Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cyber security cOmpeteNCe fOr Research anD InnovAtion†

Feasibility Study "Cybersecurity Skills Certifications"[1]

Abstract: This document contains the results of the analysis of the current situation regarding the certification of cybersecurity skills and the conclusions regarding the gaps derived by the project team.

Editors	*TÜV TRUST IT* *University of Patras*
Contributors	*TUBV* *EIT Digital*
Quality Assurance	*FORTH* *Atos* *Uni Subria* *Siemens*

† This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

1 This document is part of the Deliverable D3.2 and is to be considered as draft, pending the official approval of the European Commission

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUDA	Technical University of Darmstadt	Germany
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURFnet bv	SURFnet bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG Schweiz AG	RUAG Schweiz AG	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec Energia	EFACEC Energia	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
BMW Group	Bayerische Motoren Werke AG	Germany
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria

IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy

Executive summary

The goal of WP3 is to reinforce Europe's cybersecurity leadership by developing and evaluating building blocks for a European cross-sector cybersecurity infrastructure, specifically for collaborative threat handling, technology and service experimentation, training and education, and starting up new businesses. WP3 utilizes WP1's technology developments and WP2's industry pilots and this inter-WP cooperation has been successfully initiated in Y1.

Task 3.4, will contribute to the development of a European Education Ecosystem for Cybersecurity through a number of targeted actions addressing mainly the cybersecurity industry and its professionals (technicians, mid-level management, executives) and teachers.

As the first step of this Task and in order to develop a framework for a CONCORDIA Cybersecurity Skills certificate, a Feasibility study for a Cybersecurity Skills Certification Scheme was conducted. The Feasibility study comprised of an analysis of the relevant existing Role Profiles, frameworks and certification schemes and aimed to identify possible gaps.

The analysis identified 5 major Profile schemes and 50 Cybersecurity Skills Certification Schemes of various levels and concepts. These Certification Schemes were mapped to the most popular role profiles and the gap between the role profiles and the available Certification Schemes was identified. This Feasibility study concludes with the role profiles that are currently lacking representation in existing Cybersecurity Skills Certification and a proposal regarding the subsequent steps of the Task's implementation.

Contents

1. Introduction

As mentioned in the Executive Summary, Task 3.4, will contribute to the development of a European Education Ecosystem for Cybersecurity through a number of targeted actions addressing mainly the cybersecurity industry and its professionals (technicians, mid-level management, executives) and teachers.Within this task, the project team plans to develop a CONCORDIA Cybersecurity Skills Certification Scheme. Various studies (as shown below in the Market Analysis Section) show that there "is a strong shortage of Cybersecurity related competences in existing personnel within the organizations while at the same time, there is an increasing difficulty to find competent professionals from the market". (Frost & Sullivan, 2017). Providing high quality training and a reliable Cybersecurity Skills Certification Scheme is the way that CONCORDIA plans to address this shortage.

The introduction of a Cybersecurity Skills Certification Scheme aims to inspire trust and ensure that the qualification holders have actually acquired the learning outcomes documented in it, the CONCORDIA team has decided to follow the international best practices contained within ISO 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons. (International Organization for Standardization, 2012) and the various recommendations published by various relevant Authorities and Organizations like ISO, ISO CASCO, IAF, CEDEFOP etc. (analysis is provided in the Certification Scheme Document).

1.1. ISO 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons

ISO 17024:2012, clearly states that "A certification scheme shall contain the following elements: a) scope of certification; b) job and task description; c) required competence; d) abilities (when applicable); e) prerequisites (when applicable); f) code of conduct (when applicable)."
This means that before a CONCORDIA Cybersecurity Skills Certification Scheme is designed, the specific scope of certification, the tasks, the required competence and the relevant abilities have to be defined.

As the aim of CONCORDIA is not to further fragment the market, it was decided to design a Cybersecurity Skills Certification Scheme that will address an existing gap in the market and not introduce a Cybersecurity Skills Certification Scheme that has already been covered by another organization (private or public).

1.2. Cybersecurity Skills Certification Scheme Feasibility Study

To fulfil the above-mentioned objective, a feasibility study needs to be carried out. This

feasibility study consists of the following steps:

- Analysis on the current market situation regarding the needs of Cybersecurity Skills and relevant certifications. This is deemed mandatory since a successful certification scheme should address a practical and existing need of the market.
- Analysis on the existing frameworks regarding Cybersecurity competence in Europe and outside Europe. As shown also from ISO 17024, an acceptable profile containing the tasks, competencies and abilities should exist for the corresponding Certification Scheme to be defined.
- Analysis on the existing Cybersecurity Skills Certification Schemes, since it is important that the CONCORDIA Cybersecurity Skills Certification Scheme covers an existing need and gap of the market and not try to substitute an existing one.

The information included in this Cybersecurity Skills Certification Scheme Feasibility Study, will be used to map a course of action relevant to actions of Task 3.4.

1.3. Structure of the Document

The structure of this document is briefly described below:

Chapter 1: Introduction.

The information contained in the Chapter provides an overview of the scope of this document as well as the specific aims and perspectives.

Chapter 2: Analysis on the current situation regarding Cybersecurity Skills Gap.

This chapter describes the sources and results of the analysis conducted by the project team and pinpoint the Market situation regarding the shortage in Cybersecurity related competences and certifications.

Chapter 3: Analysis on the existing frameworks regarding Cybersecurity competence.

Since a Skill's Certification scheme can not be defined without the relevant Job Profile, this chapter contains the results of the analysis of existing frameworks regarding Cybersecurity competence in Europe and the rest of the world for given profiles.

Chapter 4: Analysis on the existing Cybersecurity Skills Certification Schemes.

There is a number of existing Cybersecurity Skills Certification Schemes that have already been designed and implemented by European and worldwide organizations. This Chapter contains the results of the relevant analysis.

Chapter 5: Identification of Current gaps in Cybersecurity Skills Certification.

Based on the results of the existing frameworks regarding Cybersecurity competence and of the existing Cybersecurity Skills Certification Schemes, a mapping has been carried out. This mapping reveals the areas where there is strong representation in the market and the areas that present low or lacking representation in the market.

Chapter 6: Conclusions and steps forward.

This final chapter of this document contains the conclusions of the Cybersecurity Skills Certification Scheme Feasibility Study and a proposal regarding the next steps towards a CONCORDIA Cybersecurity Skills Certification Scheme.

2. Analysis on the current situation regarding Cybersecurity Skills Gap.

There are several surveys conducted by Professional Organizations worldwide on the subject of Cybersecurity Skills, their current situation, the possible value of related certifications and the steps that need to be performed. The project team conducted a literature review, through which several of these surveys were analysed and their results evaluated.

The review was conducted in two steps regarding:

1. The underlying need for Cybersecurity professionals
2. The current situation regarding the existence of such professionals and related skills.

2.1. The Need for Cybersecurity Professionals

The most popular of these surveys on the subject of Cyber Threats / Risks worldwide are the following:

- Executive Perspectives on Top Risks 2019 and 2020, Protiviti (Protiviti, 2019)
- The Global Risks Report 2019, World Economic Forum (World Economic Forum, 2019)
- Ninth Annual Cost of Cybercrime Study, Accenture (Accenture, 2019)
- Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019, (ISC)2, ((ISC)2, 2019)
- State of Cybersecurity 2019 & 2020, ISACA (ISACA, 2020)

The common characteristic of these surveys is that all of them **identify threats relating to Cybersecurity as an emerging and persistent issue**. From the Executive Perspectives on Top Risks of 2020, the 1063 board members and executives across a variety of industries that participated in the survey, stated that the issue of Cyber Threats is classified as having a "Significant Impact" over the next 12 months. It's worth mentioning that the classification of "Significant Impact" (represented in the results with numbers 6 and above) is the highest category of the methodology employed. This classification has brought Cyber Threats in the sixth position of the identified Top Risks for 2020[Figure 1], with Privacy / Identity management and information security occupying the seventh position.

The survey has been conducted in 2018 and since, it is being observed that Cyber Threats remain at the same (roughly) position in all the three consecutive years.

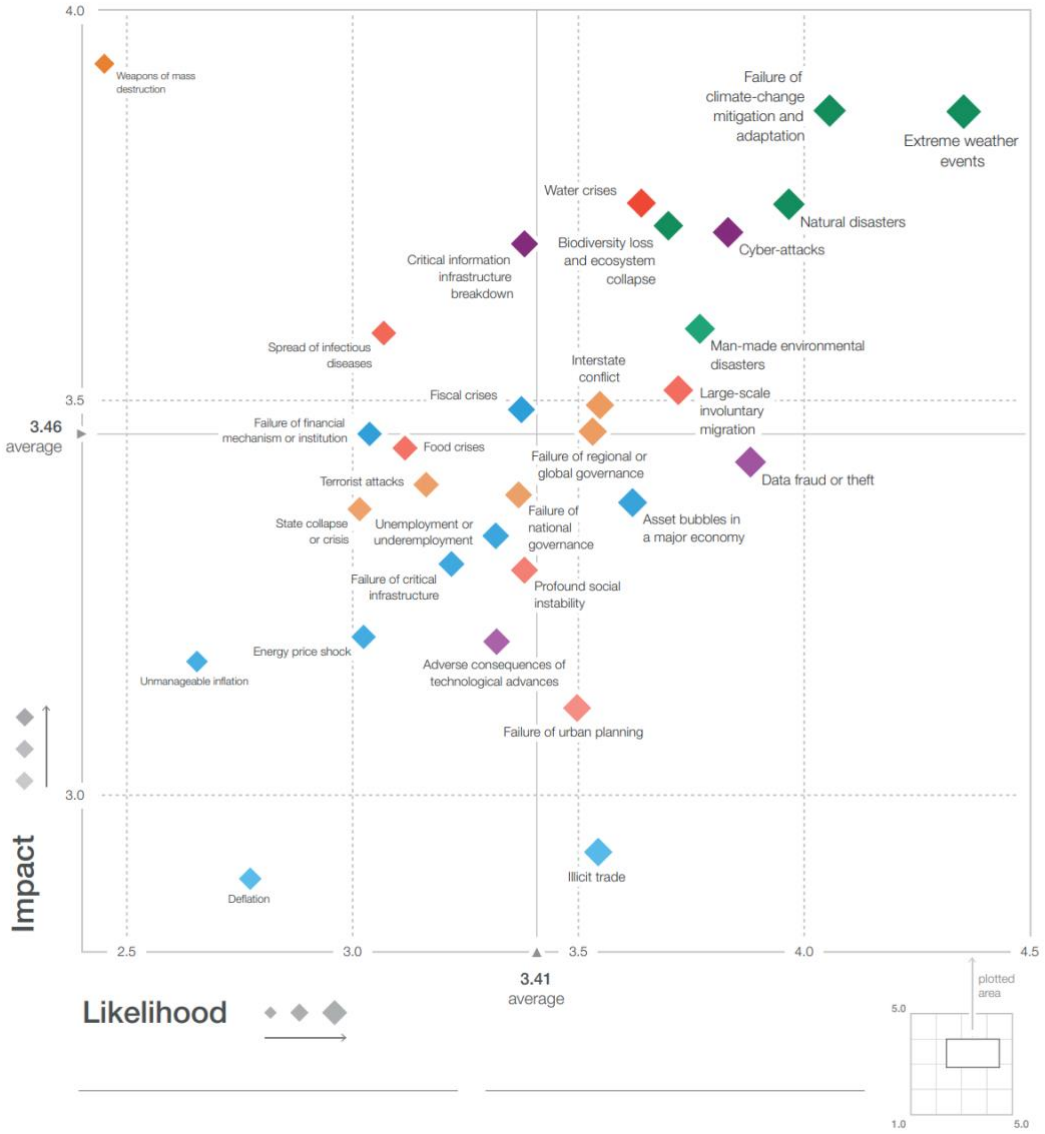
[Figure 1. Executive Perspectives on Top Risks for 2020, Infografic]

TOP 10 RISKS FOR 2020

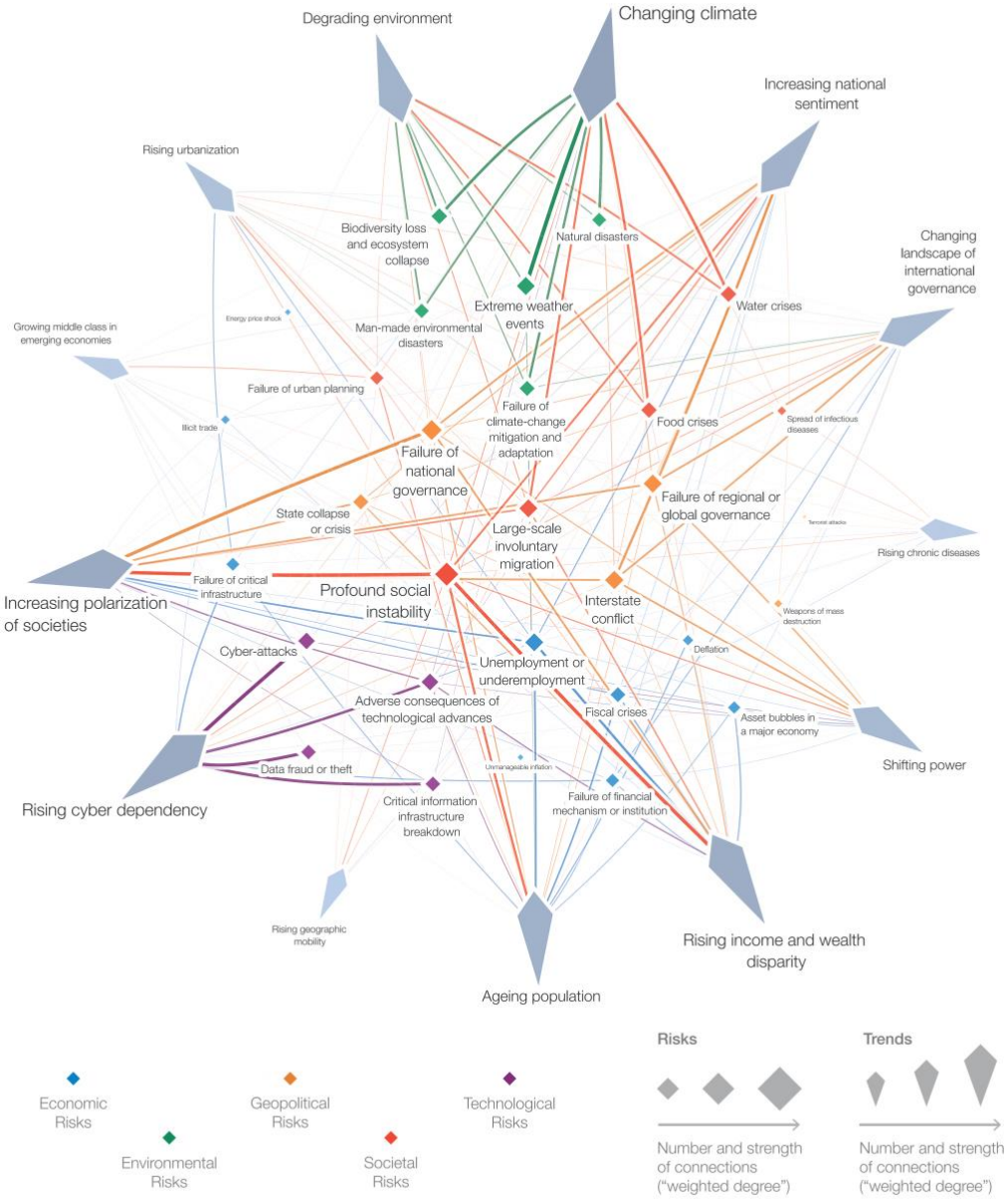
	RISK ISSUE	2020*	2019 (rank)*
1.	Impact of regulatory change and scrutiny on operational resilience, products and services	**6.38**	6.24 *(3)*
2.	Economic conditions impacting growth	**6.34**	5.93 *(11)*
3.	Succession challenges; ability to attract and retain top talent	**6.27**	6.34 *(2)*
4.	Ability to compete with "born digital" and other competitors	**6.23**	6.35 *(1)*
5.	Resistance to change operations	**6.15**	6.17 *(5)*
6.	Cyber threats	**6.09**	6.18 *(4)*
7.	Privacy/identity management and information security	**6.06**	6.13 *(7)*
8.	Organization's culture may not sufficiently encourage timely identification and escalation of risk issues	**5.83**	5.99 *(9)*
9.	Sustaining customer loyalty and retention	**5.82**	5.95 *(10)*
10.	Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees *(new in 2020)*	**5.71**	N/A *(new)*

Moreover, The Global Risks Report 2019, by the World Economic Forum[Figure 2], shows the area of Cyber as an area with emerging threats closely connected to the dependency on IT and the rise of connected services, leading to the conclusion that the related threats will not fade but rather increase in the years to come.

[Figure 2. The Global Risks Report 2019, The Global Risks Landscape 2019]



[Figure 3. The Global Risks Report 2019, The Risks-Trends Interconnections Map 2019]



Source: World Economic Forum Global Risks Perception Survey 2018–2019.
Note: Survey respondents were asked to select the three trends that are the most important in shaping global development in the next 10 years. For each of the three trends identified, respondents were asked to select the risks that are most strongly driven by those trends. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

2.2. The current situation regarding the existence of such professionals and related skills

The most popular of the surveys on the subject of Cybersecurity Skills, competencies and the existence of related Professionals, worldwide, are the following:

- Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019, (ISC)2, ((ISC)2, 2019)
- (ISC)² Cybersecurity Workforce Study in 2018, (ISC)2 ((ISC)2, 2018)
- State of Cybersecurity 2019 & 2020, ISACA (ISACA, 2020)

- 2017 Global Information Security Workforce Study, Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, Centre for Cybersecurity Studies, 2017 (Frost & Sullivan, 2017).
- Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements" Final Report (Danish Technological Institute and Fraunhofer, 2012).
- Skills Panorama (CEDEFOP, 2018)
- ICT professionals: skills opportunities and challenges (2019 update) (CEDEFOP, 2019)
- WG5 ANALYSIS Information and Cyber Security Professional Certification Task Force (EHR4CYBER), ECSO (ECSO, 2020)

Based on the Skills Panorama (CEDEFOP, 2018), around 3.5 million people were employed as ICT professionals in 2018. Employment in the occupation grew by just over 29 per cent between 2006 and 2018. Employment is projected to grow by a further 11 per cent over the period 2018 to 2030.

One of the drivers of change that will affect their skills is cybercrime and cyberterrorism. As mentioned in ICT professionals: skills opportunities and challenges (2019 update) (CEDEFOP, 2019), "The demand for cybersecurity skills relating to both software and hardware systems will grow. Besides sector-specific expertise, these professionals will probably need to have high-level qualifications to meet the demands of the interconnected "smart" infrastructure systems of the future". Also, Cedefop identifies security as a future core e-skill, in the Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements" Final Report (Danish Technological Institute and Fraunhofer, 2012).

Moreover, ECSO's (European Cyber Security Organisation) WG5 ANALYSIS Information and Cyber Security Professional Certification Task Force (EHR4CYBER) stipulate that 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. Also, it is hard for both employees and employers to assess who has the right qualifications for the open positions."

Moreover, both ISACA and (ISC)2 respectively on their publications conclude that:

- Enterprises are still short-staffed in cybersecurity, struggle to find sufficient talent for open positions and expect their cybersecurity budgets to grow. Efforts to increase the number of women in cybersecurity roles progressed slightly, and more enterprises established gender diversity programs.
- A shortage in the global cybersecurity workforce continues to be a problem for companies in all industries and of all sizes. In fact, this shortage remains the number one job concern for those working in the field. That's not surprising given that 2018 was "the year of the megabreach."

Finaly, in the (ISC)² Cybersecurity Workforce Study in 2018, the participants stated that "cybersecurity certifications and training are important for maintaining and advancing their careers". And the vast majority, 86%, are either currently pursuing cybersecurity certifications or planning to in the future, as it was considered important for Advancing their careers (56%), for maintaining their career (54%) and for beginning their careers (38%).

3. Analysis on the existing frameworks regarding Cybersecurity competence.

Jobs, roles and competences are terms commonly used when describing the actions, responsibilities, tasks and skills of people in the workplace. The terminology is often used interchangeably but still, efore proceeding further, it is important to provide definitions of relevant and frequently used.

3.1. Terms and Definitions

Term	Definition	Reference
Competence	Demonstrated ability to apply knowledge, skills and attitudes to achieve observable results. Competences form part of the Role Profiles. A demonstrated ability to apply knowledge, skills and attitudes for achieving observable results	(CEN, 2018) (CEN/TC 428, 2020)
Job description	A detailed description of what a person does so that the particular job holder can have no doubt of their tasks, duties and responsibilities and who they report to. It contains precise information about competences, skills and knowledge required as well as practical information about health and safety and remuneration. Note: Job Descriptions are not included in the Role Profiles but they can be developed from the Profiles.	(CEN, 2018)
Knowledge	Body of facts, principles, theories and practices that is related to a field of work or study. An employee needs to know the relevant selection of these to successfully perform in their job. Knowledge is a body of information applied directly to the performance of a function. represents the “set of know-what” (e.g. programming languages, design tools…) and can be described by operational descriptions.	(CEN, 2018) (NIST, 2018) (CEN/TC 428, 2020)
Role	A role derives from an organisational need to get something done. It is an organisational requirement that can be met by assigning employees to carry out all or part of the tasks required to ensure that role is carried out. One person or team may have multiple roles.	(CEN, 2018)
Role Profile	An outline or general document which demonstrates clearly the relationship between specific activities/tasks in a role and the individual skills, competences and knowledge required to undertake them.	(CEN, 2018)
Skill	The ability to use know-how and expertise to complete tasks and solve problems. Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the	(CEN, 2018) (NIST, 2018)

	psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual. the ability to carry out managerial or technical tasks	(CEN/TC 428, 2020)
Work Roles	Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.	(NIST, 2018)
Ability	is competence to perform an observable behavior or a behavior that results in an observable product.	(NIST, 2018)
Task	is a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.	(NIST, 2018)
Attitude	the "cognitive and relational capacity" (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism…). If skills are the components, attitudes are the glue, which keeps them together.	(CEN/TC 428, 2020)

3.2. European ICT Professional Role Profiles

The function of European ICT Professional Role Profiles is to offer users structure and clarity for designing or identifying and clustering the multitude of activities that are essential to support the digital strategy of an organisation. They are less detailed and less specific than job descriptions and offer a simple but flexible start point. They also represent a European multi-stakeholder shared perspective and provide a common reference language and communication tool to support mutual understanding e.g. both between countries but also within organisations such as between HR and ICT departments.

There are a huge range of different job titles across the ICT profession and they are created for a variety of purposes including attracting new recruits and providing recognition for organisation loyalty through promotion and construction of enhanced job titles. Jobs are unique, but a similar title can be used to describe a widely different jobs or similar jobs can be described by different titles. This can be confusing and prevent clear understanding between different actors and stakeholders of the job described and its associated tasks and responsibilities.

The European ICT Professional Role Profiles address this lack of clarity by clustering typical and common job role components into a consistent role profile template. These role profiles, built from an organisational perspective, may be adopted and used as a basis for many activities including, personal development, organisation and job family restructuring, curriculum and training course development. The profiles are designed to be consistent in structure but varied in content offering clear differentiation between each profile.

3.2.1. The European e-Competence Framework (e-CF)

The European e- Framework (e-CF) Competence standard EN 16234-1 is a main element of the ICT Professional Profiles description template. The e-CF provides a reference of currently 40 competences as required and applied at the ICT workplace, using a common reference language for competences, skills, knowledge and capability levels that can be understood across Europe/ internationally.

The e-CF is the result of 10 years continuing effort and commitment by the European ICT sector. As the first sector-specific and workplace-oriented implementation of the European Qualifications Framework (EQF), the e-CF supports the definition of jobs, training courses, qualifications, career paths, formal and non-formal learning paths, certifications etc. In this way, ICT service in public and private organisations, ICT professionals, managers and HR departments, vocational education, higher education and other training, assessment and accreditation bodies, social partners, professional associations, market analysts and policy makers have access to a shared reference.

The European Norm (EN) 16234-1 European e-Competence Framework (e-CF) provides a reference of 41 competences as applied to the Information and Communication Technology (ICT) workplace, using a common language for competences, skills, knowledge and proficiency levels that can be understood across Europe.

The structure of the European e-Competence Framework is based on four dimensions shown below (CEN/TC 428, 2020):

Dimension 1	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. 32 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 [Note 1].
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.

[Note 1: The European Qualifications Framework (EQF) (Council of the European Union, 2017) is a common European reference framework whose purpose is to make qualifications more readable and understandable across different countries and systems. Covering qualifications at all levels and in all sub-systems of education and training, the EQF provides a comprehensive overview over qualifications in the 39 European countries currently involved in its implementation. The core of the EQF is its eight reference levels defined in terms of learning outcomes, i.e. knowledge, skills and autonomy-responsibility. Learning outcomes express what individuals know, understand and are able to do at the end of a learning process. Countries develop national qualifications frameworks (NQFs) to implement the EQF. Based on a structured method employed by the experts of the e-CF, a mapping has been produced between the EQF levels and the e-CF levels. This table is given in Appendix B. An overview of the e-CF is provided in Appendix A.

3.2.2. Deliverables identification and description methodology

Deliverables, together with e-CF Competences, form one of the main components defining the European ICT Professional Role Profiles. Deliverables describe typical outcomes of a task in a working context. Each ICT Professional Role Profile is defined by a list of Deliverables, either in terms of being accountable, responsible or in terms of contribution.
To support European ICT Professional Role Profiles descriptions the three attributes are defined and applied as follows:

• Accountable (A): The individual ultimately answerable for the correct and thorough completion of the deliverable
• Responsible (R): The individual who performs the work to achieve the deliverable
• Contributor (C): The individual who contributes, due to their capability and knowledge

An ICT Profile includes a list of Deliverables applied as follows:

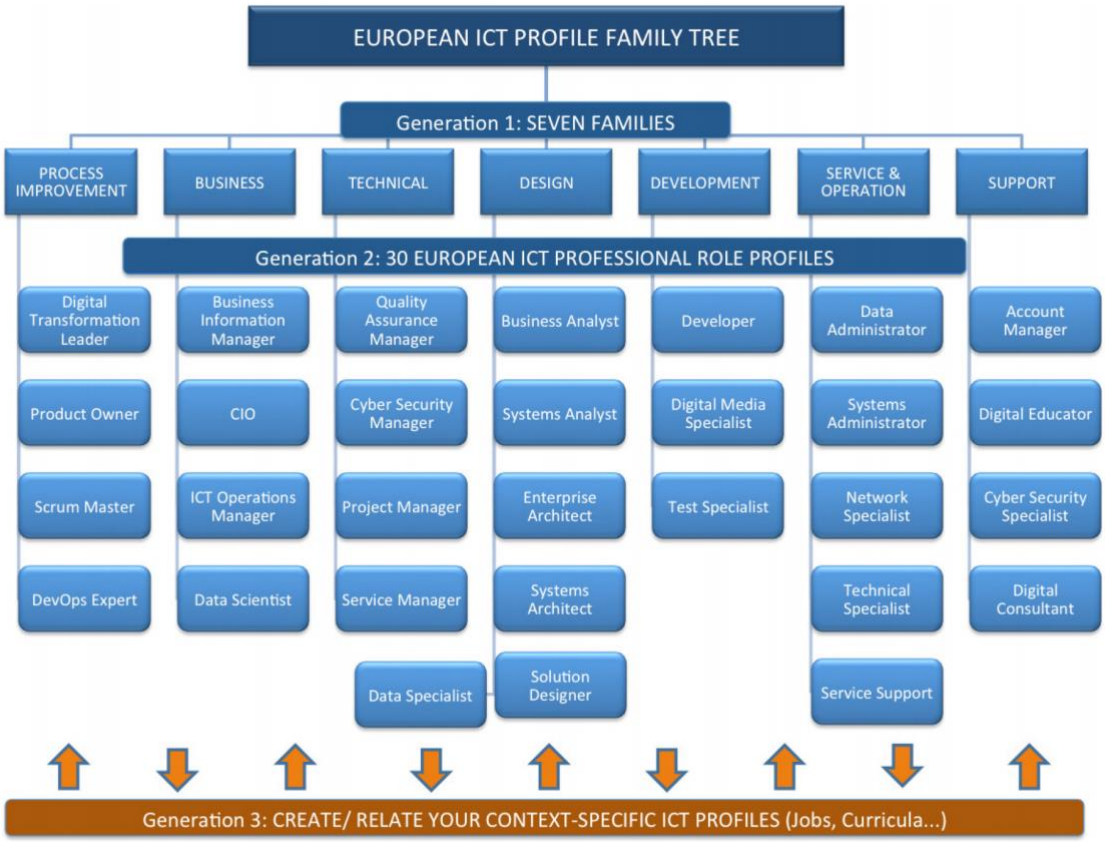
• Each profile incorporates up to six deliverables formed from a combination of accountable, responsible or contributor descriptions
• A deliverable may or may not be seen by users, may be intermediate or final, but must always be observable.

3.2.3. List of identified EU ICT Professionals Role Profiles

CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles (CEN, 2018) provides 30 European ICT Professional Role Profiles accompanied by their full descriptions.

Incorporating the competences of the European eCompetence Framework (e-CF, EN 16234-1) as a main component of profile descriptions, the 30 ICT Professional Role Profiles provide a generic set of typical roles performed by ICT Professionals in any organisation, covering the full ICT business process. Complementary to the e-CF, the European ICT Professional Role Profiles contribute to a shared European reference language for developing, planning and managing ICT Professional needs in a long-term perspective and to maturing the ICT Profession overall.

The following image, drawn from CWA 16458-1:2018, shows the 30 ICT Professional Role Profiles, in an ICT family tree. Structured from the seven main ICT Profile families, the 30 profiles reflect the top of a European ICT Profile Family Tree.



[Figure 4. CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles, European ICT Professional Role Profiles version 2: 30 profiles (generation 2) in seven families (generation 1) at the top of the European ICT Profile Family Tree]

In the document of the European ICT Professional Role Profiles referenced above, there is also a more detailed description of each ICT Professional Role Profile. Each ICT Professional Role Profiles contains the following elements:

- Profile title
- Summary statement
- Mission
- Deliverables
- Main task/s
- E-competences (from the e-CF) and
- KPI area

An example of the Professional Role Profile of the Cyber Security Manager is contained in Appendix C.

From the 30 ICT Professional Role profiles of the CWA 16458-1:2018, the ones that are relevant to Cybersecurity are:

- Cyber Security Manager
- Systems Administrator
- Network Specialist
- Cyber Security Specialist

3.3. ESCO

ESCO (European Skills, Competences, Qualifications and Occupations) (European Comission , 2020`)is the European multilingual classification of Skills, Competences, Qualifications and Occupations.

ESCO works as a dictionary describing, identifying and classifying professional occupations, skills, and qualifications relevant for the EU labour market and education and training. Those concepts and the relationships between them can be understood by electronic systems, which allow different online platforms to use ESCO for services like matching jobseekers to jobs on the basis of their skills, suggesting trainings to people who want to reskill or upskill etc.

ESCO provides descriptions of 2942 occupations and 13.485 skills linked to these occupations, translated into 27 languages (all official EU languages plus Icelandic, Norwegian and Arabic). Over time, it will also display the qualifications awarded in the education and training systems from Member States, as well as qualifications issued by private awarding bodies.

The aim of ESCO is to support job mobility across Europe and therefore a more integrated and efficient labour market, by offering a "common language" on occupations and skills that can be used by different stakeholders on employment and education and training topics.
ESCO is a European Commission project, run by Directorate General Employment, Social Affairs and Inclusion (DG EMPL). It is available in an online portal and can be consulted free of charge. Its first full version (ESCO v1) was published on the 28th of July 2017.
More specifically, ESCO concepts and descriptions can help people to understand:

- what knowledge and skills are usually required when working in a specific occupation;
- what knowledge, skills and competences are obtained as a result of a specific qualification;
- what qualifications are demanded or often requested by employers from those searching for work in a specific occupation.

The work produced by ESCO at the time of this publication, contains 2942 occupations, 13485 skills / competences and 9606 qualifications.

The search in the ESCO occupations database for Cybersecurity entitled occupations did not produce results.The only results contained within the ESCO occupations database related to Cybersecurity are the following:

Occupation Title	Alternative Occ. Titles	description
ICT security administrator	system security administrator, network security administrator, ICT security administrators, IT security administrator	ICT security administrators plan and carry out security measures to protect information and data from unauthorised access, deliberate attack, theft and corruption.

ICT security consultant	IT security expert, IT security consultant, ICT security consultants, information communications technology security consultant, consultant in ICT security activities, IT security advisor, ICT security advisor, information technology security consultant	ICT security consultants advise and implement solutions to control access to data and programs. They promote a safe exchange of information.
Chief ICT security officer	chief ICT security officers, chief information security officer, head of IT security, CISO, head IT security officer	Chief ICT security officers protect company and employee information against unauthorized access. They also define the Information System security policy, manage security deployment across all Information Systems and ensure the provision of information availability.
ICT security manager	ICT security chief, ICT technical security expert, IT security manager, information security manager, ICT security managers, security coordinator, IT security chief	ICT security managers propose and implement necessary security updates. They advise, support, inform and provide training and security awareness and take direct action on all or part of a network or system.

Director of compliance and information security in gambling	compliance director, gaming compliance and information security manager, gambling compliance and information security manager, director, compliance and information security in gaming, manager of compliance and information security in gaming, gambling compliance and information security director, manager, compliance and information security in gambling, director, compliance and information security in gambling, gaming compliance and information security director, manager, compliance and information security in gaming, security information director, security information manager, manager of compliance and information security in gambling	Directors of compliance and information security in gambling follow the regulatory compliance for gambling and oversee Information Security to ensure secure and safe use of all information technology associated in gambling.
ICT security technician	IT security officer, ICT security officer, ICT security technicians, IT security technician	ICT security technicians propose and implement necessary security updates and measures whenever is required. They advise, support, inform and provide training and security awareness.

For each of these Occupations, an analysis on Skills / Competencies is performed containing the following fields:

- Code
- Description
- Alternative label
- Regulatory aspect
- Hierarchy
- Essentials skills and competences
- Essential Knowledge
- Optional skills and competencies
- Optional Knowledge
- Status and
- Concept URI

To provide a better understanding regarding the structure and content, the example of the chief ICT security officer is provided in Appendix D.

3.4. NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) (NIST, 2017) , published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers regardless of where or for whom the work is performed .

This publication provides a fundamental reference in support of a workforce capable of meeting an organization's cybersecurity needs by using a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role. It provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role.

The components of the NICE Framework are:

- Categories
- Specialty Areas
- Work Roles
- Associated supersets of Knowledge, Skills, and Abilities and
- Tasks for each work role.

Short descriptions of the components are given as follows:

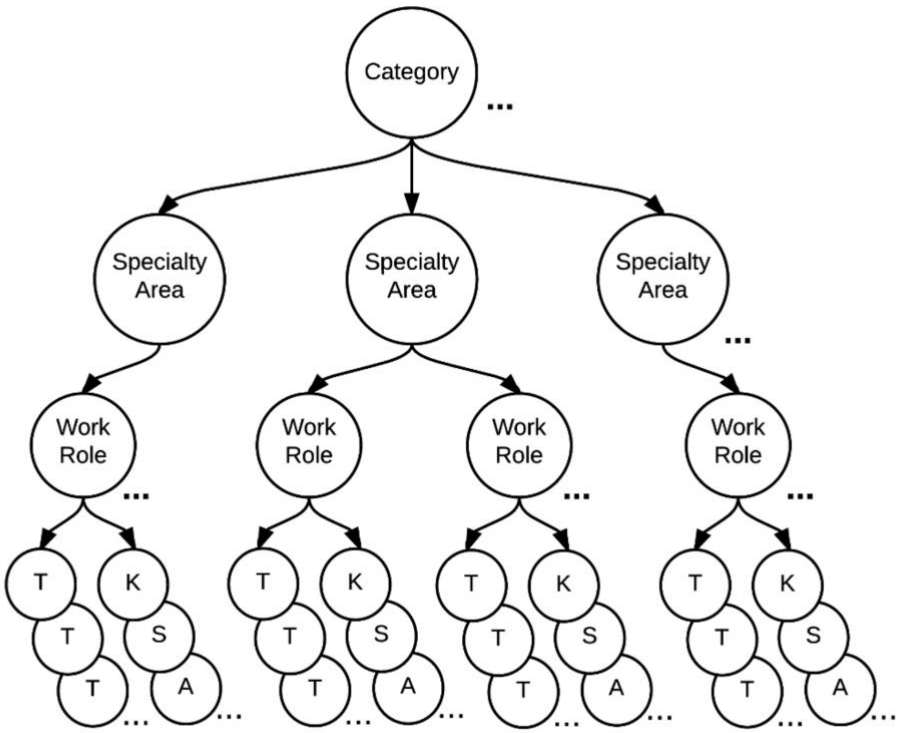
Categories: Categories provide the overarching organizational structure of the NICE Framework. There are seven Categories and all are composed of Specialty Areas and work roles. This organizational structure is based on extensive job analyses, which group together work and workers that share common major functions, regardless of job titles or other occupational terms.

Specialty Areas: Categories contain groupings of cybersecurity work, which are called Specialty Areas. There were 32 specialty areas called out in National Cybersecurity Workforce Framework version 2.0. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.

Work Roles: Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role. Work being performed in a job or position is described by selecting one or more work roles from the NICE Framework relevant to that job or position, in support of mission or business processes. To aid in the organization and communication about cybersecurity responsibilities, work roles are grouped into specific classes of categories and specialty areas.

Knowledge, Skills, and Abilities (KSAs): Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training. (The definitions for Knowledge, Skills, Abilities and Tasks under the NICE framework have been provided above and are not repeated here.).

The following image, provides for a better presentation of the relationships and hierarchy between the above-mentioned components.



[Figure 5. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) (NIST, 2017) Relationships among NICE Framework Components.]

The main NICE Framework Workforce Categories are shown in the following table:

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

[Figure 6. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) (NIST, 2017), NICE Framework Workforce Categories.]

Each Category has a number of Speciality areas:

Categories	Number of Speciality Areas
Securely Provision (SP)	7
Operate and Maintain (OM)	6

Oversee and Govern (OV)	6
Protect and Defend (PR)	4
Analyze (AN)	5
Collect and Operate (CO)	3
Investigate (IN)	2

52 Work Roles related to Cybersecurity have been identified and are contained as titles in the following table:

All Source-Collection Manager	IT Program Auditor
All Source-Collection Requirements Manager	IT Project Manager
All-Source Analyst	Knowledge Manager
Authorizing Official/Designating Representative	Law Enforcement /CounterIntelligence Forensics Analyst
Communications Security (COMSEC) Manager	Mission Assessment Specialist
Cyber Crime Investigator	Multi-Disciplined Language Analyst
Cyber Defense Analyst	Network Operations Specialist
Cyber Defense Forensics Analyst	Partner Integration Planner
Cyber Defense Incident Responder	Privacy Officer/Privacy Compliance Manager
Cyber Defense Infrastructure Support Specialist	Product Support Manager
Cyber Instructional Curriculum Developer	Program Manager
Cyber Instructor	Research & Development Specialist
Cyber Intel Planner	Secure Software Assessor
Cyber Legal Advisor	Security Architect
Cyber Operator	Security Control Assessor
Cyber Ops Planner	Software Developer
Cyber Policy and Strategy Planner	System Administrator
Cyber Workforce Developer and Manager	System Testing and Evaluation Specialist
Data Analyst	Systems Developer
Database Administrator	Systems Requirements Planner
Enterprise Architect	Systems Security Analyst
Executive Cyber Leadership	Target Developer
Exploitation Analyst	Target Network Analyst
Information Systems Security Developer	Technical Support Specialist
Information Systems Security Manager	Threat/Warning Analyst
IT Investment/Portfolio Manager	Vulnerability Assessment Analyst

The next level of description, contains the relevant Knowledge, Skills, Abilities and Tasks per Work Role, but they are too big a volume to include in this document. In total the NICE framework contains 1191 Knowledge, Skills and Abilities and 1006 Tasks. The example of the Information Systems Security Manager as an example is included in Appendix E.

3.4.1. The Cyberseek tool

Visualizing the need for and supply of cybersecurity workers across the US, a Cybersecurity Jobs Heat Map, CyberSeek, (Comptia and Burning Glass Technologies, 2020) has been

developed by CompTIA in partnership with Burning Glass Technologies. The tool provides data to help employers, job seekers, policy makers, training providers, and guidance counselors meet today's increasing demand. When the tool was first launched in 2016, CyberSeek unveiled information on the supply of workers with relevant credentials and career pathways in cybersecurity that map opportunities for advancement in the field.

In the Fall of 2019, NICE, CompTIA, and Burning Glass Technologies announced that the CyberSeek tool would be expanded to tackle the increasingly critical problem of cybersecurity skills gaps and worker shortages. CyberSeek is supported by the National Initiative for Cybersecurity Education (NICE) and is built upon the framework.

The tool contains:

- A heat map of cybersecurity supply and demand, and
- An interactive career pathway showing common roles within cybersecurity and transitions opportunities between them

By navigating in the different Roles of the interactive map, the viewer can find the following information:

- The feeder roles
- The possible advancements
- The Average Salary
- The common job titles
- The total job openings
- The common NICE Cybersecurity Workforce Framework categories
- The requested education
- The Top Certifications required and
- The Top skills requested

The Roles contained in the interactive map of Cyberseek are:

- Cybersecurity Specialist / Technician
- Cyber Crime Analyst / Investigator
- Incident Analyst / Responder
- IT Auditor
- Cybersecurity Analyst
- Cybersecurity Consultant
- Penetration & Vulnerability Tester
- Cybersecurity Manager / Administrator
- Cybersecurity Engineer
- Cybersecurity Architect

The example of the analysis of the Cybersecurity Manager / Administrator is given in Appendix F.

4. Analysis on the existing Cybersecurity Skills Certification Schemes.

For this section of the Feasibility Study, a review of public information was conducted in order to identify some of the existing cyber security skills certification schemes. For each of

these schemes, information regarding the knowledge and skills covered has been collected and compiled in this document. The source of this information is in most cases the website of the issuing organization. (e.g. for CISM certificate, ISACA, for CISSP certification, (ISC)2 etc). It has to be noted that the review was not exhaustive. The project team restricted the results to the ones referenced as Top Certifications.
Some of the sources of these references are:

- The Cyberseek website (Comptia and Burning Glass Technologies, 2020)
- The Cybrary website (Cybrary, 2020)
- The Cyberdegrees website (Cyberdegrees, 2020)/
- 10 Hot Cybersecurity Certifications For IT Professionals To Pursue In 2020, (10 Hot Cybersecurity Certifications For IT Professionals To Pursue In 2020, 2020)
- Top 10 Most Popular Cybersecurity Certifications In 2019 (Forbes, 2019)

Due to the volume of the gathered information, the results of this analysis is detailed in Appendix G. The results of this review are combined with the information contained in the following sources:

- WG5 ANALYSIS Information and Cyber Security Professional Certification, Task Force WG5 I European Human Resources Network for Cyber (EHR4CYBER), NOVEMBER 2018, ECSO, (ECSO, 2020)
- The information on the interactive career pathway regarding the Top Certifications requested for the contained roles, (Comptia and Burning Glass Technologies, 2020)

And the following table, containing the Cybersecurity Skills Certification Schemes examined by the project team, was derived:

Certification Scheme	Issuing organization
CERTIFIED INFORMATION SECURITY MANAGER	ISACA
CERTIFIED INFORMATION SYSTEMS AUDITOR	ISACA
CSX(F)	ISACA
CSX(P)	ISACA
CYBERSECURITY AUDIT	ISACA
CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL	ISACA
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT	ISACA
CERTIFIED ETHICAL HACKER	EC-COUNCIL
COMPUTER HACKING FORENSICS INVESTIGATOR	EC-COUNCIL
COMPTIA CYBERSECURITY ANALYST	COMPTIA
COMPTIA ADVANCED SECURITY PRACTITIONER	COMPTIA
COMPTIA SECURITY+	COMPTIA
COMPTIA PENTEST+	COMPTIA
COMPTIA NETWORK+	COMPTIA
OFFENSIVE SECURITY CERTIFIED PROFESSIONAL	OFFENSIVE SECURITY
OFFENSIVE SECURITY WIRELESS PROFESSIONAL	OFFENSIVE SECURITY

OFFENSIVE SECURITY CERTIFIED EXPERT	OFFENSIVE SECURITY
OFFENSIVE SECURITY EXPLOIT EXPERT	OFFENSIVE SECURITY
OFFENSIVE SECURITY WEB EXPERT	OFFENSIVE SECURITY
CERTIFIED CLOUD SECURITY PROFESSIONAL	ISC2
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL	ISC2
SYSTEMS SECURITY CERTIFIED PRACTITIONER	ISC2
CERTIFIED AUTHORIZATION PROFESSIONAL	ISC2
CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL	ISC2
HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER	ISC2
EITCA/IS	EITCI
CESG CERTIFIED PROFESSIONAL (CCP) SCHEME	CREST
GIAC CYBERSECURITY CERTIFICATIONS	GIAC
GIAC SECURITY LEADERSHIP	GIAC
GIAC SYSTEMS AND NETWORK AUDITOR	GIAC
GIAC INFORMATION SECURITY PROFESSIONAL	GIAC
GIAC STRATEGIC PLANNING, POLICY, AND LEADERSHIP	GIAC
GIAC CERTIFIED INTRUSION ANALYST	GIAC
GIAC CERTIFIED INCIDENT HANDLER	GIAC
OSSTMM PROFESSIONAL SECURITY TESTER	ISECOM
OSSTMM PROFESSIONAL SECURITY ANALYST	ISECOM
OSSTMM PROFESSIONAL SECURITY EXPERT	ISECOM
OSSTMM WIRELESS SECURITY EXPERT	ISECOM
OSSTMM CERTIFIED TRUST ANALYST	ISECOM
CERTIFIED SECURITY AWARENESS INSTRUCTOR	ISECOM
ISO/IEC 27001 LEAD AUDITOR	ANSI, AFNOR, ETC.
ISO/IEC 27001 IMPLEMENTOR	ANSI, AFNOR, ETC.
ISO/IEC 27005 RISK MANAGER	ANSI, AFNOR, ETC.
KCEH / MEH (EQUIVALENT TO CEH IN HUNGARIAN)	KÜRT AKADÉMIA / CYBER INSTITUTE

CISCO CERTIFIED NETWORK ASSOCIATE	CISCO
CISCO CERTIFIED NETWORK PROFESSIONAL	CISCO
CISCO CERTIFIED INTERNETWORK EXPERT	CISCO
IT INFRASTRUCTURE LIBRARY (ITIL) CERTIFICATION	AXELOS
PROJECT MANAGEMENT PROFESSIONAL	PMI
CERTIFIED PUBLIC ACCOUNTANT	AICPA
CERTIFIED INTERNAL AUDITOR	IIA GLOBAL
ENCASE CERTIFIED EXAMINER	OPENTEXT™ ENCASE™ FORENSIC

5. Identification of Current gaps in Cybersecurity Skills Certification.

The last step in this feasibility study is the combination of the information derived from all the above-mentioned steps, and create a matrix between Roles and Cybersecurity Skills Certification schemes. The purpose of this exercise is to identify possible areas where relevant certification schemes have not been developed.

This matrix contains:

- 62 Profile Roles derived from all the sources mentioned in Chapter 3.
- 52 Cybersecurity Skills Certification Schemes

The detailed matrix combining the above information is contained in Appendix H.

The following table contains the aggregated results of the relevant matrix.

Ref. No.	Profile Roles	Number of mapped Cert.
1	Cybersecurity Manager	8
2	System Administrator	3
3	Network Specialist	5
4	Cybersecurity Specialist	13
5	ICT SECURITY ADMINISTRATOR	12
6	ICT SECURITY CONSULTANT	0
7	CHIEF ICT SECURITY OFFICER	9
8	ICT SECURITY MANAGER	8
9	DIRECTOR OF COMPLIANCE AND INFORMATION SECURITY IN GAMBLING	10
10	ICT SECURITY TECHNICIAN	16
11	ALL SOURCE-COLLECTION MANAGER	2
12	ALL SOURCE-COLLECTION REQUIREMENTS MANAGER	0
13	ALL-SOURCE ANALYST	2

14	AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE	5
15	COMMUNICATIONS SECURITY (COMSEC) MANAGER	5
16	CYBER CRIME INVESTIGATOR	0
17	CYBER DEFENSE ANALYST	2
18	CYBER DEFENSE FORENSICS ANALYST	2
19	CYBER DEFENSE INCIDENT RESPONDER	2
20	CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST	2
21	CYBER INSTRUCTIONAL CURRICULUM DEVELOPER	0
22	CYBER INSTRUCTOR	1
23	CYBER INTEL PLANNER	0
24	CYBER LEGAL ADVISOR	4
25	CYBER OPERATOR	0
26	CYBER OPS PLANNER	0
27	CYBER POLICY AND STRATEGY PLANNER	4
28	CYBER WORKFORCE DEVELOPER AND MANAGER	3
29	DATA ANALYST	0
30	DATABASE ADMINISTRATOR	1
31	ENTERPRISE ARCHITECT	4
32	EXECUTIVE CYBER LEADERSHIP	2
33	EXPLOITATION ANALYST	2
34	INFORMATION SYSTEMS SECURITY DEVELOPER	0
35	INFORMATION SYSTEMS SECURITY MANAGER	3
36	IT INVESTMENT/PORTFOLIO MANAGER	2
37	IT PROGRAM AUDITOR	5
38	IT PROJECT MANAGER	2
39	KNOWLEDGE MANAGER	1
40	LAW ENFORCEMENT /COUNTERINTELLIGENCE FORENSICS ANALYST	0
41	MISSION ASSESSMENT SPECIALIST	3
42	MULTI-DISCIPLINED LANGUAGE ANALYST	0
43	NETWORK OPERATIONS SPECIALIST	5
44	PARTNER INTEGRATION PLANNER	0
45	PRIVACY OFFICER/PRIVACY COMPLIANCE MANAGER	1
46	PRODUCT SUPPORT MANAGER	0
47	PROGRAM MANAGER	2
48	RESEARCH & DEVELOPMENT SPECIALIST	4
49	SECURE SOFTWARE ASSESSOR	2
50	SECURITY ARCHITECT	0
51	SECURITY CONTROL ASSESSOR	5
52	SOFTWARE DEVELOPER	0
53	SYSTEM ADMINISTRATOR	3
54	SYSTEM TESTING AND EVALUATION SPECIALIST	3
55	SYSTEMS DEVELOPER	0
56	SYSTEMS REQUIREMENTS PLANNER	2
57	SYSTEMS SECURITY ANALYST	1
58	TARGET DEVELOPER	0

59	TARGET NETWORK ANALYST	0
60	TECHNICAL SUPPORT SPECIALIST	3
61	THREAT/WARNING ANALYST	0
62	VULNERABILITY ASSESSMENT ANALYST	2

The profile roles with the most mapped certification schemes are:

Profile Roles	Number of mapped Cert.
ICT SECURITY TECHNICIAN	16
Cybersecurity Specialist	13
ICT SECURITY ADMINISTRATOR	12
DIRECTOR OF COMPLIANCE AND INFORMATION SECURITY IN GAMBLING	10
CHIEF ICT SECURITY OFFICER	9
Cybersecurity Manager	8
ICT SECURITY MANAGER	8
Network Specialist	5
AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE	5
COMMUNICATIONS SECURITY (COMSEC) MANAGER	5
IT PROGRAM AUDITOR	5
NETWORK OPERATIONS SPECIALIST	5
SECURITY CONTROL ASSESSOR	5

And the profiles having no mapped certification schemes are:

- ICT SECURITY CONSULTANT
- ALL SOURCE-COLLECTION REQUIREMENTS MANAGER
- CYBER CRIME INVESTIGATOR
- CYBER INSTRUCTIONAL CURRICULUM DEVELOPER
- CYBER INTEL PLANNER
- CYBER OPERATOR
- CYBER OPS PLANNER
- DATA ANALYST
- INFORMATION SYSTEMS SECURITY DEVELOPER
- LAW ENFORCEMENT /COUNTERINTELLIGENCE FORENSICS ANALYST
- MULTI-DISCIPLINED LANGUAGE ANALYST
- PARTNER INTEGRATION PLANNER
- PRODUCT SUPPORT MANAGER
- SECURITY ARCHITECT
- SOFTWARE DEVELOPER
- SYSTEMS DEVELOPER
- TARGET DEVELOPER
- TARGET NETWORK ANALYST
- THREAT/WARNING ANALYST

6. Conclusions and steps forward

This document contains the steps followed by the project team, for the implementation of a feasibility study on Cybersecurity Skills. This feasibility study represents the first step towards the creation of a CONCORDIA Cybersecurity Skills Certification Framework.

As described at the beginning of this document, the steps conducted during the feasibility study were:

- Analysis on the current market situation regarding the needs for Cybersecurity Skills and relevant certifications.
  Conclusions: The analysis of the situation revealed that **threats relating to Cybersecurity exist and are perceived to rise in the following years** due to the high dependence to informatics and the implementation of more solutions (e.g. IoT, 5G etc). Also, a **shortage in the global cybersecurity workforce continues to be a problem** for companies in all industries and of all sizes. This shortage has been identified since 2017 and still remains. **Certification of Cybersecurity skills is a subject that professionals are pursuing in order to advance their careers or to retain their position**. Finally, employers have identified **Certification of Cybersecurity skills as a useful tool in the validation of related skills**.
- Analysis on the existing frameworks regarding Cybersecurity competence in Europe and outside Europe.
  Conclusions: The existence of formal Role Profiles addresses the lack of clarity by clustering typical and common job role components into a consistent role profile template. Within the European Union, the basis for the Professional Profiles is the European e- Framework (e-CF). The **CWA 16458-1:2018** European ICT Professional Role Profiles – Part 1: 30 ICT Profiles, defines 30 ICT profiles, of which only **four (4) are related to Information / Cyber Security**. **ESCO** provides descriptions of 2942 occupations and 13.485 skills linked to these occupations, of which **six (6) related to Information / Cyber Security**. Finally, in the US, National Initiative for Cybersecurity Education (**NICE**) Cybersecurity Workforce Framework (NICE Framework), presents **52 Work Roles related to Cybersecurity**.
- Analysis on the existing Cybersecurity Skills Certification Schemes.
  Conclusions: **52 current Cybersecurity Skills Certification** Schemes were examined by the project team.
- Identification of Current gaps in Cybersecurity Skills Certification.
  Conclusions: The results of the Role Profile analysis and the Cybersecurity Skills Certification schemes, were cross referenced and a matrix was derived showing the matches between the Role Profiles and the Certification Schemes. This cross reference revealed **Role Profiles with many available certification schemes** (e.g. ICT Security Technician with 16 mapped Certification schemes) and some **Role Profiles with no identified Certification schemes**.

The next steps, that need to be performed, leading to the Creation and Piloting of a CONCORDIA Cybersecurity Skills Certification Framework are:

- The **design of a CONCORDIA Cybersecurity Skills Certification Framework** that will incorporate the best practices of International Standards (e.g. ISO 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons).
- The further analysis regarding the Role Profiles that do not have a mapped certification scheme and would be candidates for the piloting of the **CONCORDIA Cybersecurity Skills Certification Framework.**

These next steps are given in the relevant Deliverables.

References

(ISC)2. (2018). *(ISC)² Cybersecurity Workforce Study in 2018.* (ISC)2.

(ISC)2. (2019, 1 1). *Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019.* Retrieved from (ISC)2: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

10 Hot Cybersecurity Certifications For IT Professionals To Pursue In 2020. (2020, 5 26). Retrieved from Cybercrime Magazine: https://cybersecurityventures.com/10-hot-cybersecurity-certifications-for-it-professionals-to-pursue-in-2019/

Accenture. (2019, 3 6). *Ninth Annual Cost of Cybercrime Study.* Retrieved from Accenture: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

CEDEFOP. (2018). https://skillspanorama.cedefop.europa.eu/en. Thessaloniki, Greece.

CEDEFOP. (2019, 11). https://skillspanorama.cedefop.europa.eu/en/analytical_highlights/ict-professionals-skills-opportunities-and-challenges-2019-update. Thessaloniki, Greece.

CEN. (2014). *European e-Competence Framework 3.0.* Retrieved from ECOMPETENCES.EU: http://www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf

CEN. (2018). *CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles.* Geneva: CEN.

CEN. (2018). *CWA 16458-3:2018, European ICT professional role profiles - Part 3: Methodology documentation.* Retrieved from Ecompetences: https://www.ecompetences.eu/ict-professional-profiles/

CEN/TC 428. (2020). Methodology of the e-cf.

Comptia and Burning Glass Technologies. (2020, 5 25). *Cyberseek*. Retrieved from Cyberseek: https://www.cyberseek.org/

Council of the European Union. (2017, 05 24). *Recommendation on the EQF.* Retrieved from Europa.eu: http://data.consilium.europa.eu/doc/document/ST-9620-2017-INIT/en/pdf

Cyberdegrees. (2020, 5 26). *https://www.cyberdegrees.org/resources/certifications*. Retrieved from Cyberdegrees: https://www.cyberdegrees.org/resources/certifications

Cybrary. (2020, 5 26). *https://www.cybrary.it/*. Retrieved from https://www.cybrary.it/: https://www.cybrary.it/

Danish Technological Institute and Fraunhofer. (2012). *Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements.* Thessaloniki: EUROPEAN COMISSION.

ECSO. (2020). *WG5 ANALYSIS Information and Cyber Security Professional Certification Task Force (EHR4CYBER.* ECSO.

European Comission . (2020`, 5 25). *European Skills, Competences, Qualifications and Occupations*. Retrieved from European Skills, Competences, Qualifications and Occupations: https://ec.europa.eu/esco/portal/howtouse/21da6a9a-02d1-4533-8057-dea0a824a17a

Forbes. (2019, 8 28). *Top 10 Most Popular Cybersecurity Certifications In 2019*. Retrieved from Forbes: https://www.forbes.com/sites/louiscolumbus/2019/08/28/top-10-most-popular-cybersecurity-certifications-in-2019/#53d30985360e

Frost & Sullivan. (2017). *Global Information on Cyber Security Workforce Study of 2017.* New York: Frost & Sullivan.

International Organization for Standardization. (2012). *ISO 17024:2012. Conformity assessment — General Requirements for bodies operating certificaton of persons.* Geneva: International Organization for Standardization.

ISACA. (2020, 1 1). *State of Cybersecurity 2020.* Retrieved from ISACA: https://www.isaca.org/go/state-of-cybersecurity-2020

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework).* NIST.

NIST. (2018). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Protiviti. (2019, 1 1). *protiviti-survey-top-risks-2019 & 2020.* Retrieved from https://www.protiviti.com/: https://www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-top-risks-2019-executive-summary.pdf

World Economic Forum. (2019). *The Global Risks Report 2019 - 14th Edition.* Retrieved from World Economic Forum: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Appendices

A European e-Competence Framework 3.0 overview

Dimension 1 5 e-CF areas (A – E)	Dimension 2 40 e-Competences identified	Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment				■	■
	A.2. Service Level Management			■	■	
	A.3. Business Plan Development			■	■	■
	A.4. Product/Service Planning		■	■	■	
	A.5. Architecture Design			■	■	■
	A.6. Application Design	■	■	■		
	A.7. Technology Trend Monitoring				■	■
	A.8. Sustainable Development			■	■	
	A.9. Innovating				■	■
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■	■	
	B.4. Solution Deployment	■	■	■		
	B.5. Documentation Production	■	■	■		
	B.6. Systems Engineering			■	■	
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
	C.4. Problem Management		■	■	■	
D. ENABLE	D.1. Information Security Strategy Development				■	■
	D.2. ICT Quality Strategy Development				■	■
	D.3. Education and Training Provision		■	■		
	D.4. Purchasing		■	■	■	
	D.5. Sales Proposal Development		■	■		
	D.6. Channel Management			■	■	
	D.7. Sales Management			■	■	■
	D.8. Contract Management		■	■	■	
	D.9. Personnel Development		■	■	■	
	D.10. Information and Knowledge Management			■	■	■
	D.11. Needs Identification			■	■	■
	D.12. Digital Marketing		■	■	■	
E. MANAGE	E.1. Forecast Development			■	■	
	E.2. Project and Portfolio Management		■	■	■	■
	E.3. Risk Management		■	■	■	
	E.4. Relationship Management			■	■	
	E.5. Process Improvement			■	■	
	E.6. ICT Quality Management		■	■	■	
	E.7. Business Change Management			■	■	■
	E.8. Information Security Management		■	■	■	
	E.9. IS Governance				■	■

(CEN, 2014)

B European e-CF and EQF level table

EQF levels	EQF Levels descriptions	e-CF Levels	e-CF Levels descriptions	Typical Tasks	Complexity	Autonomy	Behaviour
8	Knowledge at the most advanced frontier, the most advanced and specialised skills and techniques to solve critical problems in research and/or innovation, demonstrating substantial authority, innovation, autonomy, scholarly or professional integrity.	e-5	**Principal** Overall accountability and responsibility; recognised inside and outside the organisation for innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge.	IS strategy or programme management	Unpredictable – unstructured	Demonstrates substantial leadership and independence in contexts which are novel requiring the solving of issues that involve many interacting factors.	Conceiving, transforming, innovating, finding creative solutions by application of a wide range of technical and/or management principles.
7	Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking, critical awareness of knowledge issues in a field and at the interface between different fields, specialised problem-solving skills in research and/or innovation to develop new knowledge and procedures and to integrate knowledge from different fields, managing and transforming work or study contexts that are complex, unpredictable and require new strategic approaches, taking responsibility for contributing to professional knowledge and practice and/or for reviewing the strategic performance of teams.	e-4	**Lead Professional / Senior Manager** Extensive scope of responsibilities deploying specialised integration capability in complex environments; full responsibility for strategic development of staff working in unfamiliar and unpredictable situations.	IS strategy/ holistic solutions		Demonstrates leadership and innovation in unfamiliar, complex and unpredictable environments. Addresses issues involving many interacting factors.	
6	Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles, advanced skills, demonstrating mastery and innovation in solving complex and unpredictable problems in a specialised field of work or study, management of complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts, for continuing personal and group professional development.	e-3	**Senior Professional / Manager** Respected for innovative methods and use of initiative in specific technical or business areas; providing leadership and taking responsibility for team performances and development in unpredictable environments.	Consulting	Structured – unpredictable	Works independently to resolve interactive problems and addresses complex issues. Has a positive effect on team performance.	Planning, making decisions, supervising, building teams, forming people, reviewing performances, finding creative solutions by application of specific technical or business knowledge/skills.
5	Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge, expertise in a comprehensive range of cognitive and practical skills in developing creative solutions to abstract problems, management and supervision in contexts where there is unpredictable change, reviewing and developing performance of self and others.	e-2	**Professional** Operates with capability and independence in specified boundaries and may supervise others in this environment; conceptual and abstract model building using creative thinking; uses theoretical knowledge and practical skills to solve complex problems within a predictable and sometimes unpredictable context.	Concepts/ Basic principles		Works under general guidance in an environment where unpredictable change occurs. Independently resolves interactive issues which arise from project activities.	Designing, managing, surveying, monitoring, evaluating, improving, finding non standard solutions. Scheduling, organising, integrating, finding standard solutions, interacting, communicating, working in team.
4	Factual and theoretical knowledge in broad contexts within a field of work or study, expertise in a range of cognitive and practical skills in generating solutions to specific problems in a field of work or study, self-manageme nt within the guidelines of work or study contexts that are usually predictable, but are subject to change, supervising the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities.				Structured – predictable		
3	Knowledge of facts, principles, processes and general concepts, in a field of work or study, a range of cognitive and practical skills in accomplishing tasks. Problem solving with basic methods, tools, materials and information, responsibility for completion of tasks in work or study, adapting own behaviour to circumstances in solving problems.	e-1	**Associate** Able to apply knowledge and skills to solve straight forward problems; responsible for own actions; operating in a stable environment.	Support/ Service		Demonstrates limited independence where contexts are generally stable with few variable factors.	Applying, adapting, developing, deploying, maintaining, repairing, finding basic-simple solutions.

(CEN, 2014)

C The Professional Role Profile of the Information Security Manager

Profile title	INFORMATION SECURITY MANAGER ROLE (11)		
Summary statement	Leads and manages the organisation information security policy.		
Mission	Defines the information security strategy and manages implementation across the organisation. Embeds proactive information security protection by assessing, informing, alerting and educating the entire organisation.		
Deliverables	**Accountable**	**Responsible**	**Contributor**
	• Information Security Policy	• Knowledge or Information Base • Information Security Strategy	• Risk Management Policy • New Solution and Critical Business Integration Proposal
Main task/s	• Define the information security strategy and standards • Contribute to the development of the organisation's security policy • Manages security audits • Evaluate risks, threats and consequences • Establish and manage prevention, detection, correction and remediation plans • Inform and raise awareness among general management and across all IT users and professionals • Conduct information security operations		
e-Competences *(from e-CF)*	A.7. Technology Trend Monitoring		Level 4
	D.1. Information Security Strategy Development		Level 5
	E.3. Risk Management		Level 4
	E.8. Information Security Management		Level 4
	E.9. IS Governance		Level 5
KPI area	Security policy effectiveness		

(CEN, 2018)

D ESCO's Occupation: Chief ICT security officer

Code

2529.1

Description

Chief ICT security officers protect company and employee information against unauthorized access. They also define the Information System security policy, manage security deployment across all Information Systems and ensure the provision of information availability.

Scope notes

Includes people performing corporate security functions.

Alternative label

Head of IT security
chief information security officer
chief ICT security officers
head IT security officer
CISO

Regulatory aspect

To see if and how this occupation is regulated in EU Member States, EEA countries or Switzerland please consult the Regulated Professions Database of the Commission. Regulated Professions Database: http://ec.europa.eu/growth/single-market/services/free-movement-professionals/qualifications-recognition_en

Hierarchy

2 - Professionals
25 - Information and communications technology professionals
252 - Database and network professionals
2529 - Database and network professionals not elsewhere classified
chief ICT security officer

Essential skills and competences

- ensure adherence to organisational ICT standards
- ensure compliance with legal requirements
- ensure information privacy
- implement ICT risk management
- implement corporate governance
- lead disaster recovery exercises
- maintain plan for continuity of operations
- manage IT security compliances
- manage disaster recovery plans
- monitor technology trends
- utilise decision support system

Essential Knowledge

- ICT network security risks
- ICT security legislation
- ICT security standards
- audit techniques
- cyber security
- decision support systems
- information security strategy
- organisational resilience

Optional skills and competences

- coordinate technological activities
- create solutions to problems
- manage staff
- optimise choice of ICT solution
- train employees
- use different communication channels

Optional Knowledge

- ABAP
- AJAX
- APL
- ASP.NET
- Assembly (computer programming)
- C#
- C++
- COBOL
- CoffeeScript
- Common Lisp
- Erlang
- Groovy
- Haskell
- ICT encryption
- ICT process quality models
- ICT recovery techniques
- ICT system user requirements
- Internet of Things
- Java (computer programming)
- JavaScript
- Lisp
- MATLAB
- ML (computer programming)
- Microsoft Visual C++
- Objective-C
- OpenEdge Advanced Business Language
- PHP
- Pascal (computer programming)
- Perl
- Prolog (computer programming)
- Python (computer programming)
- R
- Ruby (computer programming)
- SAP R3
- SAS language
- Scala
- Scratch (computer programming)
- Smalltalk (computer programming)
- Swift (computer programming)
- TypeScript
- VBScript
- Visual Studio .NET
- World Wide Web Consortium standards

- computer forensics
- computer programming
- cyber attack counter-measures
- internet governance
- software anomalies
- tools for ICT test automation
- web application security threats

Status

released

Concept URI

http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28

(European Comission , 2020`)

E NICE framework: Information Systems Security Manager

Work Role Name	Information Systems Security Manager
Work Role ID	OV-MGT-001
Specialty Area	Cybersecurity Management (MGT)
Category	Oversee and Govern (OV)
Work Role Description	Responsible for the cybersecurity of a program, organization, system, or enclave.
Tasks	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
Skills	S0018, S0027, S0086
Abilities	A0128, A0161, A0170

Speciality Area: Cybersecurity Management (MGT)

NICE Specialty Area Definition: Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
Work Role: Information Systems Security Manager
Work Role Definition: Responsible for the cybersecurity of a program, organization, system, or enclave.
Work Role ID: OV-TEA-001

KSA ID	KSA
Knowledge	
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K0124	Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain.
K0146	Knowledge of the organization's core business/mission processes.
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.

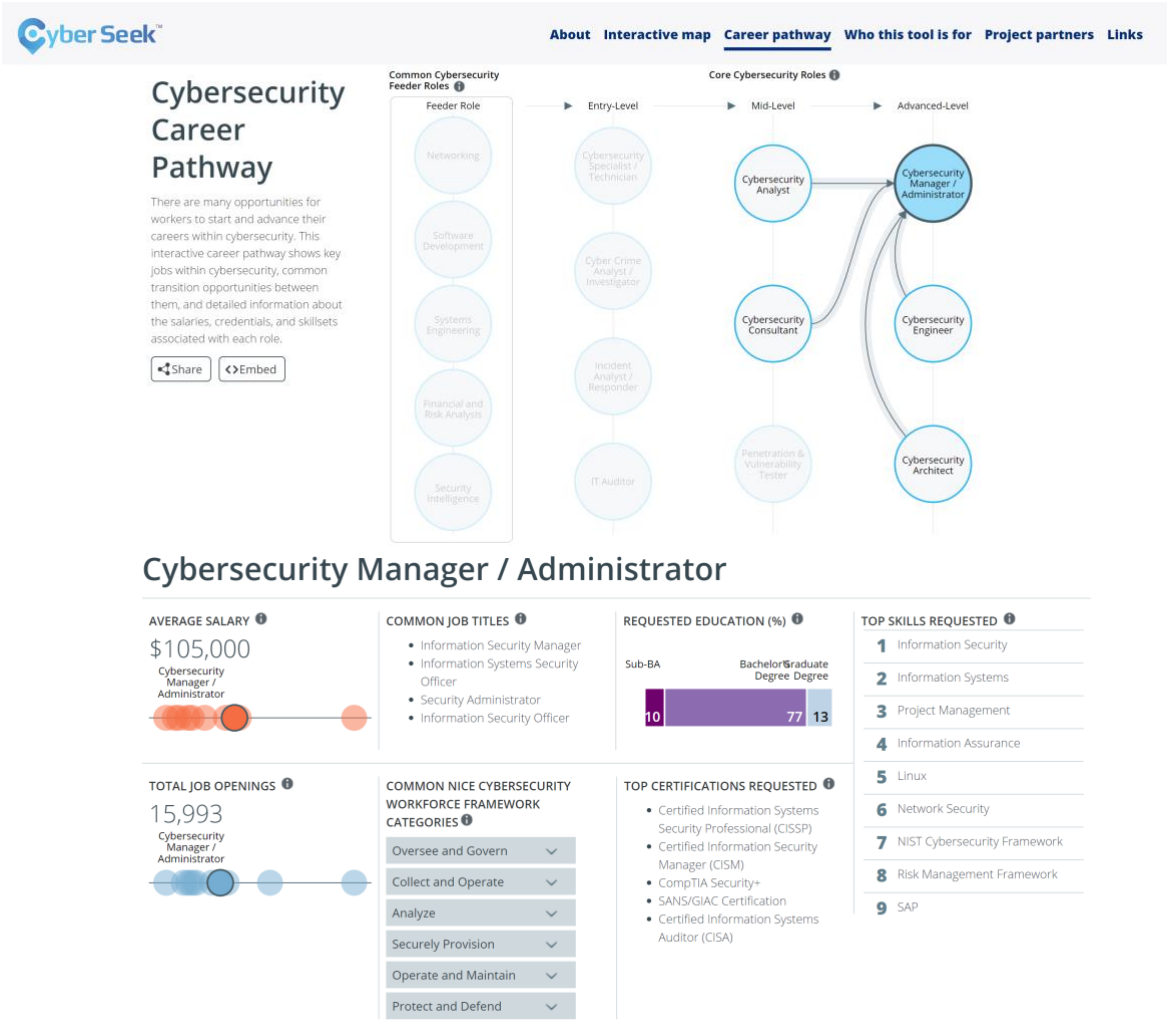
K0204	Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).
K0208	Knowledge of computer based training and e-learning services.
K0213	Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).
K0216	Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).
K0217	Knowledge of Learning Management Systems and their use in managing learning.
K0220	Knowledge of modes of learning (e.g., rote learning, observation).
K0243	Knowledge of organizational training and education policies, processes, and procedures.
K0239	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.
K0245	Knowledge of principles and processes for conducting training and education needs assessment.
K0246	Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
K0250	Knowledge of Test & Evaluation processes for learners.
K0252	Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.
K0287	Knowledge of an organization's information classification program and procedures for information compromise.
K0628	Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
Skills	
S0064	Skill in developing and executing technical training programs and curricula.
S0066	Skill in identifying gaps in technical capabilities.
S0070	Skill in talking to others to convey information effectively.
S0102	Skill in applying technical delivery capabilities.
S0166	Skill in identifying gaps in technical delivery capabilities.
S0296	Skill in utilizing feedback to improve processes, products, and services.
Abilities	
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A0018	Ability to prepare and present briefings.
A0019	Ability to produce technical documentation.
A0022	Ability to apply principles of adult learning.
A0024	Ability to develop clear directions and instructional materials.
A0032	Ability to develop curriculum for use within a virtual environment.
A0054	Ability to apply the Instructional System Design (ISD) methodology.

A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
A0055	Ability to operate common network tools (e.g., ping, traceroute, nslookup).
A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
A0058	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
A0063	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
A0070	Ability to apply critical reading/thinking skills.
A0083	Ability to evaluate information for reliability, validity, and relevance.
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.
A0105	Ability to tailor technical and planning information to a customer's level of understanding.
A0106	Ability to think critically.
A0112	Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
A0114	Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.
A0171	Ability to conduct training and education needs assessment.

Task ID	Task
T0230	Support the design and execution of exercise scenarios.
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
T0249	Research current technology to understand capabilities of required system or network.
T0345	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.
T0352	Conduct learning needs assessments and identify requirements.
T0357	Create interactive learning exercises to create an effective learning environment.
T0365	Develop or assist in the development of training policies and protocols for cyber training.
T0367	Develop the goals and objectives for cyber curriculum.
T0380	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.
T0437	Correlate training and learning to business or mission requirements.
T0442	Create training courses tailored to the audience and physical environment.
T0450	Design training curriculum and course content based on requirements.

T0451	Participate in development of training curriculum and course content.
T0534	Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).
T0926	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.

F Cyberseek: Cybersecurity Manager / Administrator



(Comptia and Burning Glass Technologies, 2020)

G Information on existing Cybersecurity Skills Certification Schemes

CERTIFIED INFORMATION SECURITY MANAGER – CISM[2]

CISM certification promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security.
CISM employees:

- Identify critical issues and customize company-specific practices to support the governance of information and related technologies
- Bring credibility to the enterprise for which they are employed
- Take a comprehensive view of information systems security management and their relationship to organizational success
- Demonstrate to enterprise customers their commitment to compliance, security and integrity; ultimately contributing to the attraction and retention of customers
- Ensure that there is improved alignment between the organization's information security program and its broader goals and objectives
- Provide the enterprise with a certification for Information security management that is recognized by multinational clients and enterprises, lending credibility to the enterprise

The domains of knowledge and abilities that the CISM certification aims to validate are the following:

Domain 1— Information Security Governance

Affirms the expertise to establish and/or maintain an information security governance framework (and supporting processes) to ensure that the information security strategy is aligned with organizational goals and objectives.
Domain 1 confirms your ability to develop and oversee an information security governance framework to guide activities that support the information security strategy.

Knowledge gained from Domain 1

- Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research)
- Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices
- Knowledge of available information security governance frameworks
- Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development
- Knowledge of the fundamental concepts of governance and how they relate to information security
- Knowledge of methods to assess, plan, design and implement an information security governance framework

2 http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

- Knowledge of methods to integrate information security governance into corporate governance
- Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development
- Knowledge of content in, and techniques to develop, business cases
- Knowledge of strategic budgetary planning and reporting methods
- Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy
- Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)
- Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security)
- Knowledge of roles and responsibilities of the information security manager
- Knowledge of organizational structures, lines of authority and escalation points
- Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users)
- Knowledge of processes to monitor performance of information security responsibilities
- Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
- Knowledge of methods to select, implement and interpret key information security metrics (e.g., key performance indicators [KPIs] or key risk indicators [KRIs])

Domain 2— Information Risk Management

Advanced ability to manage information risk to an acceptable level, in accordance with organizational risk appetite, while facilitating the attainment of organizational goals and objectives.
Domain 2 demonstrates expertise in classifying information assets to ensure measures taken to protect those assets are proportional to their business value.

Knowledge gained from Domain 2

- Knowledge of methods to establish an information asset classification model consistent with business objectives
- Knowledge of considerations for assigning ownership of information assets and risk
- Knowledge of methods to identify and evaluate the impact of internal or external events on information assets and the business
- Knowledge of methods used to monitor internal or external risk factors
- Knowledge of information asset valuation methodologies
- Knowledge of legal, regulatory, organizational and other requirements related to information security
- Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities

- Knowledge of events that may require risk reassessments and changes to information security program elements
- Knowledge of information threats, vulnerabilities and exposures and their evolving nature
- Knowledge of risk assessment and analysis methodologies
- Knowledge of methods used to prioritize risk scenarios and risk treatment/response options
- Knowledge of risk reporting requirements (e.g., frequency, audience, content)
- Knowledge of risk treatment/response options (avoid, mitigate, accept or transfer) and methods to apply them
- Knowledge of control baselines and standards and their relationships to risk assessments
- Knowledge of information security controls and the methods to analyze their effectiveness
- Knowledge of gap analysis techniques as related to information security
- Knowledge of techniques for integrating information security risk management into business and IT processes
- Knowledge of compliance reporting requirements and processes
- Knowledge of cost/benefit analysis to assess risk treatment options

Domain 3 — Information Security Program Development and Management

Establishes the ability to develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning with business goals.
Domain 3 attests to ability to ensure the information security program adds value while supporting operational objectives of other business functions (human resources, accounting, procurement, IT, etc.)

Knowledge gained from Domain 3

- Knowledge of methods to align information security program requirements with those of other business functions
- Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources
- Knowledge of current and emerging information security technologies and underlying concepts
- Knowledge of methods to design and implement information security controls
- Knowledge of information security processes and resources (including people and technologies) in alignment with the organization's business goals and methods to apply them
- Knowledge of methods to develop information security standards, procedures and guidelines
- Knowledge of internationally recognized regulations, standards, frameworks and best practices related to information security program development and management
- Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines
- Knowledge of training, certifications and skill set development for information security personnel

- Knowledge of methods to establish and maintain effective information security awareness and training programs
- Knowledge of methods to integrate information security requirements into organizational processes (e.g., access management, change management, audit processes)
- Knowledge of methods to incorporate information security requirements into contracts, agreements and third-party management processes
- Knowledge of methods to monitor and review contracts and agreements with third parties and associated change processes as required
- Knowledge of methods to design, implement and report operational information security metrics
- Knowledge of methods for testing the effectiveness and efficiency of information security controls
- Knowledge of techniques to communicate information security program status to key stakeholders

Domain 4 — Information Security Incident Management

Validates capacity to plan, establish and manage detection, investigation, response and recovery from information security incidents in order to minimize business impact.
Domain 4 establishes your skills in accurately classifying and categorizing information security incidents and developing plans to ensure timely and effective response.

Knowledge gained from Domain 4

- Knowledge of incident management concepts and practices
- Knowledge of the components of an incident response plan
- Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan
- Knowledge of incident classification/categorization methods
- Knowledge of incident containment methods to minimize adverse operational impact
- Knowledge of notification and escalation processes
- Knowledge of the roles and responsibilities in identifying and managing information security incidents
- Knowledge of the types and sources of training, tools and equipment required to adequately equip incident response teams
- Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)
- Knowledge of internal and external incident reporting requirements and procedures
- Knowledge of post incident review practices and investigative methods to identify root causes and determine corrective actions
- Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents
- Knowledge of technologies and processes to detect, log, analyse and document information security events
- Knowledge of internal and external resources available to investigate information security incidents

- Knowledge of methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process
- Knowledge of techniques to test the incident response plan
- Knowledge of applicable regulatory, legal and organization requirements
- Knowledge of key indicators/metrics to evaluate the effectiveness of the incident response plan

CERTIFIED INFORMATION SYSTEMS AUDITOR – CISA[3]

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.
CISA employees:

- Are highly qualified, experienced professionals
- Provide the enterprise with a certification for IT assurance that is recognized by multinational clients, lending credibility to the enterprise
- Are excellent indicators of proficiency in technology controls
- Demonstrate competence in five domains, including standards and practices; organization and management; processes; integrity, confidentiality and availability; and software development, acquisition and maintenance
- Demonstrate a commitment to providing the enterprise with trust in and value from your information systems
- Maintain ongoing professional development for successful on-the-job performance

The domains of knowledge and abilities that the CISA certification aims to validate are the following:

Domain 1—Information Systems Auditing Process

A. Planning
- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments

B. Execution
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques

Domain 2— Governance and Management of IT

A. IT Governance
- IT Governance and IT Strategy
- IT-Related Frameworks

[3] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization

B. IT Management

- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

Domain 3—Information Systems Acquisition, Development, and Implementation

A. Information Systems Acquisition and Development

- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design

B. Information Systems Implementation

- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review

Domain 4—Information Systems Operations and Business Resilience

A. Information Systems Operations

- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management

B. Business Resilience

- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)

Domain 5—Protection of Information Assets

A. Information Asset Security and Control

- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management

- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices

B. Security Event Management

- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

CERTIFIED ETHICAL HACKER – CEHV10[4]

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

The domains of knowledge and abilities that the CEHv10 certification aims to validate are the following:

Knowledge gained

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of foot-printing, foot-printing tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.

4 https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various cloud computing concepts, threats, attacks, and security techniques and tools.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely.

COMPTIA CYBERSECURITY ANALYST (CYSA+)[5]

CySA+ is an intermediate high-stakes cybersecurity analyst certification with performance-based questions covering security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing centre in a highly secure environment. The behavioral analytics skills covered by CySA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface. CompTIA CySA+ is for IT professionals looking to gain the following security analyst skills:

- Perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization.
- Configure and use threat-detection tools.
- Secure and protect applications and systems within an organization

The domains of knowledge and abilities that the CySA+ certification aims to validate are the following:

- THREAT MANAGEMENT: Apply environmental reconnaissance techniques using appropriate tools, analysing results, and implementing recommended response
- VULNERABILITY MANAGEMENT: Implement vulnerability management process and analyse results of the scan
- SECURITY ARCHITECTURE & TOOL SETS: Use data to recommend remediation of security issues related to identity and access management and recommend implementation strategy while participating in the Software Development Life Cycle (SDLC)
- CYBER-INCIDENT RESPONSE: Distinguish threat data to determine incident impact and prepare a toolkit with appropriate forensics tools, communication strategy, and best practices as a response

And

- Identify tools and techniques to use to perform an environmental reconnaissance of a target network or security system.
- Collect, analyze, and interpret security data from multiple log and monitoring sources.

5 https://www.comptia.org/certifications/cybersecurity-analyst

- Use network host and web application vulnerability assessment tools and interpret the results to provide effective mitigation.
- Understand and remediate identity management, authentication, and access control issues.
- Participate in a senior role within an incident response team and use forensic tools to identify the source of an attack.
- Understand the use of frameworks, policies, and procedures and report on security architecture with recommendations for effective compensating controls.

CompTIA Advanced Security Practitioner (CASP+)[6]

CASP+ is a hands-on, performance-based certification for practitioners — not managers — at the advanced skill level of cybersecurity. While cybersecurity managers help identify what cybersecurity policies and frameworks could be implemented, CASP+ certified professionals figure out how to implement solutions within those policies and frameworks. The CASP+ certification validates advanced-level competency in risk management, enterprise security operations and architecture, research and collaboration, and integration of enterprise security.

The domains of knowledge and abilities that the CASP+certification aims to validate are the following:

- RISK MANAGEMENT: Analyse security risks and frameworks that come along with specific industry threats and organizational requirements and execute risk mitigation strategies.
- TECHNICAL INTEGRATION OF ENTERPRISE SECURITY: Integrate hosts, storage, networks and applications into a secure enterprise architecture using on-premise, cloud, and virtualization technologies.
- ENTERPRISE SECURITY ARCHITECTURE: Integrate network and security components and implement security controls for host, mobile and small form factor devices.
- RESEARCH, DEVELOPMENT & COLLABORATION: Apply research methods to determine industry trends and their impact to the enterprise.
- ENTERPRISE SECURITY OPERATIONS: Implement incident response and recovery procedures and conduct security assessments using appropriate tools.

And

- Support IT governance in the enterprise with an emphasis on managing risk
- Leverage collaboration tools and technology to support enterprise security
- Use research and analysis to secure the enterprise
- Integrate advanced authentication and authorization techniques
- Implement cryptographic techniques, security controls for hosts, security controls for mobile devices, implement network security, and security in the systems and software development lifecycle.
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture

6 https://www.comptia.org/certifications/comptia-advanced-security-practitioner

- Conduct security assessments
- Respond to and recover from security incidents.

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL – OSCP [7]

This certification scheme introduces penetration testing tools and techniques via hands-on experience. The exam consists of a hands-on penetration test that takes place in our isolated VPN exam network. A passing exam grade declares the candidate as an Offensive Security Certified Professional (OSCP). The OSCP designation is well known, highly respected, and a certification requirement for many of the industry's top positions. The OSCP exam is a 24 hour lab based exam which tests technical skills as well as time management skills. The camdidate is expected to exploit a number of machines and obtain proof files from the targets in order to gain points.

The domains of knowledge and abilities that the OSCP ertification aims to validate are the following:

- Using information gathering techniques to identify and enumerate targets running various operating systems and services
- Writing basic scripts and tools to aid in the penetration testing process
- Analysing, correcting, modifying, cross-compiling, and porting public exploit code
- Conducting both remote and client-side attacks
- Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications
- Deploying tunneling techniques to bypass firewalls
- Creative problem solving and lateral thinking skills

CERTIFIED CLOUD SECURITY PROFESSIONAL – CCSP[8]

The CCSP is ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration, including those in the following positions:

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body

7 https://www.offensive-security.com/pwk-oscp/
8 https://www.isc2.org/Certifications/CCSP

of knowledge. The CCSP is a standalone credential that complements and builds upon existing credentials and educational programs, including (ISC)²'s Certified Information Systems Security Professional (CISSP) and CSA's Certificate of Cloud Security Knowledge (CCSK). The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security.

Successful candidates are competent in the following 6 domains:

Domain 1: Cloud Concepts, Architecture and Design

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Evaluate Cloud Service Providers

Domain 2: Cloud Data Security

- Describe Cloud Data Concepts
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Technologies and Strategies
- Implement Data Discovery
- Implement Data Classification
- Design and Implement Information Rights Management (IRM)
- Plan and Implement Data Retention, Deletion and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

Domain 3: Cloud Platform and Infrastructure Security

- Comprehend Cloud Infrastructure Components
- Design a Secure Data Centre
- Analyse Risks Associated with Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery (DR) and Business Continuity (BC)

Domain 4: Cloud Application Security

- Advocate Training and Awareness for Application Security
- Describe the Secure Software Development Life Cycle (SDLC) Process
- Apply the Secure Software Development Life Cycle (SDLC)
- Apply Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

Domain 5: Cloud Security Operations

- Implement and Build Physical and Logical Infrastructure for Cloud Environment
- Operate Physical and Logical Infrastructure for Cloud Environment
- Manage Physical and Logical Infrastructure for Cloud Environment

- Implement Operational Controls and Standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)
- Support Digital Forensics
- Manage Communication with Relevant Parties
- Manage Security Operations

Domain 6: Legal, Risk and Compliance

- Articulate Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues
- Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)[9]

CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.
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 competent in the following 8 domains:

Domain 1: Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements

9 https://www.isc2.org/Certifications/CISSP#

- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modelling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

Domain 2: Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

Domain 3: Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

Domain 4: Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Domain 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

Domain 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyse test output and generate report
- Conduct or facilitate security audits

Domain 7: Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Domain 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

COMPTIA SECURITY+[10]

CompTIA Security+ emphasizes hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of issues. Security+ focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection. The CompTIA Security+ certification covers the Junior IT Auditor/Penetration Tester job role, in addition to the previous job roles for Systems Administrator, Network Administrator, and Security Administrator. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills.

10 https://www.comptia.org/certifications/security

Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

The domains of knowledge and abilities that the COMPTIA Security + certification aims to validate are the following:

- THREATS, ATTACKS & VULNERABILITIES: Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- IDENTITY & ACCESS MANAGEMENT: Install and configure identity and access services, as well as management controls
- TECHNOLOGIES & TOOLS: Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- RISK MANAGEMENT: Implement and summarize risk management best practices and the business impact
- ARCHITECTURE & DESIGN: Implement secure network architecture concepts and systems design
- CRYPTOGRAPHY & PKI: Install and configure wireless security settings and implement public key infrastructure

And

- Identify strategies developed by cyber adversaries to attack networks and hosts and the countermeasures deployed to defend them.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of cryptographic standards and products.
- Install and configure network- and host-based security technologies.
- Describe how wireless and remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery.
- Summarize application and coding vulnerabilities and identify development and deployment methods designed to mitigate them.

CHFI - COMPUTER HACKING FORENSICS INVESTIGATOR[11]

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

The domains of knowledge and abilities that the CHFI certification aims to validate are the following:

11 https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/

- Perform incident response and forensics
- Perform electronic evidence collections
- Perform digital forensic acquisitions
- Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.
- Examine and analyse text, graphics, multimedia, and digital images
- Conduct thorough examinations of computer hard disk drives, and other electronic data storage media
- Recover information and electronic data from computer hard drives and other data storage devices
- Follow strict data and evidence handling procedures
- Maintain audit trail (i.e., chain of custody) and evidence integrity
- Work on technical examination, analysis and reporting of computer-based evidence
- Prepare and maintain case files
- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files
- Gather volatile and non-volatile information from Windows, MAC and Linux
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Perform keyword searches including using target words or phrases
- Investigate events for evidence of insider threats or attacks
- Support the generation of incident reports and other collateral
- Investigate and analyse all response activities related to cyber incidents
- Plan, coordinate and direct recovery activities and incident analysis tasks
- Examine all available information and supporting evidence or artefacts related to an incident or event
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
- Conduct reverse engineering for known and suspected malware files
- Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event
- Identify data, images and/or activity which may be the target of an internal investigation
- Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling
- Search file slack space where PC type technologies are employed
- File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
- Examine file type and file header information
- Review e-mail communications including web mail and Internet Instant Messaging programs
- Examine the Internet browsing history
- Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process
- Recover active, system and hidden files with date/time stamp information
- Crack (or attempt to crack) password protected files
- Perform anti-forensics detection
- Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures
- Play a role of first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and

preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Apply advanced forensic tools and techniques for attack reconstruction
- Perform fundamental forensic activities and form a base for advanced forensics
- Identify and check the possible source/incident origin
- Perform event co-relation
- Extract and analyse logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
- Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
- Assist in the preparation of search and seizure warrants, court orders, and subpoenas
- Provide expert witness testimony in support of forensic examinations conducted by the examiner

ISACA CSX(F)[12]

CSX is designed to help fortify and advance the industry by educating, training and certifying a stronger, more informed workforce—from recent college graduates to C-suite level executives.

The entry point into the cybersecurity program, Cybersecurity Fundamentals offers a certificate in the introductory concepts that frame and define the standards, guidelines and practices of the industry. The certificate and related training are an ideal way to get started on a career in cybersecurity. These skills are in high demand, as threats continue to plague enterprises around the world.

The Cybersecurity Fundamentals Certificate affirms your knowledge of cyber security's key concepts, standards, guidelines and practices and the role of the cyber security professional.

The Cybersecurity Fundamentals exam tests for foundational knowledge across five key areas of cyber security:

- Cyber security concepts
- Cyber security architecture principles
- Cyber security of networks, systems, applications and data
- Incident response
- The security implications of the adoption of emerging technologies

ISACA CSX(P)[13]

12 https://cybersecurity.isaca.org/csx-certifications/csx-fundamentals-certificate
13 https://cybersecurity.isaca.org/csx-certifications/csx-practitioner-certification

The ISACA CSX Cybersecurity Practitioner (CSX-P) certification verifies that successful candidates have the knowledge and skills required to identify assets and remediate vulnerabilities; configure and implement protective technologies; and detect, respond and recover from incidents.
CSX-P candidates are assessed on their ability to perform cybersecurity tasks.
Candidates must complete tasks of varying durations with minimal instruction while navigating between multiple virtual machines and are expected to:

Demonstrate an ability to:

- Use vulnerability assessment processes and scanning tool sets to identify and document vulnerabilities based on defined asset criticality and technical impacts.
- Obtain and aggregate information from multiple sources – for example: logs, event data, network assessments – for use in threat intelligence, metrics incident detection, and response.
- Implement specified cybersecurity controls – for network, application, endpoint, server, and more – and validate that controls are operating as required by defined policy or procedure.
- Implement and document changes to cybersecurity controls – for example: endpoint security and network security – in compliance with change management procedures.
- Identify anomalous activity and potential internal, external, and third-party threats to network resources using network traffic monitors or intrusion detection and prevention systems, as well as ensure timely detection of indicators of compromise.
- Perform initial attack analysis to determine the attack vectors, targets and scope and potential impact.
- Execute defined response plans to contain damage on affected assets.

Be comfortable working with a variety of applications, operating systems, tools, and utilities prior to sitting for the exam. This includes but is not limited to:

- Kali Linux
- Kibana
- Microsoft Windows Server 2016
- Microsoft Windows clients – all beginning with XP
- Microsoft security features
- Nmap/Zenmap
- Network troubleshooting commands
- OpenVAS
- PfSense
- Security Onion
- Squil
- Terminal applications
- Ubuntu
- Wireshark

ISACA CYBERSECURITY AUDIT [14]

14 http://www.isaca.org/info/cybersecurity-audit/index.html

ISACA Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits. It provides security professionals with an understanding of the audit process, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.
By the end of this course, you will be able to:

- Define the roles and responsibilities of a cybersecurity auditor
- Understand security frameworks to identify best practices
- Assess the threats with the help of vulnerability management tools
- Explain all aspects of cybersecurity governance
- Manage enterprise identity and information access
- Recall the definitions of cybersecurity processes and components related to cybersecurity operations
- Define threat and vulnerability management
- Build and deploy secure authorization processes
- Describe the concepts of firewall, wireless and network security technologies in reducing the risk of cyber attack

CESG CERTIFIED PROFESSIONAL (CCP) SCHEME[15]

As part of the Government's investment in cyber security, the IISP consortium has been appointed by CESG to provide certification for UK Government Information Assurance (IA) professionals. The consortium has been awarded a license to issue the CESG Certified Professional (CCP) Mark based on the IISP Skills Framework, as part of a certification scheme driven by CESG, the IA arm of GCHQ. The consortium comprises the Institute of Information Security Professionals (IISP), CREST and Royal Holloway's Information Security Group (RHUL). The IISP certifies competency, CREST provides examination for the more technical roles and RHUL supports with their experience in setting rigorous and consistent assessment processes.
The certification process is designed to increase levels of professionalism in Information Assurance and uses the established IISP Skills Framework to define the competencies, knowledge and skills required for specialist IA roles. Developed through public and private sector collaboration by world-renowned academics and security experts, the Framework has been adopted by GCHQ as the basis for its CESG Certified Professional specification.
This builds on the IISP's existing competency-based membership programmes, so not only will an individual be certified but their areas of specialism will be recognized, offering the individual and their customers' greater confidence that an individual has the right skills and experience for a role.
Applicants can gain certification in one or more of the following roles:

- Accreditor
- IA Auditor
- Communications Security Officer / Crypto Custodian
- Information Security Officer
- Security & Information Risk Advisor
- IA Architect

15 https://www.crest-approved.org/schemes/cesg-certified-professional-scheme-ccp/index.html

All roles have 3 levels of certification: Practitioner, Senior Practitioner and Lead Practitioner.

GIAC CYBERSECURITY CERTIFICATIONS[16]

GIAC Certifications develops and administers premier, professional cybersecurity certifications. More than 30 cyber security certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC Certifications provide the highest and most rigorous assurance of cyber security knowledge and skill available to industry, government, and military clients across the world.
There is a variety of certification schemes divided in the following categories:

- Cyber Defense
- Penetration Testing
- Incident Response and Forensics
- Management, Audit, Legal
- Developer
- Industrial Control Systems
- GSE

The following table depicts the available, GIAC certifications:

16 https://www.giac.org/

Certification	Category	Register
	GSEC: GIAC Security Essentials	Cyber Defense
	GCIH: GIAC Certified Incident Handler	Penetration Testing
	GCFA: GIAC Certified Forensic Analyst	Incident Response and Forensics
	GPEN: GIAC Penetration Tester	Penetration Testing
	GCIA: GIAC Certified Intrusion Analyst	Cyber Defense
	GWAPT: GIAC Web Application Penetration Tester	Penetration Testing
	GCFE: GIAC Certified Forensic Examiner	Incident Response and Forensics
	GSLC: GIAC Security Leadership	Management, Audit, Legal

	GREM: GIAC Reverse Engineering Malware	Incident Response and Forensics
	GISF: GIAC Information Security Fundamentals	Cyber Defense
	GCED: GIAC Certified Enterprise Defender	Cyber Defense
	GICSP: Global Industrial Cyber Security Professional	Industrial Control Systems
	GSNA: GIAC Systems and Network Auditor	Management, Audit, Legal
	GMON: GIAC Continuous Monitoring Certification	Cyber Defense
	GNFA: GIAC Network Forensic Analyst	Incident Response and Forensics
	GCWN: GIAC Certified Windows Security Administrator	Cyber Defense
	GXPN: GIAC Exploit Researcher and Advanced Penetration Tester	Penetration Testing

	GISP: GIAC Information Security Professional	Management, Audit, Legal
	GPPA: GIAC Certified Perimeter Protection Analyst	Cyber Defense
	GCCC: GIAC Critical Controls Certification	Cyber Defense
	GMOB: GIAC Mobile Device Security Analyst	Penetration Testing
	GAWN: GIAC Assessing and Auditing Wireless Networks	Penetration Testing
	GCTI: GIAC Cyber Threat Intelligence	Incident Response and Forensics
	GCUX: GIAC Certified UNIX Security Administrator	Cyber Defense
	GPYC: GIAC Python Coder	Penetration Testing
	GWEB: GIAC Certified Web Application Defender	Developer

	GSTRT: GIAC Strategic Planning, Policy, and Leadership	Management, Audit, Legal
	GSSP-JAVA: GIAC Secure Software Programmer-Java	Developer
	GASF: GIAC Advanced Smartphone Forensics	Incident Response and Forensics
	GLEG: GIAC Law of Data Security & Investigations	Management, Audit, Legal
	GCDA: GIAC Certified Detection Analyst	Cyber Defense
	GRID: GIAC Response and Industrial Defense	Industrial Control Systems
	GDAT: GIAC Defending Advanced Threats	Cyber Defense
	GCPM: GIAC Certified Project Manager	Management, Audit, Legal
	GSSP-.NET: GIAC Secure Software Programmer- .NET	Developer

	GDSA: GIAC Defensible Security Architecture	Cyber Defense
	GSE: GIAC Security Expert	GSE
	GCIP: GIAC Critical Infrastructure Protection	Industrial Control Systems
	GCSA: GIAC Cloud Security Automation	Developer
	GEVA: GIAC Enterprise Vulnerability Assessor	Penetration Testing
	GOSI: GIAC Open Source Intelligence	Cyber Defense
	GBFA: GIAC Battlefield Forensics and Acquisition	Incident Response and Forensics

H Information on existing Cybersecurity Skills Certification Schemes

The tables in the following tables have been simplified to facilitation inclusion in this document.

Each of the Cybersecurity Skills Certification scheme has been replaced by a number according to the following reference table.

Ref. No.	Cybersecurity Skills Certification scheme	Ref. No.	Cybersecurity Skills Certification scheme
1	Cybersecurity Manager	32	EXECUTIVE CYBER LEADERSHIP
2	System Administrator	33	EXPLOITATION ANALYST
3	Network Specialist	34	INFORMATION SYSTEMS SECURITY DEVELOPER
4	Cybersecurity Specialist	35	INFORMATION SYSTEMS SECURITY MANAGER
5	ICT SECURITY ADMINISTRATOR	36	IT INVESTMENT/PORTFOLIO MANAGER
6	ICT SECURITY CONSULTANT	37	IT PROGRAM AUDITOR
7	CHIEF ICT SECURITY OFFICER	38	IT PROJECT MANAGER
8	ICT SECURITY MANAGER	39	KNOWLEDGE MANAGER
9	DIRECTOR OF COMPLIANCE AND INFORMATION SECURITY IN GAMBLING	40	LAW ENFORCEMENT /COUNTERINTELLIGENCE FORENSICS ANALYST
10	ICT SECURITY TECHNICIAN	41	MISSION ASSESSMENT SPECIALIST
11	ALL SOURCE-COLLECTION MANAGER	42	MULTI-DISCIPLINED LANGUAGE ANALYST
12	ALL SOURCE-COLLECTION REQUIREMENTS MANAGER	43	NETWORK OPERATIONS SPECIALIST
13	ALL-SOURCE ANALYST	44	PARTNER INTEGRATION PLANNER
14	AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE	45	PRIVACY OFFICER/PRIVACY COMPLIANCE MANAGER
15	COMMUNICATIONS SECURITY (COMSEC) MANAGER	46	PRODUCT SUPPORT MANAGER
16	CYBER CRIME INVESTIGATOR	47	PROGRAM MANAGER
17	CYBER DEFENSE ANALYST	48	RESEARCH & DEVELOPMENT SPECIALIST
18	CYBER DEFENSE FORENSICS ANALYST	49	SECURE SOFTWARE ASSESSOR
19	CYBER DEFENSE INCIDENT RESPONDER	50	SECURITY ARCHITECT
20	CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST	51	SECURITY CONTROL ASSESSOR
21	CYBER INSTRUCTIONAL CURRICULUM DEVELOPER	52	SOFTWARE DEVELOPER

Ref. No.	Cybersecurity Skills Certification scheme	Ref. No.	Cybersecurity Skills Certification scheme
22	CYBER INSTRUCTOR	53	SYSTEM ADMINISTRATOR
23	CYBER INTEL PLANNER	54	SYSTEM TESTING AND EVALUATION SPECIALIST
24	CYBER LEGAL ADVISOR	55	SYSTEMS DEVELOPER
25	CYBER OPERATOR	56	SYSTEMS REQUIREMENTS PLANNER
26	CYBER OPS PLANNER	57	SYSTEMS SECURITY ANALYST
27	CYBER POLICY AND STRATEGY PLANNER	58	TARGET DEVELOPER
28	CYBER WORKFORCE DEVELOPER AND MANAGER	59	TARGET NETWORK ANALYST
29	DATA ANALYST	60	TECHNICAL SUPPORT SPECIALIST
30	DATABASE ADMINISTRATOR	61	THREAT/WARNING ANALYST
31	ENTERPRISE ARCHITECT	62	VULNERABILITY ASSESSMENT ANALYST

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CERTIFIED INFORMATION SECURITY MANAGER	■						■	■	■					■						
CERTIFIED INFORMATION SYSTEMS AUDITOR														■						
CSX(F)																				
CSX(P)				■						■										
CYBERSECURITY AUDIT																				
CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL									■					■						
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT									■											
CERTIFIED ETHICAL HACKER													■							
COMPUTER HACKING FORENSICS INVESTIGATOR																				
COMPTIA CYBERSECURITY ANALYST													■		■		■	■	■	■
COMPTIA ADVANCED SECURITY PRACTITIONER				■	■				■	■	■				■					
COMPTIA SECURITY+	■			■	■		■	■	■	■										
COMPTIA PENTEST+																				
COMPTIA NETWORK+		■	■	■	■					■										
OFFENSIVE SECURITY CERTIFIED PROFESSIONAL				■	■					■										
OFFENSIVE SECURITY WIRELESS PROFESSIONAL				■						■										
OFFENSIVE SECURITY CERTIFIED EXPERT				■	■					■										
OFFENSIVE SECURITY EXPLOIT EXPERT																				
OFFENSIVE SECURITY WEB EXPERT																				
CERTIFIED CLOUD SECURITY PROFESSIONAL			■																	
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL	■		■	■	■		■	■	■	■	■			■	■		■	■		
SYSTEMS SECURITY CERTIFIED PRACTITIONER	■			■	■		■	■	■	■										
CERTIFIED AUTHORIZATION PROFESSIONAL																				
CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL																				
HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER																				
EITCA/IS																				
CESG CERTIFIED PROFESSIONAL (CCP) SCHEME				■						■										

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
GIAC CYBERSECURITY CERTIFICATIONS																				
GIAC SECURITY LEADERSHIP	■						■	■	■											
GIAC SYSTEMS AND NETWORK AUDITOR																				
GIAC INFORMATION SECURITY PROFESSIONAL	■			■	■		■	■	■	■										
GIAC STRATEGIC PLANNING, POLICY, AND LEADERSHIP	■						■	■	■											
GIAC CERTIFIED INTRUSION ANALYST																				
GIAC CERTIFIED INCIDENT HANDLER																				
OSSTMM PROFESSIONAL SECURITY TESTER																				
OSSTMM PROFESSIONAL SECURITY ANALYST																				
OSSTMM PROFESSIONAL SECURITY EXPERT				■	■					■										
OSSTMM WIRELESS SECURITY EXPERT	■							■		■										
OSSTMM CERTIFIED TRUST ANALYST																				
CERTIFIED SECURITY AWARENESS INSTRUCTOR																				
ISO/IEC 27001 LEAD AUDITOR																				
ISO/IEC 27001 IMPLEMENTOR							■													
ISO/IEC 27005 RISK MANAGER							■													
KCEH / MEH (EQUIVALENT TO CEH IN HUNGARIAN)																				
CISCO CERTIFIED NETWORK ASSOCIATE		■	■		■					■					■					
CISCO CERTIFIED NETWORK PROFESSIONAL				■	■					■										
CISCO CERTIFIED INTERNETWORK EXPERT					■					■										
IT INFRASTRUCTURE LIBRARY (ITIL) CERTIFICATION		■	■												■				■	■
PROJECT MANAGEMENT PROFESSIONAL														■						
CERTIFIED PUBLIC ACCOUNTANT																				
CERTIFIED INTERNAL AUDITOR																				
ENCASE CERTIFIED EXAMINER																				

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
CERTIFIED INFORMATION SECURITY MANAGER																				
CERTIFIED INFORMATION SYSTEMS AUDITOR																				
CSX(F)																				
CSX(P)																				
CYBERSECURITY AUDIT																				
CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL																				
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT																				
CERTIFIED ETHICAL HACKER																				
COMPUTER HACKING FORENSICS INVESTIGATOR																				
COMPTIA CYBERSECURITY ANALYST																				
COMPTIA ADVANCED SECURITY PRACTITIONER																				
COMPTIA SECURITY+																				
COMPTIA PENTEST+																				
COMPTIA NETWORK+																				
OFFENSIVE SECURITY CERTIFIED PROFESSIONAL																				
OFFENSIVE SECURITY WIRELESS PROFESSIONAL																				
OFFENSIVE SECURITY CERTIFIED EXPERT																				
OFFENSIVE SECURITY EXPLOIT EXPERT																				
OFFENSIVE SECURITY WEB EXPERT																				
CERTIFIED CLOUD SECURITY PROFESSIONAL																				
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL																				
SYSTEMS SECURITY CERTIFIED PRACTITIONER																				
CERTIFIED AUTHORIZATION PROFESSIONAL																				
CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL																				

HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER																					
EITCA/IS																					
CESG CERTIFIED PROFESSIONAL (CCP) SCHEME																					
GIAC CYBERSECURITY CERTIFICATIONS																					
GIAC SECURITY LEADERSHIP																					
GIAC SYSTEMS AND NETWORK AUDITOR																					
GIAC INFORMATION SECURITY PROFESSIONAL																					
GIAC STRATEGIC PLANNING, POLICY, AND LEADERSHIP																					
GIAC CERTIFIED INTRUSION ANALYST																					
GIAC CERTIFIED INCIDENT HANDLER																					
OSSTMM PROFESSIONAL SECURITY TESTER																					
OSSTMM PROFESSIONAL SECURITY ANALYST																					
OSSTMM PROFESSIONAL SECURITY EXPERT																					
OSSTMM WIRELESS SECURITY EXPERT																					
OSSTMM CERTIFIED TRUST ANALYST																					
CERTIFIED SECURITY AWARENESS INSTRUCTOR																					
ISO/IEC 27001 LEAD AUDITOR																					
ISO/IEC 27001 IMPLEMENTOR																					
ISO/IEC 27005 RISK MANAGER																					
KCEH / MEH (EQUIVALENT TO CEH IN HUNGARIAN)																					
CISCO CERTIFIED NETWORK ASSOCIATE																					
CISCO CERTIFIED NETWORK PROFESSIONAL																					
CISCO CERTIFIED INTERNETWORK EXPERT																					
IT INFRASTRUCTURE LIBRARY (ITIL) CERTIFICATION																					
PROJECT MANAGEMENT PROFESSIONAL																					
CERTIFIED PUBLIC ACCOUNTANT																					
CERTIFIED INTERNAL AUDITOR																					
ENCASE CERTIFIED EXAMINER																					

	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
CERTIFIED INFORMATION SECURITY MANAGER											■											
CERTIFIED INFORMATION SYSTEMS AUDITOR											■											
CSX(F)																						
CSX(P)																						
CYBERSECURITY AUDIT																						
CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL											■			■								
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT																						
CERTIFIED ETHICAL HACKER	■																					■
COMPUTER HACKING FORENSICS INVESTIGATOR																						
COMPTIA CYBERSECURITY ANALYST	■																■					■
COMPTIA ADVANCED SECURITY PRACTITIONER								■			■			■						■		
COMPTIA SECURITY+																						
COMPTIA PENTEST+																						
COMPTIA NETWORK+			■					■	■				■			■						
OFFENSIVE SECURITY CERTIFIED PROFESSIONAL																						
OFFENSIVE SECURITY WIRELESS PROFESSIONAL																						
OFFENSIVE SECURITY CERTIFIED EXPERT																						
OFFENSIVE SECURITY EXPLOIT EXPERT																						
OFFENSIVE SECURITY WEB EXPERT																						
CERTIFIED CLOUD SECURITY PROFESSIONAL			■																			
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL			■		■			■			■											
SYSTEMS SECURITY CERTIFIED PRACTITIONER																						
CERTIFIED AUTHORIZATION PROFESSIONAL																						
CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL									■													

HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER																						
EITCA/IS																						
CESG CERTIFIED PROFESSIONAL (CCP) SCHEME																						
GIAC CYBERSECURITY CERTIFICATIONS																						
GIAC SECURITY LEADERSHIP																						
GIAC SYSTEMS AND NETWORK AUDITOR																						
GIAC INFORMATION SECURITY PROFESSIONAL																						
GIAC STRATEGIC PLANNING, POLICY, AND LEADERSHIP																						
GIAC CERTIFIED INTRUSION ANALYST																						
GIAC CERTIFIED INCIDENT HANDLER																						
OSSTMM PROFESSIONAL SECURITY TESTER																						
OSSTMM PROFESSIONAL SECURITY ANALYST																						
OSSTMM PROFESSIONAL SECURITY EXPERT																						
OSSTMM WIRELESS SECURITY EXPERT																						
OSSTMM CERTIFIED TRUST ANALYST																						
CERTIFIED SECURITY AWARENESS INSTRUCTOR																						
ISO/IEC 27001 LEAD AUDITOR																						
ISO/IEC 27001 IMPLEMENTOR																						
ISO/IEC 27005 RISK MANAGER																						
KCEH / MEH (EQUIVALENT TO CEH IN HUNGARIAN)																						
CISCO CERTIFIED NETWORK ASSOCIATE			■										■							■		
CISCO CERTIFIED NETWORK PROFESSIONAL																						
CISCO CERTIFIED INTERNETWORK EXPERT																						
IT INFRASTRUCTURE LIBRARY (ITIL) CERTIFICATION	■		■				■	■					■	■		■				■		
PROJECT MANAGEMENT PROFESSIONAL							■															
CERTIFIED PUBLIC ACCOUNTANT																						
CERTIFIED INTERNAL AUDITOR																						
ENCASE CERTIFIED EXAMINER																						