcomes.
- **Sub-categories**: further expand on a category and identify specific technical or management activities.
- **Informative references**: provide specific sections of official guidelines, standards or practice that can be referred to during implementation.

The framework illustrates how an organization can improve an existing program by providing a set of steps to follow a) **Step1**: Prioritize and Scope, b) **Step2**: Orient, c) **Step3**: Create an organization profile, d) **Step4**: Conduct a risk assessment, e) **Step5**: Create a target profile, f) **Step6**: Determine, Analyze and Prioritize Gaps, g) **Step7**: Implement an Action Plan.

C. ISO/IEC 17024:2012

ISO/IEC 17024:2012 "Conformity assessment — General requirements for bodies operating certification of persons" contains principles and requirements for a body certifying persons against specific requirements and includes the development and maintenance of a certification scheme for persons [21]. Here, all elements of the certification program are addressed. This includes the structure of the program, definition and implementation of the requirements for earning, maintaining and renewing certification, design, implementation and monitoring of assessment systems, management system requirements procedures to manage financial and staff resources, ensuring security of exams and reporting systems and providing fair and equitable treatment for all candidates for certification and certification holders.

V. FORESIGHT INITIAL CERTIFICATION FRAMEWORK

FORESIGHT H2020 project aims on building holistic cybersecurity training across all levels of expertise, utilizing the capabilities offered by Cyber Range solutions. It will also extend these capabilities through the development of a federated solution, connecting three Cyber Ranges and six Technical Environments (or Labs) across Europe. This will be wrapped in a new certification targeting both the general public as well as people from three domains, Power Grid, Aviation and Naval providing training tailored to these specific domains and their needs.

The initial approach is to design three certification levels, Beginner, Intermediate and Advance as depicted in Fig. 1.

Beginner level will provide the basic knowledge in the greater field of cybersecurity and IT (e.g. networking) while it will also provide the possibility for people that do not want to follow an IT career (e.g. secretaries) to gain awareness for cybersecurity matters so as to avoid been victimized and minimize the risk to open the "gate" to attackers (e.g. learn how to recognize phishing emails). In that way, the beginner level will offer training on curricula specified to the FORESIGHT knowledge areas described in Section III. Two options will be offered:

- The theoretical training that will introduce core themes and terminology to raise awareness of cyber security.
- The basic concepts of cyber security giving also further details on the FORESIGHT knowledge areas.

The **Beginner level** will give the chance for participants to either select to be trained only in the awareness option or select to be trained in content that includes core themes, terminology and basic concepts of cyber security. Further to that, this level will offer ECTS (European Credit Transfer and Accumulation System) credits to the participants that have to gain in order to pass the exam and renew it every 3 years in terms of validity. This level will also become the basis for the audience to be prepared for the intermediate level.

Intermediate level will provide more in-depth knowledge. Participants who are familiar with the cyber security areas will be trained to increase their skills. Both theoretical and hands-on training will be offered to domain specific and non-domain specific experts. In the case of hands-on training, participants have to follow the company's policy of enrollment that is paid by the individual or by the company. For domain specific training either people with expertise in a respective domain (proof of work) will be eligible in the training and evaluation process or everyone will be able to participate. Finally, the certification will offer ECTS credits that need to be renewed every three years in order to be valid. For the non-domain specific training, the participants will have to pass the beginner level (proof of certificate) or prove 3 years of expertise in the respective field.

Advanced level will continue from where the intermediate level stopped, providing more difficult curricula and examination process. It will engage people with high cyber security skills to be trained in order to become specialists. They will be involved in more challenging scenarios and educational modules. The process to be followed is the same as in the intermediate level as regards to domain specific and non-domain specific experts. Theoretical and hands-on training will be offered to the experts based on their level of expertise. The only difference with the intermediate level includes the proof of success or 5 years of expertise in case of non-domain specific participants.

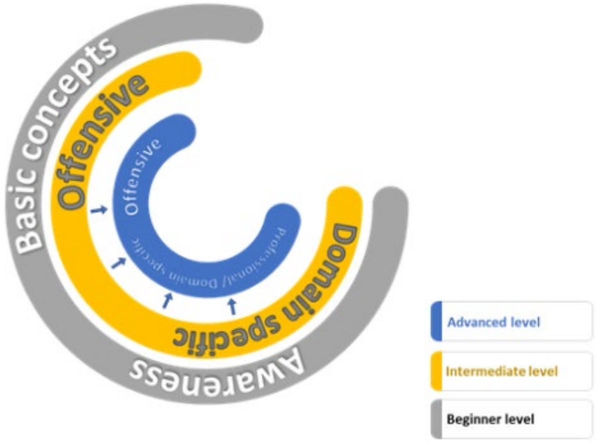

Fig. 1. FORESIGHT Certification Program

FORESIGHT certification will be the first in the field of cyber security on the three domains. The certification will be renewed every three years and Continues Education Points will be accepted for renewal. The curriculum for each subject in a knowledge area will be reviewed on a yearly basis and the knowledge areas will be reviewed every 3 years. The pathway assessments for beginner, intermediate and advanced level will be reviewed yearly.

VI. Conclusion and Future Work

Certifications are providing training and the proof that an individual has specific knowledge and falls under specific level of expertise. This paper reviews nine (9) vendor agnostic issuing organizations and their certifications in the greater area of cybersecurity. The particular selection of nine certifications was made according to the popularity and employability of these certifications, excluding product vendor certifications (e.g., CISCO, AWS, IBM). The target area of each certification, prerequisites and level of expertise was analyzed in a matrix (Table 1). Furthermore, three (3) certification frameworks were analyzed (NIST, ISO and ENISA/EU Cybersecurity Act). A detailed plan

The next step is to utilize this information, combined with the FORESIGHT training curricula, end-user needs and setup a new certification in the field of cybersecurity, which except the general training will also focus at three specific domains of Aviation, Power Grid and Naval. This will include a complete mapping between the modules offered by the nine certifications reviewed and the modules FORESIGHT will incorporate, the different pathways (e.g., incident handling, digital forensics), exact renewal points that will be needed and the sustainability schema. The FORESIGHT assessment will be set at three different levels according to the pathway that trainees will take: beginner, intermediate and advanced. The beginner pathway assessment will focus on facts and application of facts and will include an assessment for general cyber security awareness. The intermediate assessment will focus on processes associated with the FORESIGHT knowledge domain and will include general assessment pathways, domain specific pathways and offensive pathways. The advanced pathway will include domain specific assessments required to analyze and synthesize solutions and an offensive pathway.

Acknowledgment

This paper has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 833673. The work reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

References

[1] Frost & Sullivan, Global Information Cyber Security Workforce Study, https://iamcyber-safe.org/gisws/

[2] https://foresight-h2020.eu/ Retrieved June 5, 2021

[3] P. Wang, H. D'Cruze, "Cybersecurity Certification: Certified Information Systems Security Professional (CISSP)," In Proc. ITNG 2019, Advances in Intelligent Systems and Computing, vol. 800, Springer, 2019.

[4] S. Matheu, J. Hernandez-Ramos, A. Skarmeta, "Toward a Cybersecurity Certification Framework for the Internet of Things," IEEE Security & Privacy, vol. 17, no. 3, pp. 66-76, 2019.

[5] S. Matheu-García, J. Hernández-Ramos, A. Skarmeta, G. Baldini, "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices," Computer Standards & Interfaces, vol. 62, pp. 64-83, 2019.

[6] Kenneth J. Knapp, Christopher Maurer, Miloslava Plachkinova, "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance", Journal of Information Systems Education, Vol. 28(2), December 2017

[7] Steven Furnell, "The cybersecurity workforce and skills", Computers & Security, Vol. 100, January 2021.

[8] Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security, 2017(2), 5–10

[9] "Cybersecurity and IT Security Certifications and Training|(ISC)^2." isc2.org, https://www.isc2.org

[10] CompTIA Certifications (2021). Retrieved March 30, 2021, from https://www.comptia.org/certifications/

[11] ISACA Certificates (2021). Retrieved March 30, 2021 from https://www.isaca.org/credentialing/certificates

[12] GIAC Cybersecurity Certifications (2021). Retrieved March 30, 2021, from https://www.giac.org/certifications/focus-areas

[13] EC-Council Cybersecurity Programs."United States Department of Defense Embraces Hacker Certification to Protect U.S. Interests." https://www.eccouncil.org/programs/

[14] OFFENSIVE Security Certifications. Retrieved March 17, 2021 from https://offensive-security.com/courses-and-certifications/

[15] The Council for Registered Ethical Security Testers (CREST). Retrieved June 7 2021, https://www.crest-approved.org/

[16] Mile2 Cybersecurity Certification. Retrieved March 30, 2021, from https://www.mile2.com/cert-roadmap/

[17] eLearnSecurity Certifications. Retrieved March 16, 2021, from https://elearnsecurity.com/

[18] "Cybersecurity Certification: EUCC Candidate Scheme." Retrieved March 18, 2021, from https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). [Online] Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[20] "Cybersecurity Framework." nist.gov. Retrieved April 8, 2021 from https://www.nist.gov/cyberframework

[21] "How to develop schemes for the certification of persons - Guidance of ISO/IEC 17024." iso.org