Project No. 101083594 Project start: 2022-12-01

Call: DIGITAL-2021-SKILLS-01 Project duration: 36 months

D3.2
CyberSecPro Cybersecurity Certification Schema Proposal

Document Identification	
Due date	2024-03-27
Submission date	2024-05-30
Version	1.0

Related WP	WP3	Dissemination Level	PU – Public
Lead Participant	UPRC	Lead Author	Dimitrios Kallergis , Nineta Polemi (UPRC)
Contributing Participants	UPRC, TUBS, TUC, UNI, APIRO, MAG, PDMFC, FCT	Related Deliverables	D2.1, D2.3, D3.1

Abstract: The CyberSecPro cybersecurity certification schema proposal acknowledges the certification scheme unavailability of professional cybersecurity trainings, as well as the absence of a European Authority for approving both the trainings and the organisations which perform them. On these grounds, the manuscript sheds light on the certification landscape regarding relevant organisations and bodies in international and European level. Then, the standards, the criteria, and the processes regarding professional certifications are thoroughly discussed and assessed. The manuscript concludes with a proposal of three schemes which namely are: *Scheme A: Sector-agnostic scheme for a professional cybersecurity programme*, *Scheme B: Descriptions of the 12 training modules, and Scheme C: Syllabi of the 12 training modules.*

The deliverable reflects the Task 3.3 outcomes.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The CyberSecPro project aims to address the lack of a certification scheme for professional cybersecurity trainings in the European Union and to propose a common solution. Currently, there is a wide variety of cybersecurity trainings available, but they use different approaches and the certificates obtained are not compatible with each other. Additionally, there is no European Authority responsible for approving these trainings.

The situation becomes even more complex when considering sector-specific trainings. As all economic sectors heavily rely on digitalization and emerging technologies like AI, their cybersecurity maturity level is low, necessitating continuous training. However, the sector-specific programs available are fragmented, lack interoperability, and do not provide consistent skills and capabilities required for employees to work in different sectors.

To address these challenges, we propose the implementation of a professional training scheme. This scheme consists of a structured training program or set of modules specifically designed to equip learners with sector-specific cybersecurity knowledge, skills, and competencies. These schemes would need to be recognized and approved by a higher authority.

Upon successful completion of a full program or modules following this scheme, participants would be awarded a certification by the higher authority. This certification serves as a formal recognition of their expertise and abilities in cybersecurity within the specific sector. Such certifications are crucial for individuals seeking to enter or advance their cybersecurity careers, as they demonstrate proficiency and competence according to established standards.

Professional training schemes can vary in length, content, and format, ranging from short courses focused on specific skill sets to comprehensive programs covering a broader range of knowledge areas. These schemes can be offered by various training providers, including academic institutions, professional associations, industry bodies, or private organizations.

The proposed CyberSecPro schemes emphasize a combination of theoretical learning and practical training to ensure participants acquire both knowledge and hands-on experience.

By establishing standardized and recognized certification schemes for professional cybersecurity trainings, we aim to enhance the cybersecurity maturity level across multiple sectors, to promote interoperability, and to enable individuals in demonstrating their expertise to employers and clients. This initiative will contribute to the overall cybersecurity resilience of the European Union.

Document information

Contributors

Name	Beneficiary
Dimitrios Kallergis, George Exarchou, Nineta Polemi	UPRC
Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis	TUC
Iro Chatzopoulou	APIRO
Antonios Ntib	TUBS
George Kliafas, Spiros Borotis	MAG
Vasco Delgado-Gomes, Paulo Figueiras	UNI
Carlos Nuno Marques, Luís Miguel Campos, Nuno Filipe Pedrosa, Stylianos Karagiannis	PDMFC
Jose Fonseca	FCT

Reviewers

Name	Beneficiary
Shareeful Islam	SLC
Kitty Kioskli	trustilio

History

Version	Date	Contributor(s)	Comment(s)
0.1	2023-09-01	Nineta Polemi, Dimitrios Kallergis, George Exarchou	1st Draft of ToC
0.2	2023-09-23	Nineta Polemi, Dimitrios Kallergis, George Exarchou	2nd Draft of ToC

0.3	2023-10-06	Nineta Polemi, Dimitrios Kallergis, George Exarchou	3rd Draft of ToC
0.4	2023-11-03	Dimitrios Kallergis, George Exarchou, Nineta Polemi	Contribution in chapter 2
0.5	2023-12-01	Dimitrios Kallergis, Nineta Polemi	Contribution in chapter 4. Annex A added.
0.6	2023-12-14	Dimitrios Kallergis, Nineta Polemi	Contribution in chapters 4.3.1.x and 4.3.2.x
0.7	2024-02-01	Dimitrios Kallergis, Nineta Polemi, Iro Chatzopoulou, Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis, Jose Fonseca	Contribution in all chapters
0.8	2024-02-08	Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis, Nineta Polemi, Dimitrios Kallergis	Glossary
		Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis	Contribution in 2.4 and 4.2
		Antonios Ntib	Contribution in 4.2
		George Kliafas, Spiros Borotis	Contribution in 2.1.8, 2.1.9, 2.1.10, 2.1.11
0.9	2024-02-15	George Kliafas, Spiros Borotis	Contribution in 2.1.12, 2.1.13, 2.3, and 4.1
		Vasco Delgado-Gomes, Paulo Figueiras, Jose Fonseca	Contribution in 2.2.10 and 3.1
0.91	2024-02-28	Kitty Kioskli, Shareeful Islam, Dimitrios Kallergis, Nineta Polemi	1st review and contribution
0.92	2024-03-14	Shareeful Islam, Kitty Kioskli, Dimitrios Kallergis, Nineta Polemi	2nd review and contribution
0.93	2024-03-25	Dimitrios Kallergis, Nineta Polemi	Review
0.94	2024-04-22	Jeldo Arno Meppen	Review by QM
0.95	2024-05-28	Atiyeh Sadeghi	Final check and layout improvement

1.0	2024-05-30	Atiyeh Sadeghi	Final check, layout refinement and submission process

Table of Contents

Document information v

1 Introduction 1

1.1 Background 1

1.2 Relation to Other Work Packages and Deliverables 1

1.3 Methodology 1

2 Certification Landscape Related to Cybersecurity Training 3

2.1 International Certification Bodies 3

2.1.1 CompTIA 3
2.1.2 (ISC)² 4
2.1.3 The Global Information Assurance Certification (GIAC) 5
2.1.4 The American National Standards Institute (ANSI) 6
2.1.5 UK Cybersecurity Council 6
2.1.6 SANS 7
2.1.7 ISACA 16
2.1.8 CISCO Systems 20
2.1.9 Microsoft 24
2.1.10 ORACLE 28
2.1.11 Professional Evaluation and Certification Board (PECB) 35
2.1.12 SAP University Alliances 40
2.1.13 GITHUB Education 48
2.1.14 EC-Council 48

2.2 EU Certification Bodies 52

2.2.1 ENISA 52
2.2.2 EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION ACADEMY 53
2.2.3 European Cyber Security Organisation (ECSO) 53
2.2.4 European Union Agency for Law Enforcement Training (CEPOL) 53
2.2.5 EUROPOL 55
2.2.6 European Cybercrime Training and Education Group (ECTEG) 57
2.2.7 European Security and Defence College (ESDC) 60
2.2.8 European External Action Service (EEAS) 61
2.2.9 European Association for Quality Assurance in Higher Education (ENQA) 61
2.2.10 European Cybersecurity Competence Centre and Network 62

2.3 Member-States' Certification Bodies 62

2.3.1 Hellenic Authority for Higher Education (HAHE) (Greece) 62
2.3.2 AEQES • Agency for Quality Assurance in Higher Education (Belgium) 62
2.3.3 NEAA National Evaluation and Accreditation Agency (Bulgaria) 63
2.3.4 NAB National Accreditation Bureau for Higher Education (Czech Republic) 64
2.3.5 AI The Danish Accreditation Institution (Denmark) 64
2.3.6 ACQUIN Accreditation, Certification and Quality Assurance Institute (Germany) 65
2.3.7 HAKA Estonian Quality Agency for Education (former EKKA) (Estonia) 65
2.3.8 QQI • Quality and Qualifications Ireland (Ireland) 65
2.3.9 ANECA • National Agency for Quality Assessment and Accreditation of Spain (Spain) 66
2.3.10 CTI • Commission des Titres d'Ingénieur (France) 66
2.3.11 ASHE • Agency for Science and Higher Education (Croatia) 67
2.3.12 ANVUR • National Agency for the Evaluation of Universities and Research Institutes (Italy) . 67
2.3.13 CYQAA • Cyprus Agency of Quality Assurance and Accreditation in Higher Education (Cyprus) 67
2.3.14 AIC • Academic Information Centre (Latvia) 68
2.3.15 SKVC • Centre for Quality Assessment in Higher Education (Lithuania) 68
2.3.16 Comité d'accréditation pour les formations du brevet de technicien supérieur (Luxembourg) .. 68
2.3.17 MAB • Hungarian Accreditation Committee (Hungary) 69
2.3.18 MFHEA • Malta Further and Higher Education Authority (Malta) 69
2.3.19 Inspectorate of Higher Education in the Netherlands (Netherlands) 69
2.3.20 AQ Austria Agency for Quality Assurance and Accreditation Austria (Austria) 69

2.3.21 PKA • Polish Accreditation Committee (Poland) 70
2.3.22 A3ES • Agency for Evaluation and Accreditation of Higher Education (Portugal) 70
2.3.23 ARACIS • Agency for Quality Assurance in Higher Education (Romania) 70
2.3.24 SQAA • Slovenian Quality Assurance Agency for Higher Education (Slovenia) 71
2.3.25 SAAHE • Slovak Accreditation Agency for Higher Education (Slovak Republic) 71
2.3.26 FINEEC • Finnish Education Evaluation Centre (Finland) 72
2.3.27 UKÄ • The Swedish Higher Education Authority (Sweden) 72

2.4 EU Initiatives towards harmonising the EU's Cybersecyrity Training Certification landscape 72
2.4.1 European Cybersecurity Skills Framework (ENISA) 73
2.4.2 Concordia 73
2.4.3 CyberSec4Europe 73
2.4.4 Sparta 74
2.4.5 ECHO 74
2.4.6 Cybersecurity education maturity assessment 74

2.5 EU Challenges in Certifying Cybersecurity Training 75
2.5.1 General Challenges and EU efforts 75

3 Standards, Schemas, Criteria and Scales 77

3.1 Factors & Standards 77

3.2 Criteria & Schemas 79
3.2.1 Criteria for certifying cybersecurity professional trainings / modules 79
3.2.2 Cybersecurity Certification schemes for professional trainings 80

3.3 Scales 80
3.3.1 Credits in professional training modules and programmes 80

4 CyberSecPro Proposed Scheme(s) for cybersecurity hands-on trainings 85

4.1 Principles and Standards to be used 85

4.2 Criteria & Scales 86
4.2.1 Criteria 86
4.2.2 Scales 93

4.3 CyberSecPro Schemes 93
4.3.1 Objectives and requirements 93
4.3.2 CSP Scheme A: Sector-agnostic scheme for a professional cybersecurity training programme 94
4.3.3 CSP Scheme B: Descriptions of the 12 professional training modules 98
4.3.4 Description of Training Module-1: Cybersecurity Essentials and Management in <sector-name> 98
4.3.5 Description of Training Module-2: Human Factors and Cybersecurity in <sector-name> 103
4.3.6 Description of Training Module-3: Cybersecurity Risk Management and Governance in <sector-name> 107
4.3.7 Description of Training Module-4: Network Security in <sector-name> 113
4.3.8 Description of Training Module-5: Data Protection and Privacy Technologies in <sector-name> 119
4.3.9 Description of Training Module-6: Cyber Threat Intelligence in <sector-name> 124
4.3.10 Description of Training Module-7: Cybersecurity in Emerging Technologies in <sector-name> 129
4.3.11 Description of Training Module-8: Critical Infrastructure Security in <sector-name> 134
4.3.12 Description of Training Module-9: Software Security in <sector-name> 138
4.3.13 Description of Training Module-10: Penetration Testing in <sector-name> 141
4.3.14 Description of Training Module-11: Cyber Ranges and Operations in <sector-name> 146
4.3.15 Description of Training Module-12: Digital Forensics in <sector-name> 150
4.3.16 CSP Scheme C: Syllabi of the 12 training modules 154
4.3.17 Syllabus of the Training Module-1: Cybersecurity Essentials and Management for <sector-name> 155
4.3.18 Syllabus of the Training Module-2: Human Factors and Cybersecurity in <sector-name> 162
4.3.19 Syllabus of the Training Module-3: Cybersecurity Risk Management and Governance in <sector-name> 165
4.3.20 Syllabus of the Training Module-4: Network Security in <sector-name> 166

4.3.21 Syllabus of the Training Module-5: Data Protection and Privacy Technologies in <sector-name> 170
4.3.22 Syllabus of the Training Module-6: Cyber Threat Intelligence in <sector-name>.... 171
4.3.23 Syllabus of the Training Module-7: Cybersecurity in Emerging Technologies in <sector-name> 172
4.3.24 Syllabus of the Training Module-8: Critical Infrastructure Security in <sector-name>.... 173
4.3.25 Syllabus of the Training Module-9: Software Security in <sector-name> 174
4.3.26 Syllabus of the Training Module-10: Penetration Testing in <sector-name>.... 177
4.3.27 Syllabus of the Training Module-11: Cyber Ranges and Operations in <sector-name> 178
4.3.28 Syllabus of the Training Module-12: Digital Forensics in <sector-name> 179
Annex A: Glossary and Terms 181

List of Figures

Figure 1. Standards for learning, education, and training 78

Figure 2. Possible options for standards for learning services 79

1 Introduction

In this project, CyberSecPro, we acknowledged the open issue that there is not a certification scheme for professional cybersecurity trainings. As a result, the plethora of cybersecurity professional trainings available use different approaches; the certificates gained are not interoperable. Furthermore, there is not a European Authority responsible for the approval of such trainings.

The situation is even more chaotic when we deal with sector specific professional trainings. All economic sectors (e.g., transport, energy, health) due to the rapid digitalization use all types of ICT and emerging technologies (e.g., AI) their cybersecurity maturity level is low requiring continuous training. The available sector specific professional programs are fragmented, not interoperable and not providing homogeneous skills and capabilities enabling the employees their mobility in different working sectoral environments.

By a " professional training scheme" we mean to a structured training program / set of modules designed to provide learners with specific knowledge, skills, and competencies in cybersecurity for the specific sectoral environments. The schemes need to be recognized/approved by a higher authority (e.g., ECCC)

Upon successful completion of the program/set of modules that follow this scheme, participants are awarded a “certification” provided by a higher authority, which serves as a formal recognition of their acquired expertise and abilities. These certifications are often essential for individuals seeking to enter or advance their cybersecurity career in the specific sectors they work in, as they demonstrate to employers or clients that the holder meets established standards of proficiency and competence in cybersecurity as needed in the specific sector.

Professional training scheme can vary in length, content, and format, ranging from short courses focused on specific skill sets to seminars to workshops to more comprehensive programs covering a broader range of knowledge areas. They can be offered by different training providers e.g., academic institutions, professional associations, industry bodies, or private organizations.

CSP proposed scheme(s) include a combination of theoretical learning and practical training.

1.1 Background

The necessity for specialized industry-driven training has been highlighted in deliverables D2.1 and D2.3, which pointed out the need for further training across 10 Key Areas (KA). Based on this critical analysis, the CSP programme, in D2.3, has proposed the development of 12 modules specifically designed to address these needs, while deliverable D3.1 outlines CSP programme's has focused on training modules and model syllabi, templates, and key elements for these individual modules.

This deliverable aims to address the gap for common industry-driven cybersecurity professional training programmes and to propose training schemes to tackle with this issue.

1.2 Relation to Other Work Packages and Deliverables

This deliverable capitalises the knowledge gained in deliverables D2.1, D2.3, and D3.1, it complements and extends the work done in these CPS Tasks and it proposes three industry-driven cybersecurity professional training schemes

1.3 Methodology

Within the framework of D3.2, the methodology adopted is presented here, under the scope of addressing the gap for common industry-driven cybersecurity professional training programmes and proposing schemes that fulfil this need.

Phase 1: We thoroughly assess the various EU and international bodies in terms of their certification efforts on the professional trainings that especially focus on sector-specific cybersecurity. At this step, we also include EU Member-States higher education certification bodies as well as EU initiatives that aim to harmonise the cybersecurity certification landscape.

Phase 2: We critically compare and contrast various standards, principles and processes that different certification authorities currently use. On these grounds, we categorise the information to be accessed by candidates of cybersecurity professional training. At this step, we also include common elements, considerations of certification bodies. This information is combined with different scales and measurements that are currently used and it will facilitate us during the schemes proposal at the next phase.

Phase 3: We present the key factors and standards that feed the CSP training schemes proposal and we thoroughly present three (3) schemes on industry-driven cybersecurity professional training.

2 Certification Landscape Related to Cybersecurity Training

In deliverables D.2.1 and D.2.2, we review EU and international efforts in cybersecurity professional and academic trainings as well as bodies that are involved in the trainings. In this chapter, we go a step further and we assess the various bodies in terms of the certification efforts of the trainings and especially for sector specific cybersecurity trainings.

2.1 International Certification Bodies

2.1.1 CompTIA

CompTIA (Computing Technology Industry Association)[1] is involved in cybersecurity certification through various certification programs designed to validate the skills and knowledge of IT professionals in the field of cybersecurity. These certifications are widely recognized in the industry and serve as a benchmark for individuals pursuing careers in cybersecurity.

The following table summarises our findings regarding the key certifications which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
• **CompTIA Security+ (Security Plus)** Purpose: Validates foundational cybersecurity skills. Content: Covers topics such as network security, compliance and operational security, threats and vulnerabilities, application, data, and host security, access control, identity management, and cryptography. • **CompTIA Cybersecurity Analyst (CySA+)** Purpose: Focuses on the skills needed for threat detection and response. Content: Emphasizes behavioral analytics, threat intelligence, vulnerability management, and incident response. • **CompTIA Advanced Security Practitioner (CASP+)** Purpose: Targets advanced cybersecurity professionals. Content: Covers enterprise security architecture, risk management, research	These certifications are designed to cater to different levels of expertise, from entry-level to advanced cybersecurity roles. CompTIA certifications are vendor-neutral, meaning they are not tied to any specific technology or product, and they are recognized globally.

[1] https://www.comptia.org/

and collaboration, and integration of enterprise security.	

2.1.2 (ISC)²

The International Information System Security Certification Consortium (ICT)[2], is a non-profit organization that plays a significant role in cybersecurity certification. It is known for offering a range of certifications that are globally recognized and respected in the information security industry.

The following table summarises our findings regarding the key certifications which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
• **Certified Information Systems Security Professional (CISSP)** Purpose: CISSP is one of the most widely recognized certifications in cybersecurity. It validates expertise in various domains, including security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security. • **Certified Cloud Security Professional (CCSP)** Purpose: Focuses on cloud security principles, architecture, design, and operations. Content: Covers topics such as cloud concepts and architecture, data security, cloud platform and infrastructure security, application security, compliance, legal, risk, and compliance. • **Systems Security Certified Practitioner (SSCP)** Purpose: Validates foundational knowledge in information security. Content: Encompasses access controls, security operations and administration, risk identification, monitoring and analysis, incident response and recovery, cryptography, network and communication security, and systems and application security. • **Certification and Accreditation Professional (CAP)**	(ISC)² certifications are known for their high standards and are often sought after by professionals in the cybersecurity field. The certifications typically require a combination of experience, adherence to a code of ethics, and successful completion of an examination.

[2] https://www.isc2.org/

Purpose: Focuses on the skills required to authorize and maintain information systems. Content: Covers risk management framework, security categorization, security control selection, implementation, assessment, authorization, and continuous monitoring.	

2.1.3 The Global Information Assurance Certification (GIAC)

The Global Information Assurance Certification (GIAC)[3] is an organization that focuses on providing certifications for information security professionals. GIAC is affiliated with the SANS Institute, a leading provider of cybersecurity training. GIAC is affiliated with the SANS Institute, a leading provider of cybersecurity training.

Some of the well-known GIAC certifications include GIAC Certified Incident Handler (GCIH), GIAC Security Essentials Certification (GSEC), GIAC Certified Penetration Tester (GPEN), and many others.

The following table summarises our findings regarding the certifications characteristics which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
• **Practical and Hands-On Approach** GIAC certifications are known for their emphasis on practical, hands-on skills. The certification exams often include real-world scenarios and practical challenges, making them valuable for professionals seeking to apply their knowledge in practical cybersecurity situations. • **Affiliation with SANS Institute** GIAC is closely associated with the SANS Institute, a well-known organization in the cybersecurity training industry. Many of the GIAC certifications are aligned with SANS training courses, and individuals often pursue GIAC certifications after completing SANS training programs. • **Global Recognition** GIAC certifications are globally recognized in the cybersecurity industry. They are respected by employers and peers alike, and holding a GIAC certification can enhance an individual's credibility in the field.	GIAC offers a variety of certifications that cover a broad range of cybersecurity domains. These certifications are designed to validate the skills and knowledge of professionals in areas such as security administration, incident response, penetration testing, forensics, and more.

[3] https://www.giac.org/

- **Continuous Education Requirements** To maintain GIAC certifications, individuals are typically required to fulfil continuing education requirements. This ensures that certified professionals stay updated with the latest developments in the rapidly evolving field of cybersecurity.	

2.1.4 The American National Standards Institute (ANSI)

The American National Standards Institute (ANSI)[4] ANSI is a private, non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. These standards aim to enhance the competitiveness of U.S. businesses and ensure the safety and health of consumers and the environment.

ANSI is not directly involved in creating or issuing cybersecurity certifications. ANSI is a private, non-profit organization that oversees the development of voluntary consensus standards for various industries, ensuring that they are developed in an open and transparent manner.

However, ANSI does play a role in accrediting organizations that develop and administer certification programs, including those in the field of cybersecurity. ANSI accredits certification bodies to certain standards, such as ISO/IEC 17024, which is the international standard for bodies operating certification of persons. This accreditation ensures that the certification process meets specific criteria for impartiality, competence, and reliability.

In the context of cybersecurity certification, ANSI's involvement is often in the accreditation of certification bodies rather than directly in the development of specific cybersecurity certifications. Certification bodies that seek ANSI accreditation must demonstrate their adherence to relevant standards and best practices.

It's essential to note that the landscape of certifications and accreditation bodies may change, and new developments may have occurred since my last update in January 2022. For the latest and most accurate information, it's recommended to check the official ANSI website or contact ANSI directly.

2.1.5 UK Cybersecurity Council

The UK Cybersecurity Council[5] is a professional body established to help address the shortage of skilled cybersecurity professionals in the United Kingdom. The council aims to enhance the overall cybersecurity posture of the country by promoting professional standards, providing education and training, and supporting the development of cybersecurity skills.

Regarding certification, the UK Cybersecurity Council plays a role in setting and endorsing standards for cybersecurity qualifications and certifications. It collaborates with various organizations, industry experts, and academia to develop a framework that ensures the quality and relevance of cybersecurity certifications. This involvement helps establish a recognized and standardized set of qualifications that individuals can pursue to demonstrate their proficiency in cybersecurity.

It's important to note that the specifics of the UK Cybersecurity Council's involvement in certification may evolve over time, and there may have been developments or changes since my last update in January 2022. I recommend checking the official website of the UK Cybersecurity Council or other reliable sources for the latest and most accurate information on their certification initiatives.

[4] https://www.ansi.org/
[5] https://www.ukcybersecuritycouncil.org.uk/

2.1.6 SANS

The SANS Institute (also known as The Escal Institute of Advanced Technologies)[6] is a US-based cooperative research and education organisation. It offers a range of education programs related to information security, live and online training, as well as resources, including webcasts.

GIAC is closely associated with the SANS Institute, a well-known organization in the cybersecurity training industry. Many of the GIAC certifications are aligned with SANS training courses, and individuals often pursue GIAC certifications after completing SANS training programs.

The SANS Institute is the preferred partner for exam preparation for GIAC Certifications (previously Global Information Assurance Certification). GIAC provides a set of vendor-neutral computer security certifications linked to the training courses provided by the SANS.

All Cybersecurity Course or Certification undertaken and awarded by SANS, correspond to either GIAC Applied Knowledge Certicification (reffered as: *Category A*) or GIAC Practicioner Certification (reffered as: *Category B*).

The following table summarises our findings regarding the three (3) Applied Knowledge Certicifications and the forty-six (46) Practicioner Certifications which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
All Cybersecurity Course or Certification undertaken and awarded by SANS, correspond to either GIAC Applied Knowledge Certicification (Category A) or a GIAC Practicioner Certification (Category B). **Category A –Applied Knowledge Certification** 1) **GIAC Experienced Cybersecurity Specialist Certification (GX-CS)** The GIAC Experienced Cybersecurity Specialist Certification (GX-CS) demonstrates that a candidate is qualified for hands-on IT systems roles. Certification holders will validate their ability to solve complex multifaceted problems through new and diversified security practices and tasks. 2) **GIAC Experienced Intrusion Analyst Certification (GX-IA)** The GIAC Experienced Intrusion Analyst Certification (GX-IA) demonstrates that a	1) **SANS Programmes Team are ISO/IEC 27001 certified** ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet. ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 168 national standards bodies. 2) **SANS Institute is Cyber Essentials Plus certified**[7] Cyber Essentials and Cyber Essentials Plus form a UK-backed government scheme, operating under the auspices of the National Cyber Security Centre.[8]

[6] https://www.sans.org/uk_en/

[7] Id.

[8] https://www.ncsc.gov.uk/cyberessentials/overview?msc=uk-lp

candidate is qualified to solve complex and unique challenges that Intrusion Analysts encounter. Certification holders will validate their ability to solve multi-step problems through incorporating various concepts and methodologies to identify malicious activity. **3) GIAC Experienced Incident Handler Certification (GX-IH)** The GIAC Experienced Incident Handler Certification (GX-IH) demonstrates a candidate's superior incident response skills. Mastery of hands-on attacker techniques combined with incident response tools and practices validate that certification holders have the skills and knowledge to take teams to the next level. **Category B – Practitioner Certification** **1)** GIAC Security Essentials (GSEC) [Cybersecurity and IT Essentials, Cyber Defense] The GIAC Security Essentials (GSEC) certification validates a practitioner's knowledge of information security beyond simple terminology and concepts. **2)** GIAC Certified Intrusion Analyst Certification (GCIA) [Cyber Defense] The GIAC Intrusion Analyst certification validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. **3)** GIAC Open Source Intelligence Certification (GOSI) [Cyber Defense] The GOSI certification confirms that practitioners have a strong foundation in OSINT methodologies and are well-versed in data collection, analysis, and reporting. **4)** GIAC Security Leadership (GSLC) [Security Management, Legal and Audit]	**3) GIAC (SANS is the preferred partner for exam preparation for GIAC Certifications) is an accredited ISO/IEC 17024 Personnel Certification Body through the ANSI National Accreditation Body ("ANAB")**[9] ANAB is a non-governmental organization that provides accreditation services and training to public and private-sector organizations. ANAB is the largest accreditation body in North America and provides services in more than 75 countries. Fully enacted on April 1, 2003, this international ANAB/ISO/IEC 17024 was designed to harmonize the personnel certification process worldwide and create a more cost-effective global standard for workers. ANAB/ISO/IEC 17024, officially entitled "General Requirements for Bodies Operating Certification Systems of Persons," plays a prominent role in facilitating global standardization of the certification community, enhancing consistency, and protecting consumers.

[9] https://www.giac.org/about/anab/?msc=main-nav

The GIAC Security Leadership (GSLC) certification validates a practitioner's understanding of governance and technical controls focused on protecting, detecting, and responding to security issues. **5)** GIAC Cloud Threat Detection (GCTD) [Cloud Security] The GCTD certification validates a practitioner's ability to detect and investigate suspicious activity in cloud infrastructure. **6)** GIAC Penetration Tester Certification (GPEN) [Penetration Testing and Red Teaming, Offensive Operations] The GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies. **7)** GIAC Security Operations Certified (GSOC) [Cyber Defense] The GSOC certification validates a practitioner's ability to defend an enterprise using essential blue team incident response tools and techniques. **8)** GIAC Security Operations Manager Certification (GSOM) [Security Management, Legal and Audit, Cyber Defense] The GSOM certification validates a professional's ability to run an effective security operations center. **9)** GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) [Penetration Testing and Red Teaming, Offensive Operations] The GIAC Exploit Researcher and Advanced Penetration Tester certification validates a practitioner's ability to find and mitigate significant security flaws in systems and networks. **10)** GIAC Systems and Network Auditor Certification (GSNA)	

[Security Management, Legal and Audit]

The GIAC Systems and Network Auditor (GSNA) certification validates a practitioner’s ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems.

11) GIAC Reverse Engineering Malware Certification (GREM)

[Digital Forensics and Incident Response, Incident Response & Threat Hunting]

The GIAC Reverse Engineering Malware (GREM) certification is designed for technologists who protect the organization from malicious code.

12) GIAC Web Application Penetration Tester (GWAPT)

[Penetration Testing and Red Teaming, Offensive Operations]

The GIAC Web Application Penetration Tester (GWAPT) certification validates a practitioner’s ability to better secure organizations through penetration testing and a thorough understanding of web application security issues.

13) GIAC Strategic Planning, Policy, and Leadership (GSTRT)

[Security Management, Legal and Audit]

The GIAC Strategic Planning, Policy, and Leadership (GSTRT) certification validates a practitioner’s understanding of developing and maintaining cyber security programs as well as proven business analysis, strategic planning, and management tools.

14) GIAC Response and Industrial Defense (GRID)

[Digital Forensics and Incident Response, Industrial Control Systems Security, Incident Response & Threat Hunting]

The GRID certification is for professionals who want to demonstrate that they can perform Active Defense strategies specific to and appropriate for an Industrial Control System (ICS) network and systems.

15) GIAC Python Coder (GPYC)

[Offensive Operations, Red Team Operations]

The GIAC Python Coder (GPYC) certification validates a practitioner's understanding of core programming concepts, and the ability to write and analyze working code using the Python programming language. **16)** GIAC Public Cloud Security (GPCS) [Cloud Security] The GPCS certification validates a practitioner's ability to secure the cloud in both public cloud and multi cloud environments. **17)** GIAC Network Forensic Analyst (GNFA) [Digital Forensics and Incident Response, Incident Response & Threat Hunting] The GIAC Network Forensic Analyst (GNFA) certification validates a practitioner's ability to perform examinations employing network forensic artifact analysis. **18)** GIAC Continuous Monitoring Certification (GMON) [Cyber Defense] The GIAC Continuous Monitoring (GMON) certification validates a practitioner's ability to deter intrusions and quickly detect anomalous activity. **19)** GIAC Mobile Device Security Analyst (GMOB) [Penetration Testing and Red Teaming, Offensive Operations] The GIAC Mobile Device Security Analyst (GMOB) certification ensures that people charged with protecting systems and networks know how to properly secure mobile devices that are accessing vital information. **20)** GIAC Law of Data Security & Investigations (GLEG) [Security Management, Legal and Audit] The GIAC Law of Data Security & Investigations (GLEG) certification validates a practitioner's knowledge of the law regarding electronically stored and transmitted records. **21)** GIAC Information Security Professional Certification (GISP) [Security Management, Legal, and Audit, Cyber Defense]	

The GIAC Information Security Professional (GISP) certification validates a practitioner's knowledge of the 8 domains of cybersecurity knowledge as determined by (ISC)2 that form a critical part of CISSP® exam. **22)** GIAC Information Security Fundamentals (GISF) [Cybersecurity and IT Essentials, Cyber Defense] The GIAC Information Security Fundamentals (GISF) certification validates a practitioner's knowledge of security's foundation, computer functions and networking, introductory level cryptography, and cybersecurity technologies. **23)** GIAC iOS and macOS Examiner (GIME) [Digital Forensics and Incident Response, Incident Response & Threat Hunting] The GIAC iOS and macOS Examiner is a cybersecurity certification that validates a practitioner's knowledge of computer forensic analysis and incident response skills. **24)** Global Industrial Cyber Security Professional Certification (GICSP) [Industrial Control Systems Security] The GICSP bridges together IT, engineering and cyber security to achieve security for industrial control systems from design through retirement. **25)** GIAC Foundational Cybersecurity Technologies (GFACT) [Purple Team, Offensive Operations, Cyber Defense] The GFACT certification validates a practitioner's knowledge of essential foundational cybersecurity concepts. **26)** GIAC Enterprise Vulnerability Assessor Certification (GEVA) [Offensive Operations, Red Team Operations] GIAC Enterprise Vulnerability Assessor is the premier certification focused on validating technical vulnerability assessment skills and time-tested practical approaches to ensure security across the enterprise. **27)** GIAC Defensible Security Architect Certification (GDSA)	

[Cyber Defense] The GDSA certification proves that practitioners can design and implement an effective combination of network-centric and data-centric controls to balance prevention, detection, and response. **28)** GIAC Defending Advanced Threats (GDAT) [Purple Team, Offensive Operations, Cyber Defense] The GDAT certification is unique in how it covers both offensive and defensive security topics in-depth. **29)** GIAC Certified Windows Security Administrator (GCWN) [Cyber Defense] The GIAC Certified Windows System Administrator (GCWN) certification validates a practitioner's ability to secure Microsoft Windows clients and servers. **30)** GIAC Cyber Threat Intelligence (GCTI) [Digital Forensics and Incident Response, Incident Response & Threat Hunting] The GCTI certification proves practitioners have mastered strategic, operational, and tactical cyber threat intelligence fundamentals and application. **31)** GIAC Cloud Security Automation (GCSA) [Cloud Security] The GCSA certification covers cloud services and modern DevSecOps practices that are used to build and deploy systems and applications more securely. **32)** GIAC Cloud Penetration Tester (GCPN) [Cloud Security, Offensive Operations, Penetration Testing and Red Teaming] The GCPN certification validates a practitioner's ability to conduct cloud-focused penetration testing and assess the security of systems, networks, architecture, and cloud technologies.	

33) GIAC Certified Project Manager (GCPM) [Security Management, Legal and Audit] The GIAC Certified Project Manager (GCPM) certification validates a practitioner's knowledge of technical project management methodology and implementation. **34)** GIAC Cloud Security Essentials Certification (GCLD) [Cloud Security] The GCLD certification validates a practitioner's ability to implement preventive, detective, and reactionary techniques to defend valuable cloud-based workloads. **35)** GIAC Critical Infrastructure Protection Certification (GCIP) [Industrial Control Systems Security] The GCIP certification validates that professionals who access, support and maintain the critical systems have an understanding of the regulatory requirements of NERC CIP as well as practical implementation strategies. **36)** GIAC Certified Incident Handler Certification (GCIH) [Offensive Operations, Cybersecurity and IT Essentials, Digital Forensics and Incident Response, Red Team Operations, Incident Response & Threat Hunting, Cyber Defense] The GIAC Incident Handler certification validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. **37)** GIAC Cloud Forensics Responder (GCFR) [Cloud Security, Digital Forensics and Incident Response] GIAC Cloud Forensics Responder is a cybersecurity certification that validates a practitioner's ability to track incidents and collect and interpret logs across Amazon, Google, and Microsoft cloud providers. **38)** GIAC Certified Forensic Examiner (GCFE) [Digital Forensics and Incident Response]	

The GIAC Certified Forensic Examiner (GCFE) certification validates a practitioner's knowledge of computer forensic analysis, with an emphasis on core skills required to collect and analyze data from Windows computer systems. **39)** GIAC Certified Forensic Analyst (GCFA) [Digital Forensics and Incident Response, Incident Response & Threat Hunting] The GCFA certification focuses on core skills required to collect and analyze data from Windows and Linux computer systems. **40)** GIAC Certified Enterprise Defender (GCED) [Cybersecurity and IT Essentials, Cyber Defense] The GCED builds on the security skills measured by the GIAC Security Essentials certification. It assesses more advanced, technical skills that are needed to defend the enterprise environment and protect an organization as a whole. **41)** GIAC Certified Detection Analyst (GCDA) [Cyber Defense] The GCDA certification proves an individual knows how to collect, analyze, and tactically use modern network and endpoint data sources to detect malicious or unauthorized activity. **42)** GIAC Critical Controls Certification (GCCC) [Security Management, Legal and Audit] The GIAC Critical Controls Certification (GCCC) is the only certification based on the CIS Controls, a prioritized, risk-based approach to security. **43)** GIAC Battlefield Forensics and Acquisition (GBFA) [Digital Forensics and Incident Response, Operating System & Device In-Depth] The GBFA certification demonstrates that an individual is trained and qualified in the proper collection, acquisition, and rapid triage analysis of many forms of data storage.	

44) GIAC Assessing and Auditing Wireless Networks (GAWN) [Penetration Testing and Red Teaming, Offensive Operations] The GAWN certification is designed for technologists who need to assess the security of wireless networks. **45)** GIAC Advanced Smartphone Forensics Certification (GASF) [Digital Forensice and Incident Response, Operating System and Device In-Depth] The popularity of mobile devices in our work and personal lives has become increasingly broad and complex. **46)** GIAC Certified Web Application Defender (GWEB) [Cloud Security] The GIAC Web Application Defender certification allows candidates to demonstrate mastery of the security knowledge and skills needed to deal with common web application errors that lead to most security problems.	

2.1.7 ISACA

ISACA is a US-based international professional association focused on IT governance. It addresses businesses and individuals aiming to advance their skills in cybersecurity, IT risk, emerging technologies, information security and governance. Additionally it enables partners and organizations to achieve Accredited Training Organization status.

In 2022, ISACA established a European entity in Dublin, while its presence in China was established in 2018.

All Cybersecurity Courses or Certifications undertaken and awarded by ISACA, can be categorised as *Category A* and *Category B* which correspond in the two categories presented in 2.10.11. Certifications (Category A) affirm holders to be among the most qualified information systems and cybersecurity in the world, while certificates (Category B) demonstrate know-how, specific skills for technical roles, the understanding and ability to implement the global framework for enterprise governance of information and technology.

The following table summarises our findings regarding the 6 Certifications and 17 Certificates which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
Category A – ISACA Certifications **1)** Certified Information Systems Auditor (CISA)	ISACA's portfolio of experience-based certifications has provided ISACA the

The Certified Information Systems Auditor® certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. CISA is accredited by the American National Standards Institute (ANSI) under the International Standard ANSI/ISO/IEC 17024:2012. **2)** Certified Information Security Manager (CISM) ISACA's Certified Information Security Manager® certification indicates expertise in information security governance, program development and management, incident management and risk management. CISM is accredited by the American National Standards Institute (ANSI) under the International Standard ANSI/ISO/IEC 17024:2012. **3)** Certified in Risk and Information Systems Control (CRISC) CRISC certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. CRISC is accredited by the American National Standards Institute (ANSI) under the International Standard ANSI/ISO/IEC 17024:2012. **4)** Certified Data Privacy Solutions Engineer (CDPSE) CDPSE is focused on validating the technical skills and knowledge it takes to assess, build and implement comprehensive data privacy measures. **5)** Certified in the Governance of Enterprise IT (CGEIT) CGEIT is unique and framework agnostic. It is the only IT governance certification that can give you the mindset to assess, design, implement and manage enterprise IT governance systems aligned with overall business goals. CGEIT is accredited by the American National Standards Institute (ANSI) under the International Standard ANSI/ISO/IEC 17024:2012. **6)** CSX Cybersecurity Practitioner (CSX-P)	recognition of being the global leader in business technology certifications. ISACA's Certifications are accredited by the ANAB under the International Standard ANAB/ISO/IEC 17024:2012.[10]

[10] https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/fact-sheets/credentialing-fact-sheet_0321-new.pdf?la=en&hash=AC0F5FABF0A44C28FEC7A6E5CB612649FB165311

The CSX-P cybersecurity certification is retired, thus only maintenance is available for existing holders.

CSX-P was the first and only comprehensive performance certification testing one’s ability to perform globally validated cybersecurity skills spanning five security functions–Identify, Protect, Detect, Respond, and Recover–derived from the **NIST Cybersecurity Framework**. CSX-P required that candidates demonstrate critical cybersecurity skills in a live, proctored, virtual environment that assessed their analytical ability to identify assets and resolve network and host cybersecurity issues by applying the foundational cybersecurity knowledge and skills required of an evolving cyber first responder.

Category B - Certificates

1) IT Risk Fundamentals Certificate

IT Risk Fundamentals Certificate covers the principles of IT risk management, the responsibilities and accountability for IT risk, how to build risk awareness and how to communicate risk.

2) IT Audit Fundamentals Certificate

IT Audit Fundamentals Certificate covers fundamental audit concepts, how to use controls effectively to objectively conduct an audit, and the practical application of audit principles.

3) COBIT Foundation Certificate

COBIT Foundation certificate is designed to help COBIT 2019 users gain a more in-depth understanding of the COBIT Framework and provide attestation of the individual’s knowledge of the concepts, principles and methodologies used to establish, enhance and maintain a system for effective governance and management of enterprise information technology.

4) Cybersecurity Fundamentals Certificate

Cybersecurity Fundamentals Certificate candidates demonstrate their understanding of the principles that frame and define cybersecurity, and the integral role of cybersecurity professionals in protecting enterprise data and infrastructure.

5) Blockchain Fundamentals Certificate

Blockchain Fundamentals utilizes a hybrid learning approach to help build an understanding of blockchain concepts, usage and considerations.

6) Computing Fundamentals Certificate

Aiming to develop a base-level knowledge and skillset through a hybrid learning approach of information technology (IT)—specifically in the areas of basic computing, networks, virtualization and security.

7) Certificate of Cloud Auditing Knowledge

Developed by ISACA and **Cloud Security Alliance® (CSA)**, the Certificate of Cloud Auditing Knowledge is the first-ever technical, vendor-neutral credential for cloud auditing. It prepares IT professionals to address the unique challenges of auditing the cloud; ensuring the right controls for confidentiality, integrity and accessibility; and mitigating risks and costs of audit management and non-compliance.

8) COBIT Design and Implementation Certificate

Developing the skills and knowledge necessary to design and implement an effective IT governance system and run governance improvement programs with the COBIT Design and Implementation program. Intended for more experienced COBIT users, the certificate program supports enterprise goal achievement.

9) Cybersecurity Audit Certificate

The Cybersecurity Audit Certificate provides audit/assurance professionals with the skills and knowledge needed to excel in audit cybersecurity processes, policies and tools, helping to ensure their organization has the infrastructure needed to prevent cyberthreats. This certificate also provides IT risk professionals with an understanding of cyber-related risk and mitigation controls.

10) COBIT 5 Certificates

ISACA's COBIT 5 credentials affirm holders among the world's most-qualified enterprise IT governance professionals.. COBIT 5 is provided in participation from ISACA's accredited partners; **APMG** and **PeopleCert**.

11) Implementing the NIST Cybersecurity Framework using COBIT 2019 Certificate

Building expertise in leading frameworks NIST and COBIT®, learning how to effectively combine cybersecurity standards and Enterprise Governance of Information & Technology (EGIT). Intended for COBIT users with foundational knowledge of the framework and a basic understanding of cybersecurity concepts.

12) Cloud Fundamentals Certificate

IT professionals increasingly need to understand the cloud as it has proven crucial in connecting businesses to critical data and services remotely. Cloud Fundamentals builds on how to assess risks, ensure

security, implement effective governance of services and providers, and optimize potential in the cloud **13)** Networks and Infrastructure Fundamentals Certificate Networks and Infrastructure Fundamentals offers the opportunity to build a base-level knowledge and skillset of the key concepts and terminology of computer networks and internets, network and infrastructure standards, protocols and models, basic network components, topologies, functions, and processes. **14)** AI Fundamentals Certificate AI focuses on building smart machines capable of performing tasks that typically require humans and is drastically increasing in demand as it continues to change the future of virtually every field of technology. AI Fundamentals allows the understanding of AI’s risks. **15)** IoT Fundamentals Certificate Thanks to the universality of wireless networks, uses for the IoT are endlessly growing -- boosting demand for IT professionals that understand its implications. IoT Fundamentals, demonstrates how to assess the risks, governance, control settings and outside security threats accompanying this evolving technology. **16)** Data Science Fundamentals Certificate Develops the ability to extract information from data sets and understand key data analysis concepts. **17)** Software Development Fundamentals Certificate Key concepts and principles of software development through a hybrid of knowledge-based lessons and hands-on training labs.	

2.1.8 CISCO Systems

Cisco Systems, Inc., commonly known as Cisco, is a multinational technology conglomerate headquartered in San Jose, California. The company specializes in networking, cybersecurity, and telecommunications equipment. Cisco is widely recognized for its substantial role in the development of the Internet's infrastructure through its array of networking hardware, software, and telecommunications equipment. Additionally, Cisco is known for its focus on specific tech markets, such as the Internet of Things (IoT), domain security, and energy management.

In the realm of cybersecurity, Cisco offers a range of certifications that cater to various levels of expertise and specializations in the field. These certifications are designed to validate the skills and knowledge of professionals in network security, threat detection, and cybersecurity management. They are separated into four categories, Category A : Expert, Category B: Professional, Category C: Associate and Category D: Entry Level. Some of the notable cybersecurity-related certifications offered by Cisco include:

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
Category A – Cisco Certifications 1) CCIE Security The Cisco Certified Internetwork Expert (CCIE) Security is an expert-level certification for network security professionals. It validates skills in designing, implementing, and troubleshooting complex security solutions using Cisco technologies. The certification process includes a comprehensive written exam and a demanding hands-on lab exam. Achieving CCIE Security indicates a high level of expertise in network security and proficiency with Cisco products and solutions. 2) CCIE Data Center This expert-level certification is tailored for professionals specializing in data center solutions, including the critical aspect of security. It encompasses the design, planning, implementation, and management of complex data center infrastructure, emphasizing secure network architectures, data center protection, and security policies. This certification is ideal for individuals responsible for ensuring security in data centers along with their operational efficiency. 3) CCIE Service Provider Aimed at network engineers and professionals in service provider environments, this certification focuses on high-end routing, switching, and troubleshooting, with a significant emphasis on securing infrastructures. It addresses the security challenges unique to service providers, including protecting large-scale networks, implementing advanced security techniques, and managing secure, high-availability services. 4) DevNet Expert As Cisco's expert-level certification for software developers and DevOps professionals, this credential underscores the importance of security in software development and network automation within Cisco ecosystems. It covers developing secure applications, automating workflows with a focus on security, and integrating robust security measures into Cisco-based systems and solutions. 5) CCIE Enterprise Infrastructure	

This certification is designed for network engineers involved in designing and managing enterprise networking solutions. It includes a comprehensive understanding of network security within enterprise infrastructures, such as securing network access, implementing advanced threat protection, and integrating security protocols in enterprise network architectures. 6) CCIE Enterprise Wireless Focused on wireless networking, this certification also heavily emphasizes the security aspects of wireless solutions. It covers wireless network design, implementation, and optimization with a strong focus on securing wireless networks against threats, implementing secure wireless access, and maintaining the integrity of wireless communications **Category B - Certificates** 1) CCNP Enterprise This professional-level certification is designed for engineers working with enterprise networking solutions. While it covers a broad range of topics including routing, switching, and wireless, there is a significant focus on security within enterprise networks. It teaches professionals how to secure and manage enterprise network infrastructures against modern cybersecurity threats. 2) CCNP Data Center Tailored for professionals managing data center solutions, this certification includes aspects of data center security. It covers the design, implementation, and management of data center infrastructure with a strong emphasis on securing data center environments against internal and external threats. 3) CCNP Security Specifically focused on security, this certification is ideal for network security engineers and professionals. It covers security in routers, switches, networking devices, and appliances, as well as choosing, deploying, supporting, and troubleshooting firewalls, VPNs, and IDS/IPS solutions for networking environments. 4) CCNP Service Provider Aimed at professionals working in service provider environments, this certification addresses not just high-end routing and switching but also the security challenges unique to service providers. It includes securing large-scale network infrastructures and protecting network data flowing through service provider networks.	

5) CyberOps Professional

This certification is specifically designed for cybersecurity professionals in operational roles. It focuses on advanced cybersecurity skills and knowledge needed for cybersecurity operations, including threat detection, incident response, forensic analysis, and understanding cybersecurity policies and frameworks.

6) DevNet Professional

Aimed at software developers and DevOps professionals working with Cisco technologies, this certification includes a significant component on implementing security in software development. It covers developing secure applications and automating workflows with a strong focus on integrating secure practices and methodologies within Cisco environments.

Category C - Certificates

1) CCNA

This foundational certification is ideal for entry-level network professionals. While it covers a broad range of networking concepts, including network access, IP connectivity, and automation, it also has a strong emphasis on network security. The CCNA prepares professionals to install, configure, and operate secure network infrastructures, ensuring they understand basic cybersecurity principles and can address security threats and vulnerabilities in network environments.

2) CyberOps Associate

Specifically designed for cybersecurity beginners, this certification focuses on security operations and incident response. It teaches foundational cybersecurity skills, including how to detect and respond to cybersecurity incidents, understanding cybersecurity policies, and the basics of digital forensics. This certification is ideal for those aiming to work in security operations centers (SOCs) and seeking to develop a career in cybersecurity.

3) DevNet Associate

Targeted at software developers and DevOps engineers focusing on Cisco platforms, this associate-level certification includes aspects of security in software development and network automation. It covers developing and maintaining applications built on Cisco platforms with a strong emphasis on implementing secure coding practices and understanding how to

integrate security into automated network configurations and applications. **Category D – Certificates** 1) Cisco Certified Support Technician (CCST) The Cisco Certified Support Technician (CCST) program, comprising the CCST Networking and CCST Cybersecurity certifications, is designed to equip individuals with foundational tech skills, with a strong focus on security aspects. The Networking certification, while centered on network operations, also incorporates essential network security knowledge. The Cybersecurity certification, more directly targeted at security, covers core principles and practices in cybersecurity, including risk management and incident response. Both certifications validate the necessary skills for entry-level roles in their respective fields of networking and cybersecurity	

2.1.9 Microsoft

Microsoft, as a technology giant, plays a pivotal role in tech certifications, offering a diverse range of credentials that are key to professional development in the IT industry. These certifications cover various aspects of technology, including cybersecurity, cloud computing, and software development, catering to different levels of expertise.

Regarded globally as benchmarks of proficiency, Microsoft's certifications not only validate skills in using its technologies but also aid in career progression. They are designed to align with the latest industry trends and demands, ensuring that professionals are equipped with relevant and up-to-date knowledge.

By providing these certifications, Microsoft contributes significantly to shaping the skills and capabilities of the IT workforce. Its certifications are not just about acquiring credentials; they represent a commitment to continuous learning and adapting in a rapidly evolving tech environment. This role of Microsoft makes it a leader in tech certifications, helping to set standards and guide professional growth in the global IT community. Certifications are set in three categories Category A: Advanced, Category B: Intermediate and Category C: Beginner. Some of the cybersecurity related courses are mentioned below:

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
Category A – Microsoft Certifications 1) Microsoft Certified: Cybersecurity Architect Expert	

This advanced certification is designed for experienced IT professionals who specialize in cybersecurity. It focuses on developing comprehensive cybersecurity strategies and implementing solutions across multiple domains, including identity management, data protection, application security, and network infrastructure. The certification emphasizes creating robust security frameworks that adhere to Zero Trust principles and address various aspects of organizational security. 2) Exam SC-100: Microsoft Cybersecurity Architect This expert-level certification focuses on the development and implementation of cybersecurity strategies to safeguard an organization's assets. This role involves creating security solutions across various domains, emphasizing Zero Trust principles and best practices. The certification recognizes the ability to collaborate with IT security professionals and integrate security solutions in diverse areas like identity, data, and network security, as well as risk management. It's designed for professionals with experience in key cybersecurity areas, ensuring the alignment of security measures with business needs. **Category B - Certificates** 1) Configure SIEM security operations using Microsoft Sentinel This certification is designed for IT professionals specializing in security operations and threat management. This certification focuses on utilizing Microsoft Sentinel, a cloud-native SIEM (Security Information and Event Management) platform, for monitoring, detecting, and responding to security threats. It covers configuring, managing, and operating the Sentinel platform to enhance an organization's security posture, including setting up security alerts, incident management, and integration with other security tools. This certification is suitable for those looking to develop expertise in managing security operations and threat intelligence using Microsoft's advanced SIEM solutions. 2) Implement security through a pipeline using Azure DevOps This certification focuses on integrating security practices within the Azure DevOps pipeline. This program is tailored for professionals who are involved in the development and operations (DevOps) processes and are looking to embed security measures into their workflow. It covers implementing security in various stages of software development and deployment, including continuous integration and continuous	

delivery (CI/CD) processes. The certification emphasizes on securing code, managing vulnerabilities, and ensuring compliance, making it ideal for those seeking to strengthen the security aspect of their DevOps practices. 3) Exam AZ-500: Microsoft Azure Security Technologies This certification is tailored for IT professionals focusing on the security aspects of Azure services. This exam tests a candidate's ability to implement and manage security controls, maintain the security posture, and identify as well as remediate vulnerabilities within Azure environments. Key areas covered include securing network infrastructures, managing identity and access, protecting data, applications, and virtualization strategies in Azure. The certification is suitable for those looking to demonstrate their expertise in Azure security and to ensure robust protection for cloud-based services and applications. 4) Microsoft Certified: Azure Security Engineer Associate The Microsoft Certified: Azure Security Engineer Associate certification is designed for IT professionals specializing in securing Azure cloud environments. This certification validates the skills necessary to implement security controls, manage identity and access, and protect data, applications, and networks within Azure. It focuses on areas such as network security, threat protection, security management, and ensuring a robust security posture for Azure-based services. Ideal for individuals aiming to showcase their expertise in Azure security, this certification demonstrates the ability to create and maintain secure and compliant cloud environments. 5) Microsoft Certified: Security Operations Analyst Associate The Microsoft Certified: Security Operations Analyst Associate certification is aimed at IT professionals specializing in security operations. This certification focuses on equipping candidates with the skills necessary for threat detection, response, and remediation within an organization's IT environment, particularly leveraging Microsoft security solutions. It emphasizes on managing and analyzing security alerts, implementing threat protection strategies, and understanding the landscape of cybersecurity threats. This certification is ideal for those responsible for monitoring and responding to security incidents in network environments, ensuring robust defense against cybersecurity threats.	

6) Exam SC-200: Microsoft Security Operations Analyst

This certification is designed for IT professionals focusing on security operations within network environments. This certification emphasizes the skills needed for threat detection, investigation, response, and remediation, using Microsoft's security tools and services. It is particularly suitable for those who manage and analyze security alerts, implement threat protection measures, and address cybersecurity threats in real-time. The certification ensures proficiency in handling security incidents and maintaining robust cybersecurity defenses in organizational IT infrastructures.

Category C - Certificates

1) Microsoft Certified: Cybersecurity Architect Expert

The Microsoft Certified: Cybersecurity Architect Expert certification is designed for seasoned IT professionals who specialize in creating and implementing comprehensive cybersecurity strategies. This certification validates expertise in designing cybersecurity solutions that protect an organization’s digital assets across various domains, such as identity management, data protection, network security, and application security. It emphasizes a deep understanding of security principles, including Zero Trust, and the ability to effectively integrate these principles into a cohesive security strategy that aligns with an organization's operational needs and objectives. This certification is ideal for professionals who are experienced in various aspects of cybersecurity and are seeking to demonstrate their capabilities in architecting advanced security solutions within diverse IT environments

2) Exam SC-100: Microsoft Cybersecurity Architect

The Microsoft Certified: Cybersecurity Architect certification, which includes passing the Exam SC-100, is tailored for experienced cybersecurity professionals. This certification focuses on evaluating a candidate's ability to design and implement comprehensive cybersecurity strategies and solutions in diverse IT environments. It encompasses aspects such as designing secure infrastructure, managing identity, data, and application security, and aligning cybersecurity strategies with business objectives. The certification is ideal for professionals with a broad range of cybersecurity knowledge and experience, looking to demonstrate their expertise in architecting and overseeing the implementation of security solutions in complex organizational contexts.

2.1.10 ORACLE

Oracle stands as a cornerstone in the realm of technology certifications, particularly emphasizing the crucial area of security. Through its comprehensive suite of credentials, Oracle empowers IT professionals to master various dimensions of cybersecurity, cloud security, and data protection. These certifications are globally recognized as standards of excellence, underscoring a professional's ability to navigate and secure Oracle's complex technology landscapes.

With a focus on real-world application and the latest security practices, Oracle's certifications serve as a testament to an individual's commitment to staying abreast of technological advancements and safeguarding digital assets. Oracle's dedication to offering these certifications underscores its influence in molding a proficient and security-conscious IT workforce, prepared to tackle the challenges of today's cyber-threat landscape. By investing in Oracle certifications, professionals demonstrate their dedication to excellence and a proactive approach to cybersecurity, positioning themselves as valuable assets in the global IT community. Next are certifications offered by ORACLE related to cybersecurity:

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
1) Oracle APEX Cloud Developer Professional Exam Number: 1Z0-770 The Oracle APEX Cloud Developer Professional certification (1Z0-770) primarily assesses expertise in developing secure, robust applications using Oracle Application Express (APEX) in cloud environments. It emphasizes understanding of APEX security features, including user authentication, authorization, data protection, and secure application deployment on Oracle Cloud. Candidates demonstrate the ability to implement best practices for securing data and ensuring privacy, crucial for creating trustworthy cloud-based applications. This certification is vital for professionals aiming to specialize in the security aspects of APEX cloud development. 2) Oracle SOA Suite 12c Essentials Exam Number: 1Z0-434 The Oracle SOA Suite 12c Essentials certification, denoted by exam number 1Z0-434, validates expertise in implementing robust and secure service-oriented architecture solutions using Oracle SOA Suite 12c. This certification focuses on ensuring that candidates have a strong understanding of securing services and composite applications, including configuring security policies, managing secure interactions, and applying best practices for protecting services in a SOA environment. Professionals seeking this certification are tested on their ability to design, deploy, and manage secure	

integrations and customizations using the suite's extensive set of tools. It's particularly crucial for individuals looking to demonstrate their skills in creating secure, reliable, and scalable services using Oracle SOA Suite 12c, making them valuable assets in complex enterprise environments where security is a top priority.

3) Oracle Business Process Management Suite 12c Essentials
   Exam Number: 1Z0-435

The Oracle Business Process Management Suite 12c Essentials certification, associated with exam number 1Z0-435, is geared towards professionals adept in implementing business solutions using Oracle BPM Suite 12c. While the certification encompasses various aspects of business process management, including modelling, simulation, and execution, it also ensures that candidates understand the security measures and best practices essential to deploying and managing business processes.

Candidates are expected to have knowledge of handling security within the suite, focusing on securing business processes, ensuring data integrity, and managing user roles and access to process resources. The security aspect, though not the sole focus, is integral to managing and automating sensitive and critical business processes efficiently and safely within the Oracle BPM Suite 12c framework. This certification is ideal for professionals aiming to validate their comprehensive skills, including security considerations, in business process management using Oracle's tools.

4) Oracle Business Process Management Suite 12c Essentials
   Exam Number: 1Z0-435

The Oracle Business Process Management Suite 12c Essentials certification (Exam Number: 1Z0-435) acknowledges professionals skilled in deploying, managing, and optimizing business processes with Oracle BPM Suite 12c. While the certification covers various facets of BPM, including design, execution, and monitoring of business processes, it also ensures that the candidates are conversant with implementing necessary security measures.

Candidates are expected to demonstrate knowledge in securing business processes, managing user roles, access privileges, and ensuring that the processes adhere to compliance and governance standards. Security in this context is about safeguarding process integrity, data confidentiality, and ensuring that the business workflows are robust against unauthorized access or breaches. This certification is ideal for individuals looking to prove their expertise in not just managing and optimizing business processes using Oracle BPM Suite 12c, but also in ensuring these processes are securely executed and managed.

5) Oracle WebLogic Server 12c: Administration I Exam Number: 1Z0-133

The Oracle WebLogic Server 12c: Administration I certification (Exam Number: 1Z0-133) is aimed at professionals specializing in the administration and management of Oracle WebLogic Server 12c. The certification encompasses a comprehensive understanding of deploying, configuring, and securing applications on Oracle WebLogic Server.

Security, while a part of the certification, focuses on the ability to configure and manage robust security environments within WebLogic Server. Candidates are expected to demonstrate proficiency in securing the server environment, implementing SSL, managing user accounts, securing application resources, and ensuring secure communication across domains and applications. This involves understanding security realms, authentication, authorization, and auditing mechanisms pertinent to Oracle WebLogic Server 12c.

This certification is crucial for administrators seeking to validate their skills in effectively managing and securing Oracle WebLogic Server environments, ensuring applications run securely and efficiently.

6) Oracle Exadata Database Machine X9M Implementation Essentials Exam Number: 1Z0-902

The Oracle Exadata Database Machine X9M Implementation Essentials certification (Exam Number: 1Z0-902) targets professionals involved in the setup, configuration, and maintenance of the Oracle Exadata Database Machine. This certification ensures candidates have a detailed understanding of the Exadata Database Machine features and capabilities, with a specific focus on implementing solutions that leverage its high performance and scalability for optimal database operations.

While the certification comprehensively covers Exadata's architecture, software, and hardware components, it also includes aspects of security essential for safeguarding data and operations. Candidates should understand how to implement Exadata security features, including database encryption, secure configuration, and administration practices that protect against unauthorized access and ensure data integrity. Knowledge of network isolation, storage security, and compliance with security best practices specific to Exadata environments is also crucial.

This certification is vital for professionals looking to demonstrate their expertise in deploying and managing Oracle Exadata Database Machine environments with a keen understanding of maintaining high security and performance standards.

7) Oracle Database Security Administration Exam Number: 1Z0-116

The Oracle Database Security Administration certification (Exam Number: 1Z0-116) is tailored for database administrators, security administrators, and IT professionals responsible for implementing, managing, and maintaining security in Oracle Database environments. This certification affirms the candidate's in-depth knowledge and skills in securing Oracle Databases against various threats and unauthorized access.

Key areas of focus include understanding and applying Oracle Database security features, such as encryption and redaction, user management and access control, auditing and compliance, and securing data both at rest and in transit. Candidates are tested on their ability to implement robust security policies, manage privileges, and create a secure database environment using Oracle's advanced security options.

This certification is essential for professionals aiming to specialize in the security aspects of Oracle Database administration, ensuring the confidentiality, integrity, and availability of data in enterprise settings. It validates an individual's commitment to maintaining best-in-class security practices in Oracle Database environments.

8) Oracle Database 19c: Data Guard Administration
Exam Number: 1Z0-076

The Oracle Database 19c: Data Guard Administration certification (Exam Number: 1Z0-076) is designed for database administrators who specialize in creating, managing, and maintaining Data Guard configurations. Oracle Data Guard is a key feature of Oracle Database that provides data protection and high availability for enterprise data.

This certification focuses on the candidate's ability to set up and manage Oracle Data Guard environments, ensuring data is protected against failures, disasters, and data corruptions. Key topics include configuring and managing physical and logical standby databases, performing switchover and failover operations, and effectively utilizing Data Guard for data protection and disaster recovery purposes.

While the certification primarily centers around high availability and data protection, there's an inherent aspect of security in ensuring that the data remains consistent, intact, and secure during various operations and in different scenarios. Understanding the security implications in the context of Data Guard, such as network configuration and encryption for secure data transport, is also crucial.

This certification is vital for database administrators looking to prove their expertise in maintaining high data availability, protection, and disaster recovery using Oracle Database 19c Data Guard.

9) Oracle Database 19c: RAC, ASM, and Grid Infrastructure Administration
Exam Number: 1Z0-078

The Oracle Database 19c: RAC, ASM, and Grid Infrastructure Administration certification (Exam Number: 1Z0-078) is aimed at database administrators and IT professionals focusing on the advanced configuration, management, and maintenance of Oracle Real Application Clusters (RAC), Automatic Storage Management (ASM), and Grid Infrastructure.

This certification ensures candidates have a comprehensive understanding of deploying and managing Oracle RAC environments for high availability, scalability, and

performance. It includes in-depth knowledge of setting up and managing ASM for optimal database storage, as well as configuring and administering the Grid Infrastructure which is foundational to RAC and ASM.

While the certification focuses on the technical aspects of setting up and maintaining RAC, ASM, and Grid Infrastructure, it also includes elements of security, particularly in terms of ensuring the integrity and resilience of data and database services. Candidates should understand how to configure these components securely, manage role-based access, protect against unauthorized access, and ensure data is securely stored and handled within these complex environments.

Professionals who earn this certification are recognized for their ability to effectively administer Oracle Database 19c environments utilizing RAC, ASM, and Grid Infrastructure, ensuring high performance, availability, and secure database operations.

10) Oracle Cloud Fusion Analytics Warehouse 2023 Implementation Professional Exam Number: 1Z0-1118-23

The Oracle Cloud Fusion Analytics Warehouse 2023 Implementation Professional certification (Exam Number: 1Z0-1118-23) is designed for professionals

involved in implementing and managing Oracle Fusion Analytics Warehouse solutions. This certification validates an individual's comprehensive understanding of the architecture, setup, and effective management of Fusion Analytics Warehouse to drive insightful analytics and reporting across business processes. Candidates are expected to demonstrate proficiency in configuring the analytics warehouse, integrating data sources, setting up data models, and ensuring the overall solution is tailored to meet business requirements. While the focus is on implementing analytics solutions, there's an underlying emphasis on securing data and analytics infrastructure, managing user access, and ensuring compliance with data governance standards. Security aspects might include understanding how to protect sensitive data, manage data access securely, and ensure that the analytics environment is robust against unauthorized access or data breaches. As analytics often involve handling sensitive business information, a thorough understanding of security best practices in the context of Oracle Fusion Analytics Warehouse is crucial. This certification is vital for individuals looking to validate their skills in leveraging Oracle's powerful analytics platform to transform data into actionable business insights, all while maintaining high standards of security and compliance. 11) Oracle Cloud Infrastructure 2023 Architect Associate Exam Number: 1Z0-1072-23 The Oracle Cloud Infrastructure 2023 Architect Associate certification (Exam Number: 1Z0-1072-23) is designed for individuals who are involved in the architecture, design, and maintenance of solutions in Oracle Cloud Infrastructure (OCI). This certification validates a candidate's deep understanding of OCI services and architecture, including computing, networking, storage, and database services, and how to best deploy these in a cloud environment. Candidates are tested on their ability to design scalable, secure, and robust cloud solutions using Oracle Cloud Infrastructure. While the certification covers a wide range of knowledge about OCI's offerings, a significant emphasis is placed on security aspects. This includes understanding how to implement security and compliance policies, manage identity and access, and ensure data protection through encryption, network security, and other best practices. Professionals seeking this certification should be able to effectively design and implement OCI solutions that meet business requirements while ensuring data is	

secure and systems are resilient against threats. This certification is ideal for architects and administrators looking to demonstrate their expertise in building and managing cloud solutions on Oracle's cloud platform, with a particular focus on maintaining high security and performance standards.

12) Oracle Cloud Infrastructure 2023 Developer Professional
Exam Number: 1Z0-1084-23

The Oracle Cloud Infrastructure 2023 Developer Professional certification (Exam Number: 1Z0-1084-23) is tailored for developers and professionals who specialize in designing, developing, and deploying applications on Oracle Cloud Infrastructure (OCI). This certification assesses a comprehensive understanding of OCI services related to application development, including computing, storage, database, networking, and security, as well as developer tools provided by Oracle.

Candidates pursuing this certification are expected to demonstrate their skills in building cloud-native applications, integrating services, automating processes, and implementing effective solutions using OCI's development tools and platforms. A significant focus is also placed on understanding and applying best practices for application security, including securing application data, managing user authentication and authorization, and ensuring the applications are resilient against various threats.

While the certification broadly covers all aspects of cloud application development on OCI, it ensures that developers are proficient in implementing security measures at every stage of the development and deployment process. This includes securing application codes, protecting data, and configuring the cloud environment securely.

Professionals earning this certification are recognized for their ability to develop secure, scalable, and efficient applications leveraging the comprehensive capabilities of Oracle Cloud Infrastructure, ensuring they meet the evolving needs of modern businesses.

13) Oracle Cloud Infrastructure 2023 Security Professional
Exam Number: 1Z0-1104-23

The Oracle Cloud Infrastructure 2023 Security Professional certification (Exam Number: 1Z0-1104-23) is specifically designed for individuals who are focused on the security aspects of Oracle Cloud Infrastructure (OCI). This certification validates the in-depth knowledge and skills required to understand,

implement, and manage the advanced security services and features within OCI. Candidates are tested on a wide array of security topics, including identity and access management, data encryption, secure network architecture, security compliance requirements, and the use of Oracle's security and monitoring tools. They need to demonstrate proficiency in designing, implementing, and managing comprehensive security strategies to protect applications, data, and infrastructure in the cloud. The certification ensures that the professionals are adept at applying best security practices, understanding the latest security threats and how to mitigate them, configuring and managing cloud security services, and understanding regulatory compliance aspects relevant to cloud security. Professionals who earn this certification are recognized as experts in OCI security, capable of securing cloud environments and advising organizations on security best practices, strategies, and solutions. This certification is crucial for security specialists, cloud architects, and IT professionals responsible for managing and safeguarding cloud infrastructure and applications.	

2.1.11 Professional Evaluation and Certification Board (PECB)

PECB (Professional Evaluation and Certification Board) holds a prominent position as a distinguished tech certification provider. With a global footprint, PECB offers an extensive array of professional certifications, catering to diverse technology and cybersecurity disciplines.

At its core, PECB's mission revolves around validating the expertise and competence of professionals in these domains. PECB certifications are universally acknowledged and esteemed, serving as a gold standard for excellence in the tech and cybersecurity sectors. These certifications adhere to stringent international standards and best practices, ensuring that certified individuals possess the knowledge and skills required to excel in their roles.

PECB goes beyond certification by fostering continuous professional development. Through its programs, it equips individuals with the latest industry insights and trends, enabling them to stay at the forefront of their respective fields. By doing so, PECB contributes to enhancing the capabilities of professionals and the security of organizations.

Ultimately, PECB's role extends to supporting both individuals and organizations in the tech and cybersecurity realms. It empowers professionals to achieve their career goals while helping organizations secure their data, mitigate risks, and ensure compliance with industry regulations. PECB's comprehensive approach to certification and professional development plays a vital role in shaping the competence and standards within the ever-evolving tech and cybersecurity landscape. Next are certifications offered by PECB related to cybersecurity:

Stakeholders

End-user viewpoint	Certification scheme viewpoint
PECB Certifications ISO/IEC 27002 Information Security Controls The ISO/IEC 27002 Information Security Controls certification provided by PECB is a respected standard that focuses on implementing effective security controls within organizations. This certification emphasizes the practical application of security measures to protect information assets. By adhering to ISO/IEC 27002 guidelines, businesses can establish a comprehensive set of security controls tailored to their specific needs. PECB's certification program equips professionals and organizations with the knowledge and skills to select, implement, and manage these controls effectively. This certification demonstrates a commitment to robust information security practices and enhances an organization's ability to safeguard its digital assets and sensitive information. PECB Chief Information Security Officer The PECB Chief Information Security Officer (CISO) certification is a prestigious credential that equips individuals with the knowledge, skills, and competencies needed to lead and manage an organization's information security strategy. It emphasizes strategic planning, risk management, leadership, and technical expertise. This certification is ideal for those aspiring to or currently in senior information security leadership roles, demonstrating their commitment and readiness to address complex cybersecurity challenges. Risk Assessment Methods PECB's Risk Assessment Methods certification provides professionals with comprehensive expertise in assessing and managing risks. This credential focuses on practical methodologies for identifying, analyzing, and mitigating risks across various domains. It equips individuals with the skills needed to enhance organizational resilience and make informed decisions. This certification is highly valuable for professionals seeking to strengthen their risk management capabilities and contribute effectively to their organization's overall risk strategy. ISO/IEC 27005 Information Security Risk Management PECB's ISO/IEC 27005 Information Security Risk Management certification offers in-depth knowledge and skills in managing information security risks. It concentrates on practical methodologies for identifying, assessing, and mitigating risks in accordance with global standards. This certification empowers	

individuals to enhance information security, make informed risk-based decisions, and strengthen organizational resilience. It is a valuable credential for professionals aiming to excel in the field of information security risk management. ISO/IEC 27035 Information Security Incident Management PECB's ISO/IEC 27035 Information Security Incident Management certification offers comprehensive knowledge and skills in managing security incidents effectively. This certification emphasizes the implementation of industry best_practices for incident detection, response, and recovery, aligning with international standards. It equips individuals with the capabilities to minimize the impact of security incidents and ensure business continuity. This certification is a valuable asset for professionals looking to excel in the field of information security incident management, provided by PECB. Cybersecurity Management PECB's Cybersecurity Management certification provides comprehensive expertise in effectively managing cybersecurity practices. This certification focuses on implementing best practices for cybersecurity governance, risk management, and compliance. It equips individuals with the skills to protect critical assets, detect and respond to threats, and ensure a robust cybersecurity posture. This certification is highly valuable for professionals aiming to excel in the field of cybersecurity management, offered by PECB. Cloud Security PECB's Cloud Security certification equips professionals with comprehensive expertise in securing cloud environments effectively. This certification focuses on best practices for cloud security governance, risk management, and compliance. It empowers individuals to protect data in cloud platforms, detect and respond to cloud-specific threats, and ensure a secure cloud infrastructure. This certification is highly valuable for professionals seeking to excel in the field of cloud security, offered by PECB. Penetration Testing Professional PECB's Penetration Testing Professional certification provides comprehensive expertise in conducting penetration tests to assess and strengthen cybersecurity defenses. This certification focuses on practical methodologies for identifying vulnerabilities, exploiting them ethically, and providing recommendations for remediation. It equips individuals	

with the skills to enhance an organization's security posture through rigorous testing. This certification is highly valuable for professionals aiming to excel in the field of penetration testing, offered by PECB. Ethical Hacking PECB's Ethical Hacking certification equips professionals with comprehensive expertise in identifying and addressing vulnerabilities in information systems. This certification focuses on ethical hacking techniques, penetration testing, and security assessments to secure networks and applications effectively. It empowers individuals with the skills to proactively safeguard organizations from cyber threats. This certification is highly valuable for professionals seeking to excel in the field of ethical hacking, offered by PECB. SCADA Security Manager PECB's SCADA Security Manager certification is a specialized program for professionals looking to secure Supervisory Control and Data Acquisition (SCADA) systems. Key features include deep insights into SCADA systems, threat assessment, risk management, security controls, incident response, compliance knowledge, practical skills, global recognition, and career advancement opportunities. This certification equips individuals to protect critical infrastructure from cyber threats efficiently. Computer Forensics PECB's Computer Forensics certification is a specialized program for professionals focused on digital investigation and cybercrime analysis. Key features include in-depth knowledge of digital forensics, evidence handling, cybercrime investigation techniques, legal compliance, practical skills, global recognition, and career advancement opportunities. This certification equips individuals to investigate digital incidents and contribute to the field of cybersecurity effectively. ISO/IEC 27033 Network Security PECB's ISO/IEC 27033 Network Security certification is a specialized program for professionals specializing in securing network infrastructures. Key features include in-depth knowledge of network security, risk assessment, security controls, compliance with ISO/IEC 27033 standards, practical skills, global recognition, and career advancement opportunities. This certification equips individuals to design and maintain secure network environments, ensuring the confidentiality, integrity, and availability of critical data.	

Cybersecurity Maturity Model Certification PECB's Cybersecurity Maturity Model Certification (CMMC) training is designed for professionals focusing on cybersecurity and compliance in the defense industry. Key features include a comprehensive understanding of CMMC requirements, assessment methodologies, security controls, compliance readiness, practical skills, global recognition, and career advancement opportunities. This certification equips individuals to help defense contractors meet cybersecurity standards, safeguard sensitive information, and navigate compliance obligations effectively. NIS 2 Directive PECB's NIS 2 Directive certification is tailored for professionals involved in cybersecurity and critical infrastructure protection. Key features include a deep understanding of the NIS 2 Directive, risk assessment, security measures, compliance readiness, practical skills, global recognition, and career advancement opportunities. This certification equips individuals to assist organizations in complying with NIS 2 regulations, fortifying their cybersecurity posture, and ensuring the resilience of critical services and infrastructure. ISO 31000 Risk Management PECB's ISO 31000 Risk Management certification is designed for professionals focused on risk management and organizational resilience. Key features include comprehensive knowledge of ISO 31000 principles, risk assessment, risk treatment, practical risk management skills, global recognition, and career advancement opportunities. This certification equips individuals to implement effective risk management practices, enhance decision-making processes, and contribute to the overall resilience and success of organizations ISO/IEC 27701 Privacy Information Management System PECB's ISO/IEC 27701 Privacy Information Management System (PIMS) certification is tailored for professionals specializing in privacy management and data protection. Key features include a deep understanding of ISO/IEC 27701 requirements, privacy risk assessment, data protection controls, practical skills in managing privacy information, global recognition, and career advancement opportunities. This certification equips individuals to help organizations establish robust privacy management systems, comply	

with privacy regulations, protect personal data, and build trust with stakeholders. General Data Protection Regulation (GDPR) PECB's General Data Protection Regulation (GDPR) certification is designed for professionals focusing on data protection and compliance with GDPR standards. Key features include a comprehensive understanding of GDPR requirements, data protection principles, compliance readiness, practical skills in GDPR implementation, global recognition, and career advancement opportunities. This certification equips individuals to assist organizations in complying with GDPR regulations, protecting individuals' data rights, and ensuring data privacy in an increasingly digital world. ISO 28000 Supply Chain Security Management System PECB's ISO 28000 Supply Chain Security Management System certification is ideal for professionals specializing in supply chain security and risk management. Key features include a deep understanding of ISO 28000 requirements, supply chain risk assessment, security controls, practical skills in managing supply chain security, global recognition, and career advancement opportunities. This certification equips individuals to help organizations secure their supply chains, mitigate risks, and ensure the safe and efficient movement of goods from origin to destination. ISO 18788 Security Operations Management System PECB's ISO 18788 Security Operations Management System certification is tailored for professionals focused on security operations and risk management. Key features include a comprehensive understanding of ISO 18788 requirements, security operations planning, risk assessment, practical skills in managing security operations, global recognition, and career advancement opportunities. This certification equips individuals to help organizations establish and maintain effective security operations, protect assets, and respond to security threats efficiently.	

2.1.12 SAP University Alliances

The SAP University Alliances program is a global initiative that enables educational institutions to integrate the latest SAP technologies into their teaching. By joining this program, universities and colleges gain access to SAP software tools, academic resources, and curricular content, which can be incorporated into their courses and academic projects. This initiative is designed to expose students to leading SAP technologies and best practices, thereby enhancing their job market readiness in fields related to business and information technology. The security related SAP certifications offered are the following:

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
SAP Certifications 1) SAP Certified Technology Associate - SAP HANA The SAP Certified Technology Associate - SAP HANA certification with a focus on its security components is designed for professionals who want to validate their expertise in managing and securing SAP HANA environments. This certification assesses the candidate's knowledge in configuring and implementing security measures within SAP HANA, understanding the database's architecture from a security perspective, and ensuring data protection and compliance with relevant standards and practices. Key topics covered include authentication, authorization, data encryption, and audit logging, as well as best practices for securing SAP HANA both on-premise and in cloud deployments. By earning this certification, individuals demonstrate their skills in safeguarding SAP HANA databases against unauthorized access and threats, making them valuable assets to organizations that prioritize data security within their SAP landscapes. 2) SAP Certified Technology Associate - SAP System Security and Authorizations The SAP Certified Technology Associate - SAP System Security and Authorizations certification is tailored for IT professionals seeking to affirm their expertise in the security and authorization aspects of SAP systems. This certification focuses on the candidate’s ability to configure and manage security settings, design and implement authorization concepts, and ensure compliance with security policies and standards within SAP environments. Key areas of emphasis include understanding the fundamentals of SAP system security, managing user authentication and authorizations, securing network communications, and applying best practices for system security. Additionally, it covers the practical aspects of managing access control and preventing unauthorized system use, ensuring that candidates are well-versed in protecting SAP systems against potential security breaches. Achieving this certification signifies a thorough understanding of how to maintain a secure and compliant SAP system, addressing the critical need for security expertise in today’s SAP-enabled business processes.	

3) SAP Certified Technology Associate - SAP NetWeaver Application Server for SAP S/4HANA

The The SAP Certified Technology Associate - SAP NetWeaver Application Server for SAP S/4HANA certification, with a refined focus on security aspects, is tailored for professionals aiming to excel in securing and managing the SAP NetWeaver Application Server within SAP S/4HANA environments. This certification rigorously assesses the candidate's expertise in implementing security measures, configuring secure system settings, and maintaining the integrity and confidentiality of data processed by the SAP NetWeaver Application Server.

Key security-focused areas of this certification include understanding how to protect the application server against various security threats and vulnerabilities, implementing authentication and authorization mechanisms to control access to system resources, and ensuring secure communication between the SAP NetWeaver Application Server and other components within the SAP landscape. It also covers the management of encryption technologies for data in transit and at rest, along with the setup of audit logging to monitor and record security-related events.

Furthermore, the certification delves into best practices for security patch management and the regular updating of system components to mitigate potential security risks. It emphasizes the importance of configuring the SAP NetWeaver Application Server to comply with organizational security policies and regulatory requirements, ensuring that the system's administration adheres to high standards of security governance.

Achieving this certification signifies that the individual is proficient in safeguarding the SAP NetWeaver Application Server for SAP S/4HANA, demonstrating their capability to manage security aspects efficiently. This credential is especially relevant for system administrators, security consultants, and IT professionals responsible for the secure operation and technical maintenance of SAP S/4HANA solutions, highlighting their specialized skills in securing one of SAP's core technology platforms against cybersecurity threats.

4) SAP Certified Development Associate - SAP Fiori Application Developer

The The SAP Certified Development Associate - SAP Fiori Application Developer certification, with a special emphasis on security aspects, targets developers and IT professionals focused on creating secure SAP Fiori applications. This certification evaluates the candidate's ability to implement SAP Fiori applications with robust security measures to protect sensitive data and ensure secure user interactions within the SAP ecosystem. In this security-oriented approach, the certification covers essential security concepts and practices for SAP Fiori development, including secure coding techniques to prevent common vulnerabilities such as cross-site scripting (XSS) and SQL injection. Candidates are tested on their proficiency in utilizing authentication and authorization mechanisms to control access to applications and data, ensuring that SAP Fiori apps adhere to the principle of least privilege. The certification also delves into the secure configuration of SAP Fiori apps, highlighting the importance of encrypting data in transit and at rest, and configuring secure communication channels between SAP Fiori apps and backend services. Additionally, it addresses the application of SAP Fiori's security best practices, such as implementing HTTPS for network communication and utilizing SAP’s identity management solutions to manage user identities and access controls efficiently. Moreover, candidates are expected to demonstrate knowledge in monitoring and auditing SAP Fiori applications to identify and respond to security incidents, ensuring continuous improvement of the security posture of SAP Fiori applications. Achieving this certification indicates that the individual has a deep understanding of how to develop SAP Fiori applications with a strong security foundation, making them invaluable to organizations looking to enhance their SAP application landscapes' security. This credential is particularly valuable for SAP Fiori application developers, security consultants, and IT professionals involved in the secure design, development, and deployment of SAP Fiori applications, emphasizing their commitment to creating secure and resilient SAP solutions.and user engagement.managed.	

5) SAP Certified Technology Associate - SAP Business Technology Platform The The SAP Certified Technology Associate - SAP Business Technology Platform certification with a focus on security aspects is tailored for IT professionals who seek to validate their expertise in securing applications, data, and services on the SAP BTP. This certification assesses a candidate's proficiency in implementing and managing security features within the SAP BTP environment, highlighting the importance of identity and access management (IAM) for managing user identities, authentication, and authorization. It delves into data protection and privacy by emphasizing the need for data encryption, anonymization, and compliance with global data protection regulations. Additionally, it covers network and communication security, ensuring secure connections between SAP BTP and other systems or services, and underscores the significance of security monitoring and compliance through the use of SAP BTP's tools to detect and mitigate security threats. The certification also focuses on the application of security best practices for developing secure applications, including secure coding practices and vulnerability management. Achieving this certification signifies that an individual has a comprehensive understanding of security measures on the SAP Business Technology Platform, ensuring the safeguarding of applications and data against potential security threats. This credential is especially relevant for security specialists, cloud architects, developers, and IT administrators tasked with the secure design, deployment, and operation of applications on SAP BTP.efficiently. 6) SAP Certified Technology Specialist - SAP S/4HANA Conversion and SAP System Upgrade The Oracle Exadata Database Machine X9M Implementation Essentials certification (Exam Number: 1Z0-902) targets professionals involved in the setup, configuration, and maintenance of the Oracle Exadata Database Machine. This certification ensures candidates have a detailed understanding of the Exadata Database Machine features and capabilities, with a specific focus on implementing solutions that leverage its high performance and scalability for optimal database operations. While the certification comprehensively covers Exadata's architecture, software, and hardware components, it also includes aspects of security essential for safeguarding data and operations.	

Candidates should understand how to implement Exadata security features, including database encryption, secure configuration, and administration practices that protect against unauthorized access and ensure data integrity. Knowledge of network isolation, storage security, and compliance with security best practices specific to Exadata environments is also crucial. This certification is vital for professionals looking to demonstrate their expertise in deploying and managing Oracle Exadata Database Machine environments with a keen understanding of maintaining high security and performance standards. 7) SAP Certified Technology Associate - SAP Solution Manager Mandatory and Managed System Configuration The SAP Certified Technology Associate - SAP Solution Manager Mandatory and Managed System Configuration certification, emphasizing security components, is aimed at IT professionals who specialize in configuring and managing SAP Solution Manager with a strong focus on implementing security measures. This certification validates the candidate's expertise in setting up SAP Solution Manager to monitor and manage the security of SAP and non-SAP systems within an enterprise's landscape. This certification covers the essential security aspects of configuring SAP Solution Manager, including setting up secure communication channels between SAP Solution Manager and managed systems, ensuring that monitoring and alerting mechanisms are in place for security-related events, and implementing best practices for access control to safeguard sensitive system configuration and performance data. It also focuses on the importance of maintaining compliance with internal and external security policies and regulations through the configuration and use of SAP Solution Manager. Candidates are tested on their ability to configure SAP Solution Manager for optimal security, including the management of users and authorizations, the secure setup of technical monitoring and alerting infrastructure, and the deployment of security patches and updates. Additionally, the certification examines the candidate's knowledge of integrating SAP Solution Manager with other security tools and platforms to enhance the overall security posture of the SAP system landscape.	

Achieving this certification demonstrates that the individual possesses a thorough understanding of how to leverage SAP Solution Manager for managing system configurations, with a keen emphasis on implementing and maintaining robust security measures to protect against potential threats and vulnerabilities in the SAP environment. This certification is particularly valuable for system administrators, SAP technology consultants, and security specialists tasked with the secure configuration and management of SAP systems.environments. 8) SAP Certified Application Associate - SAP BusinessObjects Business Intelligence Platform The The SAP Certified Application Associate - SAP BusinessObjects Business Intelligence Platform certification, with a focus on security aspects, is designed for professionals aiming to validate their skills in deploying, managing, and securing SAP BusinessObjects BI solutions. This certification underscores the importance of implementing robust security measures to ensure the integrity, confidentiality, and availability of data and analytics provided by the SAP BusinessObjects Business Intelligence platform. In this certification, candidates are evaluated on their ability to configure security settings within the SAP BusinessObjects Business Intelligence platform, emphasizing the creation and management of secure access and authentication methods to protect sensitive business data. It covers critical security topics such as managing user rights and access levels, securing data connections, and implementing data encryption to safeguard information during transmission and at rest. The certification also delves into the best practices for configuring and managing the platform's security features, including the administration of security domains, the application of security patches, and the monitoring of security-related events within the system. Additionally, it addresses the importance of compliance with data protection regulations and how SAP BusinessObjects Business Intelligence platform can be configured to meet these requirements. Achieving this certification signifies that the individual has a comprehensive understanding of the security features and best practices necessary for managing the SAP BusinessObjects Business Intelligence platform. It	

demonstrates the individual's capability to ensure that the platform is not only optimized for performance and scalability but also secured against potential threats and vulnerabilities, making them a valuable asset to organizations that rely on SAP BusinessObjects for their business intelligence needs. This certification is particularly relevant for BI administrators, security analysts, and IT professionals responsible for the secure deployment and management of SAP BusinessObjects environments. 9) SAP Certified Application Associate - SAP Ariba Procurement The SAP Certified Application Associate - SAP Ariba Procurement certification, with an emphasis on security aspects, targets professionals seeking to demonstrate their skills in the secure configuration and management of SAP Ariba Procurement solutions. This certification focuses on the candidate's ability to ensure the security and integrity of procurement processes and data within the SAP Ariba platform. This certification covers the essential security measures required to protect sensitive procurement data, including configuring secure access controls, managing user permissions, and ensuring that data transmission and storage comply with best practices for data encryption and privacy. It also emphasizes the importance of implementing robust authentication mechanisms to verify the identity of users accessing the SAP Ariba system, thereby preventing unauthorized access and potential data breaches. Candidates are assessed on their understanding of how to apply security policies within SAP Ariba Procurement to meet compliance requirements and adhere to corporate governance standards. This includes the management of supplier and buyer information, securing confidential procurement transactions, and safeguarding against fraud and cyber threats. Moreover, the certification examines the individual’s knowledge of monitoring and reporting capabilities within SAP Ariba Procurement for identifying and responding to security incidents promptly, ensuring the continuity and reliability of procurement operations. Achieving this certification signifies that the individual is proficient in navigating the security landscape of SAP Ariba Procurement, capable of implementing and	

managing security measures that protect the organization's procurement activities. This credential is highly relevant for procurement specialists, system administrators, and IT security professionals involved in the secure deployment and operation of SAP Ariba Procurement solutions, ensuring that procurement processes are not only efficient but also secure from potential vulnerabilities and threats.	

2.1.13 GITHUB Education

While GitHub Education provides an invaluable set of resources and tools for learning and teaching software development and version control, it's important to note that it does not offer certifications. The program is focused on providing educational resources and tools rather than certifying skills or knowledge in GitHub or any specific technology. Therefore, participants should consider GitHub Education as a means to enhance their learning and development experience in the field of software engineering and computer science, rather than as a pathway to obtaining formal certification.

2.1.14 EC-Council

EC-Council is a cybersecurity certification, education, training, and services company based in Albuquerque, New Mexico.

It invented the Certified Ethical Hacker. Founded in 2001 in response to 9/11, EC-Council's mission is to provide the training and certifications apprentice and experienced cybersecurity professionals need to keep corporations, government agencies and others who employ them safe from attack.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different trainings, certificates, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited Organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified 10,000 professionals across the globe. Trusted by seven of the Fortune 10, half of the Fortune 100, and the intelligence communities of 140 nations, EC-Council is the gold standard in cybersecurity education and certification.

A truly global organization with a driving belief in bringing diversity, equity and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia. The company can be reached online at www.eccouncil.org/.

EC-Council's mission is to "create a better, safer world through awareness and education." They create courseware and certifications in a variety of security topics including the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) and Licensed Penetration Tester (LPT) programs.

This quick reference guide will highlight the various certification tracks to help you find your path through the EC-Council programs.

EC-Council breaks their certification programs up into six tracks, each one focusing on a different element of cybersecurity.

The six tracks are:

1. Foundation
2. Vulnerability Assessment and Penetration Testing
3. Cyber Forensics

4. Network Defense and Operations
5. Software Security
6. Governance

FOUNDATION CERTIFICATIONS

The Foundation Track was designed for computer users. It provides foundational training on cybersecurity awareness and basic security knowledge. It consists of three certifications. The Foundation Track was designed for computer users. It provides foundational training on cybersecurity awareness and basic security knowledge. It consists of three certifications.

- CSCU - Certified Secure Computer User

CSCU is an introductory certification to basic security awareness and fundamental security knowledge. It will help prove that you can limit your exposure to the common threats that users face online like identity theft, e-mail hoaxes, hacking and social engineering attacks, among others.

- ECSS - EC-Council Certified Security Specialist

ECSS continues where CSCU left off by testing your knowledge of information security. Specifically, you will be expected to understand how to protect data against confidentiality, integrity and availability attacks as well as utilizing proper access control to keep data secure.

- ECES - EC-Council Certified Encryption Specialist

ECES will prove your knowledge of the field of cryptography. You will be expected to demonstrate your understanding of the various encryption algorithms as well as how these ciphers are used in Information Technology such as disk encryption and VPNs. With the knowledge gained from studying for this certification, you will be better prepared to select and deploy appropriate encryption technology for your organization.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING CERTIFICATIONS

This track is one of the most well-known EC-Council tracks. These certifications focus on the defensive and offensive sides of security testing to reduce your attack surfaces. This track consists of four certifications.

- CND - Certified Network Defender
  - CND is designed for network administrators to learn how to make their networks more resilient against attacks and to detect and respond to intrusions. Essentially, this is a defensive security certification.
  - **Related training**: CND - Certified Network Defender

- CEH - Certified Ethical Hacker
  - CEH is designed for security experts to learn the hacking techniques of real threat actors so they can better prepare for the threats and identify the vulnerabilities before they are exploited. Essentially, this is an offensive security certification. Once you achieve the CEH certification, you can pursue the title of CEH Master by completing a practical evaluation that tests your skills in real-world situations.
  - **Related training**: CEH - Certified Ethical Hacker v11

- CPENT – Certified Penetration Testing Professional
  - CPENT is designed to test your penetration testing expertise. With this certification, you prove that you have what it takes to bypass the perimeter security of an enterprise network, pivot into other subnetworks, design exploits, and ultimately defend your enterprise from these attack techniques. Successfully passing this certification at a 90% or higher also gives you the LPT Master certification.

- LPT - Licensed Penetration Tester
  - This 18-hour long practical examination is designed to separate the masters from everyone else. You will be required to demonstrate mastery in advanced pen-testing techniques and tools in real-life scenarios. It is an intensive exam designed to push you and prove that you have what it takes to do penetration testing in the real world.

CYBER FORENSICS CERTIFICATIONS

The Cyber Forensics track is designed to train and certify professionals to investigate cyberattacks and collect evidence securely, often to present in a court of law to prosecute a cybercriminal. This track starts with Core certifications CND and CEH (see above). You would then proceed with the following advanced certifications.

- CTIA - Certified Threat Intelligence Analyst
  - CTIA is a “comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence” including planning and reporting on threat intelligence as well as addressing all stages of the Threat Intelligence Life Cycle.

Advanced

- ECIH - EC-Council Certified Incident Handler
  - ECIH requires a strong understanding of the nine stages of incident handling to minimize the impacts and loss following security incidents in the enterprise.
- CHFI - Computer Hacking Forensic Investigator
  - Whether your goal is to work for law enforcement or to help an organization with internal investigations and audits, CHFI will prove your knowledge of the forensic process, including evidence gathering, data recovery and analysis.
  - Related training: CHFI - Computer Hacking Forensic Investigator v9

NETWORK DEFENSE AND OPERATIONS CERTIFICATIONS

The Network Defense and Operations track is focused on the ability to defend the network from threats by doing proper incident response and disaster recovery. The Core of the NDO track includes CND (see above) but also has advanced-level certifications, including CTIA and ECIH (see above).

Core

- CSA - EC-Council Certified SOC Analyst
  - The SOC is one of the most important teams in an enterprise security program. They are on the front lines of incident response monitoring and triaging alerts to catch security incidents before they do any damage. This certification, perfect for Tier 1 and Tier 2 analysts, shows that you have the know-how to function in a dynamic enterprise-level Security Operations Center with an entry-level or intermediate-level skillset. A good

candidate for this exam will understand log management and correlation, SIEM deployment, advanced incident detection, and incident response.

Advanced

- EDRP - EC-Council Disaster Recovery Professional
  - When disaster strikes your organization, you must rely on skilled execution of Business Continuity and Disaster Recovery plans. EDRP is a certification that validates a candidate’s ability to plan, strategize, implement, and maintain a BCP and DRP.

SOFTWARE SECURITY CERTIFICATIONS

In today’s world where everything is available online, it’s never been more important than it is now to secure web applications. However, there is a significant drought of security-focused application developers. In this track, emphasis is given to the importance of developing applications with security as part of the design rather than as an afterthought or add-on.

To complete this track, you would start with CND and CEH (see above), and end with CPENT and LPT (see above). In between are two certifications focused specifically on two common web application technologies, Java and .Net.

- CASE Java - Certified Application Security Engineer Java
  - The CASE Java certification tests the knowledge and skills of a developer to implement security throughout the Software Development Life Cycle (SDLC), specifically with the Java application platform.
- CASE .Net - Certified Application Security Engineer .Net
  - Like CASE Java, CASE .Net tests the knowledge and skills of a developer to implement security throughout the SDLC, specifically with the .Net application platform.

GOVERNANCE CERTIFICATIONS

The governance track is focused on security leadership through the CCISO-Certified Chief Information Security Officer.

This certification is broken into five domains:

1. Governance
2. Security Risk Management, Control, and Audit Management
3. Security Program Management and Operations
4. Information Security Core Competencies
5. Strategic Planning, Finance, and Vendor Management.

The goal of this certification is to give the security executive the skills to strategically lead the security efforts of his or her organization and ensure that those security efforts stay in line with the overall business strategies and objectives.

POPULAR EC-COUNCIL TRAINING

Enrolling in formal training classes immerses you in a learning environment designed to help you rapidly develop the critical skills and concepts, as well as certification prep. As a multi-time EC-Council Training Center of the Year award winner, our class quality is recognized by EC-Council. Our courses are led by expert instructors with real-world experience. You practice applying what you learn with virtual, hands-on labs and collaborate with fellow IT professionals.

- Certified Network Defender
- Certified Ethical Hacker
- Computer Hacking Forensic Investigator
- Cybersecurity Certification Training

2.2 EU Certification Bodies

2.2.1 ENISA

ENISA contributes to the development and promotion of European cybersecurity certification schemes and standards. By providing guidance on certification processes, ENISA indirectly influences the skills and training required for compliance with these schemes. ENISA is responsible to implement the Cybersecurity Act[11].

ENISA recognized the necessity in Europe for a holistic strategy that outlines a defined set of roles and skills pertinent to the cybersecurity domain. In response, ENISA undertook the creation of the European Cybersecurity Skills Framework (ECSF), marking a crucial advancement in Europe’s digital landscape.

The European Cybersecurity Skills Framework (ECSF) serves as a practical resource designed to assist in identifying and describing the tasks, competencies, skills, and knowledge linked to the roles of cybersecurity professionals in Europe. It stands as the European Union's benchmark for delineating and evaluating pertinent skills, aligning with the specifications outlined in the recently introduced Cybersecurity Skills Academy by the European Commission.

Comprising 12 profiles, the ECSF condenses cybersecurity-related roles, delving into the specifics of their respective responsibilities, skills, synergies, and interdependencies. This framework promotes a shared understanding of the key roles, competencies, skills, and knowledge essential in the field of cybersecurity. Moreover, it facilitates the recognition of cybersecurity skills and aids in the development of training programs related to cybersecurity.

ENISA is not a certification body, it is not directly involved in issuing cybersecurity certifications. However, ENISA plays a crucial role in supporting and promoting European cybersecurity certification efforts, standards, and frameworks. Here's how ENISA is generally involved:

Development of Frameworks and Guidelines: ENISA contributes to the development of European cybersecurity certification frameworks and guidelines. This includes providing guidance on best practices, standards, and methodologies that can be adopted by certification bodies and organizations offering cybersecurity training.

Support for European Cybersecurity Certification Schemes: ENISA supports the establishment and recognition of European cybersecurity certification schemes. These schemes aim to provide a common framework for assessing and certifying the cybersecurity capabilities of products, services, and professionals.

Promotion of European Cybersecurity Certification: ENISA actively promotes the adoption of European cybersecurity certification among member states, industry stakeholders, and relevant organizations. This promotion includes raising awareness about the importance of certifications in enhancing cybersecurity resilience.

Collaboration with Stakeholders: ENISA collaborates with various stakeholders, including industry, academia, and member states, to ensure that cybersecurity certification initiatives align with the evolving needs of the European cybersecurity landscape. This collaboration helps in the development of effective and relevant certification programs.

[11] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Provision of Resources and Information: ENISA provides resources, reports, and information related to cybersecurity certifications. These resources aim to assist organizations and individuals in understanding the importance of certifications and navigating the available frameworks.

Involvement in Policy Discussions: ENISA participates in policy discussions at the EU level related to cybersecurity certifications. This involvement includes providing expertise and recommendations to policymakers on the development and improvement of certification initiatives.

While ENISA does not directly issue certifications, its role is instrumental in creating a conducive environment for the development, recognition, and adoption of cybersecurity certifications in Europe.

2.2.2 EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION ACADEMY

2.2.3 European Cyber Security Organisation (ECSO)

European Cybersecurity Organisation (ECSO)[12], established in 2016, ECSO was formed as the contractual counterpart to the European Commission, entrusted with the implementation of Europe's distinctive Public-Private Partnership in Cybersecurity, known as cPPP (2016-2020). Evolving from the success of the cPPP, ECSO currently stands as the exclusive European cross-sectoral and independent membership organization dedicated to cybersecurity. It brings together and advocates for a collaborative approach among various European public and private stakeholders in the field of cybersecurity. ECSO's diverse membership encompasses large corporations, SMEs, startups, research centers, universities, end-users, operators of essential services, clusters, associations, as well as local, regional, and national public administrations across the European Union Member States and the European Free Trade Association (EFTA).

ECSO is primarily focused on fostering cooperation and collaboration among various cybersecurity stakeholders rather than directly providing cybersecurity certifications. ECSO plays a key role in bringing together public and private entities, including large companies, SMEs, research centers, universities, and others, to collectively address cybersecurity challenges in Europe.

While ECSO itself does not administer cybersecurity certifications, it may play an indirect role in the broader ecosystem by supporting initiatives, projects, or partnerships that contribute to the development of cybersecurity skills and expertise. It is essential to note that the specific activities and initiatives of organizations like ECSO may evolve over time.

2.2.4 European Union Agency for Law Enforcement Training (CEPOL)

CEPOL[13] is the agency of the European dedicated to develop, to implement and to coordinate training for law enforcement officials. CEPOL’s headquarters are located in Budapest, Hungary.

The following table summarises our findings regarding the training schemes which are offered by the organisation. These schemes span across several thematic areas.

[12] https://ecs-org.eu/who-we-are/#

[13] https://www.cepol.europa.eu/

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
CEPOL's training schemes span across the following thematic areas:[14] **a) Counter-Terrorism** Aiming at preventing radicalisation, enhancing information exchange, cutting off terrorist financing and addressing the phenomenon of foreign terrorist fighters, among others. **b) Cybercrime and cyber-related crime** The rapidly increasing digitalisation of society and the economy, as well as the emergence of technologies such as blockchain, the Internet of Things and the increased use of Artificial Intelligence, create new vulnerabilities that call for the strengthening of law enforcement officials' digital skills. **c) Fundamental rights and data protection** Reinforcing the protection of fundamental rights in law enforcement work cannot be achieved through training alone, but training is an essential component in achieving this goal. Fundamental rights is a cross-cutting element that should be integrated in each and every training activity. **d) Higher education and research** CEPOL recognises the importance of transferring, within the law enforcement community, scientific evidence and research-based insights and findings from the academic to the professional sphere. **e) Law enforcement cooperation, information exchange and interoperability** To combat cross-border crimes and terrorism, law enforcement authorities of different EU countries must cooperate effectively. Large-scale IT systems are crucial for successful cross-border cooperation. CEPOL raises awareness and strengthens the knowledge of law enforcement officials on EU	CEPOL aims to consistently deliver training and services that meet its stakeholders 'expectations while complying with the high-quality requirements for learning services outside formal education, including all life-long learning, as defined by the **ISO 29993:2017** standard. Moreover, CEPOL ensures compliance with the agency's internal control standards and the internationally recognised management standard ISO 9001:2015, which sets out the criteria for a quality management system. In terms of courses and seminars, CEPOL maintains an evaluation system covering the first three levels of the Kirkpatrick Model, a globally recognised method of evaluating the results of training and learning programs, measuring the satisfaction with the activity, the knowledge obtained, and the detailed benefits of the training activity on a personal level (enhanced job performance). The fourth level of the Kirkpatrick Model is partially assessed at CEPOL by looking at the organisational impact evidenced by concrete examples through post-course evaluation.[15]

[14] https://www.cepol.europa.eu/thematic-areas/

[15] https://www.cepol.europa.eu/training-education/training-quality-standards

information sharing systems for security and border management, cooperation tools and other support mechanisms available to Member States. **f) Law enforcement technologies, forensics, and specific areas** Law enforcement officials use a wide array of methods, techniques and tools to combat crimes. Law enforcement technologies are advancing, with innovative solutions appearing every day. Under this thematic area, CEPOL provides specific practical and theoretical knowledge on several pivotal topics. **g) Leadership, training and other skills** Enhancing leadership performance and strengthening the competencies of law enforcement decision-makers is of paramount importance. CEPOL's offer in this area helps officials build managerial skills and increase foreign language abilities, and contributes to improve the effectiveness and the quality of law enforcement training in the EU. **h) Public order and prevention** CEPOL contributes to fostering a relationship of trust between the police and society in today's EU and to improving the prevention and detection of crimes by facilitating the exchange of good investigative methods and community policing practices. **i) Serious and organised crime** Serious and organised crime represents a significant threat to the safety of EU citizens, businesses and institutions and undermines the rule of law. Criminals easily operate across borders, which creates a need for consistent European–level action.	

2.2.5 EUROPOL

In 2013, Europol established the European Cybercrime Centre (EC3) aiming to strengthen the law enforcement response to cybercrime in the European Union and thus to help protect European citizens, businesses, and governments from online crime.

From an operational standpoint, EC3 focuses on the following types of cybercrimes:

a) Cyber-dependent crime;
b) Child sexual exploitation; and
c) Payment fraud.

Among its objectives, EC3 supports training and capacity-building initiatives, in particular for the relevant authorities in Member States.

As a key part of Europol's mission in ensuring the development and maintaining of required capacities.

In 2010, Europol together with the European Commission and the EU Member States established the European Union CYBERCRIME TASK FORCE (EUCTF). Membership of the EUCTF is comprised of the Heads of the National Cybercrime Units from the various member states as well as representatives from Europol, the European Commission, Eurojust and CEPOL. EC3 provides a permanent secretariat service to support the work of the EUCTF and the Board.

Among its objectives, EUCTF oversees training development activities.[16]

The following table summarises our findings regarding the training courses which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
The training that EC3 offers includes courses on open-source IT forensics, some of which use material developed by the European Cybercrime Training and Education Group (ECTEG). Others include representatives from the industry as keynote speakers and workshop facilitators. EC3 also offers courses on: **a)** Payment fraud; **b)** Payment card fraud forensic; and **c)** Combating the online sexual exploitation of children. The rapid development of cybercrime demands a quick and effective response from law enforcement across Europe. Part of EC3's mission in this connection is two-fold: **a)** To help train law enforcement authorities in the latest methods of combating cybercrime; and **b)** To ensure that all such authorities across the EU have full access to the tools they need to fight cybercrime effectively. To these ends, the EC3 works closely with CEPOL, and with the European Cybercrime Training and Education Group (ECTEG) and other partners. Some courses are also open to law enforcement authorities outside the EU.	

[16] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf

Course offerings on tackling cybercrime Among the courses that EC3 has offered under the aforementioned rubrics are the following: - a course at the Spanish National Police Academy in Avila on open-source IT forensics; - a course in Selm, Germany, that offered training on combatting child sexual exploitation and that was offered by Focal Point Twins, a team of specialists in EC3 that helps combat all forms of criminal online behaviour against children; - a course on payment fraud forensics and investigations at the Spanish National Police Academy; - in close cooperation with Germany's Federal Criminal Police Office, a course for forensic experts on examining skimming devices.[17]	

2.2.6 European Cybercrime Training and Education Group (ECTEG)

The European Cybercrime Training and Education Group (ECTEG) is a Belgium-registered International Non-Profit Association (AISBL), composed of European Union and European Economic Area Member States law enforcement agencies, international bodies, academia, private industries, and experts.

The European Union supported "Falcone" project[18], which recommended the creation of a suite of Europe-wide Cybercrime Investigator training courses at introductory, intermediate and advanced levels.

Europol agreed to act as the coordinating body in 2007 and created the European Working Group on the Hamonisation of Cybercrime Investigation Training to support its efforts. The primary aim of the working group is to provide experience and knowledge to further enhance the coordination of cybercrime training, by identifying opportunities to build the capacity of countries to combat cybercrime through the development and delivery of a robust and enduring training programme. The working group changed its name on the 11th of November 2009 to "European Cybercrime Training and Education Group" (ECTEG).

The ECTEG is funded by the European Commission and working in close cooperation with Europol-EC3 and CEPOL, both members of the advisory group. Their activities aim to:

- Support international activities to harmonise cybercrime training across international borders.
- Share knowledge, expertise and find training solutions.
- Promote standardisation of methods and procedures for training programmes and cooperation with other international organisations.

[17] https://www.europol.europa.eu/operations-services-and-innovation/services-support/training-and-capacity-building

[18] JAI/2001/Falcone/127 – "Training Cybercrime Investigation – building a platform for the future"

- Collaborate with academic partners to establish recognised academic qualification in the field of cybercrime and work with universities that have already created such awards making them available across international borders.
- Collaborate with industry partners to establish frameworks whereby their existing and future efforts to support law enforcement by the delivery of training, harmonised into an effective programme that makes best use of available resources.

The ECTEG provides training and education material and reference trainers to international partners, supporting their efforts to train law enforcement on cybercrime issues globally. The following table summarises our findings regarding the training courses which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
All courses that have been developed for ECTEG are freely available for law enforcement organisations. The courses include the following properties: **a)** Expertise: each course is designed by a team of subject matter experts; **b)** Internationality: all courses are developed for an international audience; **c)** Tested: all courses have at least run once in pilot training. Some key characteristics of ECTEG course development standards are as follows: - Start with an analysis of feedback from other existing training courses including non ECTEG ones; - List skills and competencies addressed, describing links with TCF profiles whenever possible. Relevant certification process materials can be included as a dedicated work package; - Deliver trainer manual based on ECTEG template. ECTEG training materials include but are not limited to:[19] - Apple File System Forensics - Digital Forensics Examiner – introductory course - Live Data Forensics - Online Investigator project - Dark web and virtual currencies basic	ECTEG course development follows standards as provided by Europol, CEPOL, Eurojust, ENISA and ENFSI.[22]

[19] https://www.ecteg.eu/course-packages/

[22] https://www.ecteg.eu/course-packages/

- E-First : First responders e-learning package
- Linux as an Investigative Tool, part 1
- Linux as an Investigative Tool, part 2
- Python programming for investigators
- Malware Investigations
- Core Skills in Mobile Phone Forensics
- Intermediate Mobile Phone Forensics
- Network Investigations
- Network Forensic Intermediate Course
- Internet Investigations
- Wireless LAN & VOIP Investigations
- Windows Forensics
- Windows File Systems Advanced Forensics
- Mac Forensics Course
- Solid State and other Storage media Forensic
- Data Mining and Databases
- Forensic Scripting using Bash.

From November 2017 and thanks to EU funding, ECTEG coordinates and funds projects led by members. Projects are prioritised by the members, with a final decision from Law Enforcement supported by the advisory group, where EUROPOL and CEPOL are permanently represented.

Among on-going projects, the Global Cybercrime Certification project is connected to the topic of cybersecurity certification.

Global Cybercrime Certification Project[20]

In 2014, the Training of Trainers (TOT) project was funded by the European Union and managed by the Universidad Autónoma de Madrid, to improve efficiency, cooperation and mutual understanding of the main actors involved in the fight against cybercrime; Law Enforcement Agencies and Prosecutors. One of the goals was to create a framework for the certification of European Cybercrime Investigators and Cybercrime European Prosecutors to establish the basis for the development of a group of professionals with the ability to deal properly with transnational problems of cybercrime.

The project explores the fact that currently no EU standards for training and certification exist.

According to a Resolution 2017/2068(INI) from the European Parliament dated 3 October 2017, future trends in cybercrime require an increasing level of

[20] https://www.ecteg.eu/running/gcc/

expertise from practitioners, it welcomes the fact that existing initiatives such as ECTEG the TOT Project and the training activities under the EU Policy Cycle framework are already paving the way towards addressing the expertise gap at EU level.[21] Now, the **Global Cybercrime Certification Project** (i.e. TOT Project) funded by **ECTEG** provides an opportunity to implement the work done in the TOT Project **creating an international certification framework based on the Training Competency Framework for Cybercrime (TCF)** to enable Law Enforcement Agents and Judicial Authorities to develop their knowledge and skills and to enhance confidence within the criminal justice system of their jurisdiction as well as international investigations. **Objective and expected outcomes of the TOT project** The three main objectives of this project are to seek sustainability of this certification system, to develop certification requirements for the roles of **"Head of Cybercrime Unit"**, **"Online Investigator"**, **"Digital Forensic Examiner"** and **"Judicial Authorities dealing with Cybercrime Investigations"**, as well as to and to deliver pilots for the target LEAs and Judicial Authorities.	

2.2.7 European Security and Defence College (ESDC)

Within the framework of the Common Foreign and Security Policy (CFSP), the European Security and Defence College (ESDC)[23] offers training and education at the EU level, specifically focusing on the Union's Common Security and Defence Policy (CSDP). The goal is to foster a shared comprehension of CSDP among both civilian and military personnel and to recognize and share effective practices related to various CSDP matters through its training initiatives. In this manner, the ESDC supplements the training and educational endeavors undertaken at the national level.

While ESDC may not issue certifications in the same way as some other training programs, it is involved in developing the knowledge and skills of individuals in the field of CSDP. The specifics of certification processes or the recognition of training achievements by ESDC may vary depending on the nature of the training programs and courses offered. Certification and recognition of completion might be granted in collaboration with relevant national authorities or in accordance with the standards set by the European Union.

[21] Article 71, Resolution 2017/2068(INI), European Parliament, 3 October 2017 (https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.html?redirect)

[23] https://esdc.europa.eu/who-we-are/

2.2.8 European External Action Service (EEAS)

The European External Action Service (EEAS) is the European Union's diplomatic service. Since 2011, the EEAS carries out the EU's Common Foreign and Security Policy to promote peace, prosperity, security, and the interests of Europeans across the globe.

The following table summarises our findings regarding the activities and guidance which are offered by the organisation.

Stakeholders	
End-user viewpoint	Certification scheme viewpoint
The EEAS, through its Strategic Compass initiative,[24] provides further guidance on strengthening the EU's ability to prevent, deter and respond to cyber-attacks. The EU is determined to promote and protect a global, open, stable, and secure cyberspace for everyone to have a safe digital experience. Increased cybersecurity is essential for the EU to become a resilient, green, and digital Union. According to the EU Cybersecurity Strategy, resilience, technological sovereignty and EU leadership must be further increased, mainly through the development of operational capacity to counter malicious cyber-activities and the promotion of cooperation for a global and open cyberspace. Through its External Cyber Capacity building, the EU Cybersecurity Strategy plans to increase cyber resilience & capacities of partners to investigate and prosecute cybercrimes. [25]	

2.2.9 European Association for Quality Assurance in Higher Education (ENQA)

The European Association for Quality Assurance in Higher Education (ENQA)[26] was first established in 2000 as the European Network for Quality Assurance in Higher Education to promote European cooperation in the field of quality assurance in higher education. In 2004, it became the European Association for Quality Assurance in Higher Education with the aim to contribute to the maintenance and enhancement of the quality of European higher education, and to act as a major driving force for the development of quality assurance across all the Bologna Process signatory countries.

ENQA members are higher education quality assurance agencies based in the European Higher Education Area. In order to become a member of ENQA, agencies must demonstrate their compliance with the Standards and Guidelines for Quality Assurance in the EHEA (ESG). The Standards and

[24] https://www.eeas.europa.eu/eeas/strategic-compass-eu-0_en
[25] https://www.eeas.europa.eu/eeas/cybersecurity_en
[26] https://www.enqa.eu/

guidelines for quality assurance in the European Higher Education Area provide the framework for internal and external quality assurance. These standards and guidelines are divided into three parts:

1. Internal quality assurance
2. External quality assurance
3. Quality assurance agencies

The Standards and Guidelines for Quality Assurance in the EHEA (ESG) are designed to be applied to all higher education, regardless of place or mode of delivery. The Standards set out the agreed and accepted practice, while the Guidelines describe how the standards might be implemented, however this will vary depending on the context.

The ENQA and its member agencies do not provide any standards and guidelines for professional training.

2.2.10 European Cybersecurity Competence Centre and Network

The European Cybersecurity Competence Centre and Network (ECCC)[27] is addressing cybersecurity skills in a dedicated working group. One of the main objectives of the Network and the Centre is to align the high educational programmes and certifications in all cybersecurity sectors (such as network security, cloud security, hardware security) and provide a comprehensive matrix that matches skills and workforce. It will be a continuous effort of the Network and the Centre to build comprehensive curricula and training programmes addressing industrial needs covering all cybersecurity sectors.

2.3 Member-States' Certification Bodies

2.3.1 Hellenic Authority for Higher Education (HAHE) (Greece)

The Hellenic Authority for Higher Education (HAHE)[28] was established in 2020 as the successor to Greece's Quality Assurance and Accreditation Agency, which had operated since 2006. The Authority is an independent body with full administrative and operational autonomy and a legal supervision by the Minister of Education. It is governed by its President and Supreme Council. Quality assurance is managed by the Evaluation and Accreditation Council. HAHE is a member of the European Association for Quality Assurance in Higher Education (ENQA).

The standards, procedures, and criteria issued by HAHE are in line with national legislation and the European Standards and Guidelines of the European Higher Education Area (ESG 2015).

In a nutshell, HAHE provides **(1) Evaluation** of the work performed by institutions is performed in two stages: **(a)** internal evaluation carried out by institutions themselves, and **(b)** external evaluation carried out by a panel of independent experts under the supervision of the HAHE, and **(2) Accreditation** as an external evaluation process based on specific, predetermined, internationally accepted quantitative and qualitative criteria and indicators that have been published in advance and are in line with the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG 2015).

2.3.2 AEQES • Agency for Quality Assurance in Higher Education (Belgium)

The Agency for the Evaluation of Quality in Higher Education (AEQES) is an independent body responsible for quality assurance in higher education within its jurisdiction. Established to promote and evaluate the quality of higher education institutions, AEQES operates with a mission to ensure that educational offerings meet both national and international standards of excellence.

[27] https://cybersecurity-centre.europa.eu/
[28] https://www.ethaae.gr/en/

AEQES's operations are guided by principles of transparency, autonomy, and stakeholder involvement, ensuring that its processes are inclusive and accountable. The agency conducts its quality assurance activities through a dual approach:

Internal Evaluation: Institutions conduct self-assessments to scrutinize their academic programs, research activities, governance, and student services. This self-reflective process is aimed at identifying strengths and areas for improvement, fostering a culture of continuous quality enhancement within institutions.

External Evaluation: Following the internal evaluation, AEQES coordinates peer reviews by panels of independent experts. These experts, including international participants to ensure a broader perspective, conduct site visits and thorough assessments of the institutions and their programs against predefined criteria. This external evaluation culminates in a report that highlights commendations, recommendations for improvement, and, where applicable, areas requiring immediate action.

The standards, procedures, and criteria used by AEQES are aligned with the overarching frameworks of national legislation and the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG 2015). This alignment ensures that the quality assurance process not only meets local needs but also harmonizes with broader European expectations, facilitating mutual recognition and mobility within the higher education sector.

AEQES is a member of the European Association for Quality Assurance in Higher Education (ENQA) and participates actively in the European Quality Assurance Register for Higher Education (EQAR), reflecting its commitment to maintaining the highest standards of quality assurance in higher education. Through its rigorous evaluation and accreditation processes, AEQES plays a pivotal role in enhancing the quality and international standing of higher education institutions within its remit.[29]

2.3.3 NEAA National Evaluation and Accreditation Agency (Bulgaria)

The National Evaluation and Accreditation Agency (NEAA) is a pivotal institution in Bulgaria, dedicated to ensuring the highest standards of quality in higher education. Established as an independent entity, the NEAA operates with the primary mandate to evaluate, accredit, and assure quality across higher education institutions (HEIs) within the country. This agency is instrumental in adopting a comprehensive criteria system, internal procedures, and standards, all underpinned by Bulgarian law. Its funding sources include the state budget and fees from HEIs for accreditation procedures, ensuring operational autonomy while maintaining accountability to both the Ministry of Education and the broader public through transparent dissemination of accreditation results.

Governed by a structured management system, the NEAA features two key levels of oversight: the Accreditation Council, appointed by the Prime Minister, and eight Standing Committees focused on various study fields, each appointed by the Accreditation Council. This structure facilitates a broad coverage across the national higher education landscape, guaranteeing the reliability and integrity of accreditation decisions. Moreover, the NEAA's commitment to fostering a quality culture within the Bulgarian higher education system is evident through its engagement in information sharing, consultation, and active stakeholder participation.

As a member registered with the European Quality Assurance Register for Higher Education (EQAR), the NEAA aligns with international quality assurance standards, underscoring its dedication to excellence and the internationalization of Bulgarian higher education. This alignment not only enhances the domestic educational landscape but also positions Bulgarian HEIs within the broader context of the European Higher Education Area (EHEA).[30]

[29] https://aeqes.be/english_about_us.cfm

[30] https://www.enqa.eu/membership-database/neaa-national-evaluation-and-accreditation-agency/#

2.3.4 NAB National Accreditation Bureau for Higher Education (Czech Republic)

The National Accreditation Bureau for Higher Education (NAB) in the Czech Republic serves as the cornerstone of the country's commitment to maintaining and enhancing educational quality and standards in higher education. This esteemed body, established to oversee accreditation processes, operates with a keen focus on upholding the integrity, excellence, and international competitiveness of Czech higher education institutions.

Structured to function with independence yet under the strategic guidance of the Czech Ministry of Education, Youth, and Sports, the NAB embodies a comprehensive approach to quality assurance. It employs a dual-system of evaluation, encompassing both internal assessments conducted by HEIs and rigorous external evaluations executed by panels of independent experts. This ensures a holistic view of institutional performance against nationally and internationally recognized criteria and standards.

The NAB's operations are characterized by transparency, inclusivity, and a commitment to continuous improvement. By publishing its criteria, procedures, and accreditation outcomes, it fosters an environment of trust and accountability. Moreover, the NAB actively participates in the European Higher Education Area (EHEA), adhering to the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG 2015). This not only aligns Czech higher education with European norms but also facilitates the international mobility of students and the mutual recognition of qualifications.

In essence, the NAB is dedicated to ensuring that Czech higher education institutions not only meet the required standards of quality and excellence but also strive for innovation and improvement, thus contributing to the development of a knowledge-based society both nationally and internationally.[31]

2.3.5 AI The Danish Accreditation Institution (Denmark)

The Danish Accreditation Institution (AI) stands as a central figure in Denmark's higher education landscape, dedicated to ensuring the quality and relevance of higher education in the country. Established as an autonomous institution, AI operates under the auspices of the Danish Ministry of Higher Education and Science, embodying the national commitment to excellence in education through rigorous accreditation and quality assurance processes.

AI's approach to accreditation encompasses a comprehensive review of higher education institutions (HEIs) and their programs, focusing on both academic standards and the relevance of programs in meeting the demands of the labor market. This dual focus ensures that Danish HEIs not only provide high-quality education but also prepare graduates for successful careers. The institution's methodology includes both internal self-assessments by HEIs and external evaluations by panels of experts, fostering a culture of continuous improvement and accountability in the Danish higher education sector.

A key feature of AI's operations is its emphasis on internationalization, recognizing the importance of global standards and cooperation in higher education. AI actively engages in dialogue and partnerships with international accreditation bodies, ensuring that its processes and criteria are in line with global best practices. This international outlook not only elevates the quality of Danish higher education but also facilitates the mobility of students and the recognition of Danish qualifications abroad.[32]

[31] https://www.enqa.eu/membership-database/nab-national-accreditation-bureau-for-higher-education/

[32] https://www.enqa.eu/membership-database/ai-the-danish-accreditation-institution/

2.3.6 ACQUIN Accreditation, Certification and Quality Assurance Institute (Germany)

The Accreditation, Certification and Quality Assurance Institute (ACQUIN) is a prominent quality assurance agency in Germany, focusing on the accreditation of study programs and HEIs across the country and internationally. As a member of the German Accreditation Council, ACQUIN operates with a commitment to enhancing the transparency, comparability, and quality of higher education, aligning with European standards and guidelines.

ACQUIN's accreditation process is characterized by a rigorous evaluation of study programs against predefined criteria that encompass curriculum content, teaching methodologies, faculty qualifications, and the availability of resources. This ensures that programs not only meet academic standards but also address the needs and expectations of students and the broader society. ACQUIN's procedures involve a thorough review by peers, including academics and professionals from the relevant fields, ensuring a balanced and fair assessment of program quality.

A distinctive aspect of ACQUIN's work is its holistic approach to quality assurance, which extends beyond program accreditation to include institutional audits and the development of quality culture within HEIs. By doing so, ACQUIN contributes to the continuous improvement of higher education institutions, encouraging them to adopt innovative practices and to remain responsive to the evolving demands of the knowledge economy.[33]

ACQUIN also emphasizes international cooperation, working closely with partner institutions and networks worldwide to promote the international compatibility and recognition of German higher education qualifications. This global engagement is crucial for fostering academic mobility and enhancing the international competitiveness of German HEIs.

2.3.7 HAKA Estonian Quality Agency for Education (former EKKA) (Estonia)

The Estonian Quality Agency for Higher Education (HAKA), formerly known as EKKA, is a key pillar in Estonia's higher education system, tasked with the enhancement and assurance of educational quality across Estonian higher education institutions (HEIs). As an autonomous body, HAKA operates under the principles of impartiality and transparency, conducting thorough evaluations of both institutional management and specific study programs to ensure they meet national and international quality standards.

HAKA's accreditation process is designed to be comprehensive, involving a detailed review of the institution's internal quality assurance processes, academic programs, and overall governance. This evaluation not only assesses compliance with established criteria but also encourages continuous improvement and innovation in teaching, learning, and research. By involving a mix of local and international experts in its panels, HAKA ensures that Estonian higher education remains competitive and aligned with global educational trends and standards.

Additionally, HAKA plays a significant role in promoting the internationalization of Estonian higher education. Through its work, the agency facilitates the mobility of students and academics, ensuring that Estonian qualifications are recognized globally. This effort supports Estonia's vision of creating an open and collaborative educational environment that attracts talent from across the world.[34]

2.3.8 QQI • Quality and Qualifications Ireland (Ireland)

Quality and Qualifications Ireland (QQI) is responsible for maintaining the standards of education and training in Ireland, encompassing higher education, further education, and training. As a statutory body, QQI advocates for the enhancement of quality across Ireland's education sector and is instrumental in

[33] https://www.acquin.org/en/

[34]https://www.enqa.eu/membership-database/ekka-estonian-quality-agency-for-higher-and-vocational-education/

the development of the National Framework of Qualifications (NFQ), a system designed to classify and assure the quality of qualifications in the country.

QQI's approach to quality assurance includes the validation of programs, the review of providers, and the establishment of quality guidelines that education and training providers must adhere to. This ensures a consistent and high level of educational experience for learners, facilitating both personal and professional development. QQI also engages in the international recognition of Irish qualifications, enhancing the mobility and employability of Irish graduates abroad.

One of QQI's key strengths is its comprehensive oversight across various sectors of education, allowing for a holistic approach to quality assurance and qualification recognition. This broad mandate supports the creation of seamless pathways between different levels and types of education, ensuring that learners can progress effectively through the education system in Ireland and beyond.[35]

2.3.9 ANECA • National Agency for Quality Assessment and Accreditation of Spain (Spain)

The National Agency for Quality Assessment and Accreditation of Spain (ANECA) is a cornerstone of Spain's strategy to ensure and improve the quality of higher education. Established as an independent foundation, ANECA's mission is to contribute to the continuous enhancement of the quality of the higher education system through the evaluation, certification, and accreditation of teachings, professors, and institutions.

ANECA's methodology is grounded in transparency, objectivity, and participation, employing a range of evaluation programs designed to assess various aspects of higher education provision. This includes program accreditation, institutional evaluation, and faculty assessment, ensuring comprehensive coverage of the factors that contribute to educational quality. ANECA's activities are guided by both national priorities and the European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), promoting alignment with international best practices.

A significant focus of ANECA's work is on fostering the internationalization of Spanish higher education, enhancing the global mobility of students and the international recognition of Spanish degrees. Through its commitment to quality assurance and accreditation, ANECA plays a pivotal role in supporting the adaptability and competitiveness of Spain's higher education institutions in the face of global educational challenges.[36]

2.3.10 CTI • Commission des Titres d'Ingénieur (France)

The Commission des Titres d'Ingénieur (CTI) is the authoritative body in France charged with the evaluation and accreditation of higher education institutions offering engineering degrees. Established to ensure the highest standards in engineering education, CTI's mandate includes the periodic review of engineering programs to guarantee they meet stringent educational and professional requirements. This ensures that graduates are well-prepared to enter the engineering profession, not only in France but also on an international level.

CTI's accreditation process is comprehensive, involving an assessment of program content, teaching methods, faculty qualifications, research activity, and the integration of industry trends and needs. A unique aspect of CTI's approach is its emphasis on continuous improvement, encouraging institutions to innovate and adapt their programs in response to evolving technological and industrial landscapes.

[35] https://www.qqi.ie/

[36] https://www.enqa.eu/membership-database/aneca-national-agency-for-quality-assessment-and-accreditation-of-spain/

Furthermore, CTI plays a crucial role in the internationalization of French engineering education. It works closely with international partners and participates in global networks to ensure the mutual recognition of degrees, facilitating the mobility of French engineers and students worldwide. This global perspective underscores France's commitment to maintaining an engineering education system that is competitive, dynamic, and aligned with international standards.[37]

2.3.11 ASHE • Agency for Science and Higher Education (Croatia)

The Agency for Science and Higher Education (ASHE) in Croatia plays a vital role in maintaining the quality and integrity of higher education in the country. Operating independently with administrative autonomy, ASHE ensures adherence to national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), ASHE is committed to upholding international quality assurance standards. The agency conducts comprehensive evaluations, including both internal assessments by institutions and external evaluations facilitated by independent panels of experts under ASHE's supervision. Accreditation, an essential aspect of ASHE's mandate, entails an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure accountability, transparency, and alignment with European quality assurance standards.[38]

2.3.12 ANVUR • National Agency for the Evaluation of Universities and Research Institutes (Italy)

The National Agency for the Evaluation of Universities and Research Institutes (ANVUR) in Italy is a key institution responsible for ensuring the quality and standards of higher education and research in the country. Operating independently with administrative autonomy, ANVUR ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), ANVUR is committed to upholding international quality assurance standards. The agency conducts both internal evaluations by institutions and external evaluations facilitated by independent panels of experts under ANVUR's supervision. Accreditation, a pivotal aspect of ANVUR's mandate, involves an external evaluation process based on predefined criteria and indicators. These criteria are transparently communicated in advance to ensure fairness, consistency, and alignment with European quality assurance standards.[39]

2.3.13 CYQAA • Cyprus Agency of Quality Assurance and Accreditation in Higher Education (Cyprus)

The Cyprus Agency of Quality Assurance and Accreditation in Higher Education (CYQAA) plays a pivotal role in ensuring the quality and integrity of higher education in Cyprus. Established with full administrative autonomy, CYQAA operates independently while adhering to national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), CYQAA is committed to upholding international quality assurance standards. The agency conducts both internal evaluations by institutions and external evaluations facilitated by independent panels of experts under CYQAA's supervision. Accreditation, a key aspect of CYQAA's mandate, involves an external evaluation process based on predefined criteria

[37] https://www.enqa.eu/membership-database/cti-commission-des-titres-dingenieur/

[38] https://www.enqa.eu/membership-database/ashe-agency-for-science-and-higher-education/

[39]https://www.enqa.eu/membership-database/anvur-national-agency-for-the-evaluation-of-universities-and-research-institutes/

and indicators. These criteria are transparently communicated in advance to ensure consistency, fairness, and alignment with European quality assurance standards.[40]

2.3.14 AIC • Academic Information Centre (Latvia)

In Latvia, the Academic Information Center (AIC) is essential to upholding high standards in the nation's higher education system. AIC maintains administrative autonomy while operating independently to guarantee adherence to both national laws and European Standards and Guidelines (ESG 2015). AIC is committed to maintaining global quality assurance standards as a member of the European Association for Quality Assurance in Higher Education (ENQA). Under the direction of AIC, the center is in charge of both external evaluations carried out by impartial expert panels and internal assessments carried out by institutions. One of the core components of AIC's goal is accreditation, which involves an external assessment procedure using predetermined standards and metrics. To guarantee responsibility, openness, and compliance with European quality assurance standards, these requirements are disclosed in a transparent manner beforehand.[41]

2.3.15 SKVC • Centre for Quality Assessment in Higher Education (Lithuania)

The Centre for Quality Assessment in Higher Education (SKVC) in Lithuania plays a crucial role in maintaining the quality and integrity of higher education in the country. Operating independently with administrative autonomy, SKVC ensures adherence to national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), SKVC is committed to upholding international quality assurance standards. The center conducts comprehensive evaluations, including both internal assessments by institutions and external evaluations facilitated by independent panels of experts under SKVC's supervision. Accreditation, a central aspect of SKVC's mandate, involves an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure fairness, consistency, and alignment with European quality assurance standards.[42]

2.3.16 Comité d'accréditation pour les formations du brevet de technicien supérieur (Luxembourg)

The country's higher education standards and quality are guaranteed by the Comité d'accréditation pour les formations du brevet de technicien supérieur en Luxembourg. The committee, which functions autonomously and has administrative authority, guarantees adherence to both national laws and European Standards and Guidelines (ESG 2015). The committee is committed to maintaining global quality assurance standards as a member of the European Association for Quality Assurance in Higher Education (ENQA). It is in charge of both external evaluations carried out by independent expert panels under its direction and internal evaluations carried out by institutions. A key component of the committee's mandate is accreditation, which entails an external review procedure using predetermined standards and metrics. To guarantee responsibility, openness, and compliance with European quality assurance standards, these requirements are disclosed in a transparent manner beforehand.[43]

[40]https://www.enqa.eu/membership-database/cyqaa-cyprus-agency-of-quality-assurance-and-accreditation-in-higher-education-2/

[41] https://www.enqa.eu/membership-database/aic-academic-information-centre/

[42] https://www.enqa.eu/membership-database/skvc-centre-for-quality-assessment-in-higher-education/

[43]https://www.enqa.eu/membership-database/comite-daccreditation-pour-les-formations-du-brevet-de-technicien-superieur/

2.3.17 MAB • Hungarian Accreditation Committee (Hungary)

The Hungarian Accreditation Committee (MAB) is instrumental in maintaining high standards of higher education in Hungary. Operating with administrative autonomy, MAB ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), MAB upholds international quality assurance standards. The committee oversees both internal evaluations conducted by institutions and external evaluations facilitated by independent panels of experts under MAB's supervision. Accreditation, a core function of MAB, involves an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure fairness, consistency, and alignment with European quality assurance standards.[44]

2.3.18 MFHEA • Malta Further and Higher Education Authority (Malta)

In order to guarantee the integrity and quality of further and higher education in Malta, the Malta Further and Higher Education Authority (MFHEA) is essential. With administrative autonomy and independent operation, MFHEA guarantees adherence to both national laws and European Standards and Guidelines (ESG 2015). MFHEA is dedicated to maintaining global quality assurance standards as a member of the European Association for Quality Assurance in Higher Education (ENQA). Under the direction of MFHEA, the authority supervises both external evaluations carried out by impartial panels of experts and internal reviews carried out by institutions. One of the main responsibilities of MFHEA is accreditation, which entails an external review procedure using predetermined standards and metrics. To guarantee responsibility, openness, and compliance with European quality assurance standards, these requirements are disclosed in a transparent manner beforehand.[45]

2.3.19 Inspectorate of Higher Education in the Netherlands (Netherlands)

The Inspectorate of Higher Education in the Netherlands plays a pivotal role in maintaining high standards and quality assurance in higher education. Operating independently with administrative autonomy, the inspectorate ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), the inspectorate is committed to upholding international quality assurance standards. It conducts comprehensive evaluations, including both internal assessments by institutions and external evaluations facilitated by independent panels of experts under the inspectorate's supervision. Accreditation, a fundamental aspect of the inspectorate's mission, entails an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure fairness, consistency, and alignment with European quality assurance standards.[46]

2.3.20 AQ Austria Agency for Quality Assurance and Accreditation Austria (Austria)

The Agency for Quality Assurance and Accreditation Austria (AQ Austria) is instrumental in ensuring the quality and standards of higher education in Austria. Operating independently with administrative autonomy, AQ Austria ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), AQ Austria upholds international quality assurance standards. The agency oversees both internal evaluations conducted by institutions and external evaluations facilitated by independent

[44] https://www.mab.hu/

[45] https://mfhea.mt/

[46] https://www.enqa.eu/membership-database/inspectorate-of-higher-education-in-the-netherlands/

panels of experts under AQ Austria's supervision. Accreditation, a core function of AQ Austria, involves an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure accountability, transparency, and alignment with European quality assurance standards.[47]

2.3.21 PKA • Polish Accreditation Committee (Poland)

The Polish Accreditation Committee (PKA) is essential in maintaining high standards and quality assurance in higher education in Poland. Operating with administrative autonomy, PKA ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), PKA is committed to upholding international quality assurance standards. The committee oversees both internal evaluations conducted by institutions and external evaluations facilitated by independent panels of experts under PKA's supervision. Accreditation, a pivotal aspect of PKA's mandate, involves an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure fairness, consistency, and alignment with European quality assurance standards.[48]

2.3.22 A3ES • Agency for Evaluation and Accreditation of Higher Education (Portugal)

The Agency for Evaluation and Accreditation of Higher Education (A3ES) in Portugal plays a critical role in ensuring the quality and integrity of higher education in the country. Operating independently with administrative autonomy, A3ES ensures compliance with national legislation and European Standards and Guidelines (ESG 2015). As a member of the European Association for Quality Assurance in Higher Education (ENQA), A3ES upholds international quality assurance standards. The agency conducts comprehensive evaluations, including both internal assessments by institutions and external evaluations facilitated by independent panels of experts under A3ES's supervision. Accreditation, a central aspect of A3ES's mandate, involves an external evaluation process based on predefined criteria and indicators. These criteria are communicated transparently in advance to ensure accountability, transparency, and alignment with European quality assurance standards.[49]

2.3.23 ARACIS • Agency for Quality Assurance in Higher Education (Romania)

The Agency for Quality Assurance in Higher Education (ARACIS) in Romania plays a crucial role in maintaining the quality and standards of higher education within the country. Founded as the successor to the Romanian National Council for Academic Evaluation and Accreditation in 1994, ARACIS was formally established in 2005 through a Government Emergency Ordinance. Its primary mission is to conduct external evaluations of the educational offerings provided by higher education institutions and other organizations offering higher education study programs in Romania.

As an autonomous public institution of national interest, ARACIS is funded through evaluation fees and project funds. It is tasked with various evaluation activities, including provisional authorization to operate, accreditation procedures, and periodic evaluations for study programs, institutional evaluations, and evaluations in the domains of master and doctoral studies. Notably, ARACIS also holds the authority to award the EUR-ACE® Label for engineering study programs as a member of the European Network for Accreditation of Engineering Education (ENAEE), underlining its commitment to upholding high standards in engineering education specifically.

[47] https://www.aq.ac.at/de/

[48] https://pka.edu.pl/

[49] https://www.a3es.pt/en/about-a3es

ARACIS is a member of the European Association for Quality Assurance in Higher Education (ENQA) and is registered in the European Quality Assurance Register for Higher Education (EQAR), affirming its adherence to the European Standards and Guidelines (ESG) for quality assurance in higher education. This membership and registration highlight ARACIS's commitment to international quality assurance standards and its role in enhancing the global recognition and validity of Romanian higher education qualifications.[50] [51]

2.3.24 SQAA • Slovenian Quality Assurance Agency for Higher Education (Slovenia)

The Slovenian Quality Assurance Agency for Higher Education (SQAA), also known as NAKVIS, is a pivotal entity in the Slovenian education system, dedicated to ensuring the quality of higher education within Slovenia. Established in 2010, SQAA operates independently with a mandate to uphold professionalism, impartiality, legality, and political neutrality, in alignment with the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). As a member of prominent organizations such as the European Association for Quality Assurance in Higher Education (ENQA), the European Quality Assurance Register for Higher Education (EQAR), and the European Consortium for Accreditation (ECA), SQAA contributes significantly to the international recognition and validity of Slovenian higher education.

SQAA's operations encompass the accreditation and external evaluation of higher education institutions (HEIs) and study programs, ensuring they meet both national criteria and European standards. The agency's role includes developing principles and procedures for quality assessment in collaboration with stakeholders, thereby adopting decisions on accreditations and evaluations that affect the overall quality of education provided by HEIs in Slovenia. This process involves a rigorous assessment based on self-evaluation reports prepared by the institutions, which are then examined by the agency to establish compliance with the required standards.[52]

2.3.25 SAAHE • Slovak Accreditation Agency for Higher Education (Slovak Republic)

The Slovak Accreditation Agency for Higher Education (SAAHE) plays a pivotal role in the Slovak higher education landscape, focusing on quality assurance and accreditation in line with European standards. Established to enhance the performance of Slovak higher education institutions, SAAHE's efforts are aligned with the European Standards and Guidelines (ESG 2015), emphasizing its commitment to upholding high-quality education standards. The agency has initiated significant reforms, including the "New Approach to Higher Education Accreditation," part of a broader Renewal Plan aimed at improving Slovak higher education's quality and performance.

One of SAAHE's key achievements is the development and implementation of new accreditation standards that have raised the bar for the delivery of study programs and the internal quality assurance systems within higher education institutions. This reform has led to a considerable reduction in the number of study programs, with institutions eliminating or adapting programs to meet the new, stringent criteria. The aim is to ensure that education provided is of high quality, student-oriented, and meets the socio-economic needs of the community.

SAAHE's strategy for the coming years includes detailed plans for thematic analyses, reports, and the continuous improvement of the internal quality assurance system. The agency is poised to assess the internal quality systems of higher education institutions, with a focus on involving international

[50] https://www.enqa.eu/membership-database/aracis-agency-for-quality-assurance-in-higher-education/

[51] https://www.eqar.eu/register/agencies/agency/?id=17

[52] https://www.nakvis.si/about-sqaa/?lang=en

reviewers, students, and external stakeholders in the review process to ensure comprehensive and balanced evaluations.[53]

2.3.26 FINEEC • Finnish Education Evaluation Centre (Finland)

The Finnish Education Evaluation Centre (FINEEC) is recognized as a key independent governmental agency in Finland, dedicated to the comprehensive evaluation of education across all levels, from early childhood to higher education. Established to consolidate the evaluation activities of several previous bodies in May 2014, FINEEC operates with a commitment to maintaining and enhancing the quality and effectiveness of the Finnish education system. Its broad mandate covers the assessment of educational outcomes, quality audits of educational institutions, and thematic evaluations, aimed at supporting educational providers and stakeholders in their continuous improvement efforts.

FINEEC's approach to evaluation emphasizes enhancement-led evaluations, focusing not just on meeting predefined standards but on fostering continuous development within institutions. This method ensures that evaluations contribute constructively to the educational landscape, helping institutions to align with both national objectives and the broader European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG).

In higher education specifically, FINEEC carries out quality audits, thematic evaluations, and accreditations of engineering degree programmes, offering a Quality Label for Excellence to institutions that meet its rigorous standards. This label, valid for six years, signifies an institution's adherence to both European principles and national criteria for quality management in higher education[54]

2.3.27 UKÄ • The Swedish Higher Education Authority (Sweden)

The Swedish Higher Education Authority (UKÄ) is an autonomous governmental body responsible for overseeing the quality of higher education and research in Sweden. It carries out this mandate through a range of activities including legal supervision, quality assurance, and the compilation of official statistics on higher education. UKÄ's quality assurance process is thorough, involving evaluations of higher education institutions (HEIs) and research to ensure high standards beneficial for students, employers, and society. Moreover, UKÄ has the authority to review and grant degree-awarding powers to public-sector institutions, further ensuring the educational standards are maintained across the country. The agency operates under a public service agreement issued annually by the government, which outlines targets and funding, and it may receive additional specific assignments throughout the year. UKÄ also provides administrative support to The Higher Education Appeals Board and The Higher Education Expulsions Board, contributing to its comprehensive role in the Swedish higher education system.[55]

2.4 EU Initiatives towards harmonising the EU’s Cybersecyrity Training Certification landscape

In tandem with the international, EU, and member-states’ certification bodies previously presented, EU initiatives play a crucial role in shaping the cybersecurity training certification landscape. As part of broader efforts to harmonize cybersecurity education and certification practices, these EU initiatives aim to establish unified standards and frameworks. This subsection delves into the initiatives spearheaded

[53] https://saavs.sk/en/

[54] https://www.karvi.fi/en

[55] https://www.uka.se/swedish-higher-education-authority

by the EU, examining their impact on the certification landscape and their alignment with CyberSecPro's objectives.

All the following endeavours are instrumental in defining a common European framework for cybersecurity certification, aligning with the broader objectives of CyberSecPro, as they share a commitment to advancing cybersecurity education, standardization, and workforce development within the European context. Through its dedicated efforts, CyberSecPro seeks to contribute valuable insights and solutions to refine and strengthen the certification standards and practices set forth by the existing work by focusing on the self-development of the students and/or professionals, bridging the gap between the knowledge and skills earned by universities and those required by the industry. This way it ensures a more comprehensive and aligned approach to cybersecurity training and certification in the European context.

2.4.1 European Cybersecurity Skills Framework (ENISA)

European Cybersecurity Skills Framework (ECSF) is a practical tool to support the identification and articulation of tasks, competences, skills, and knowledge associated with the roles of European cybersecurity professionals. It is the EU reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy, which was recently announced by the European Commission. The ECSF summarises the cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge mostly required in cybersecurity, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes.

2.4.2 Concordia

Concordia [https://www.concordia-h2020.eu] is a Horizon-2020 project, which constitutes a noteworthy EU initiative in the realm of cybersecurity training and certification. Concordia represents a collaborative effort involving industry, academia, and research organizations, with the overarching goal of establishing a European Cybersecurity Competence Network. The Concordia project concentrates on cybersecurity education, aiming to establish a skills certification scheme tailored for the European Cybersecurity Consultant profile. It also seeks to furnish information about courses for cybersecurity professionals and develop methodologies to assist high-school teachers in discussing cybersecurity with their students [https://www.cyberwatching.eu/projects/1484/concordia]. It also focuses on sharing cybersecurity scenarios, best practices, and creating a European threat intelligence platform to enhance information sharing among academic, industrial, and other organizations, including the European cybersecurity emergency response team (CERT).

2.4.3 CyberSec4Europe

CyberSec4Europe [https://cybersec4europe.eu], a European Commission pilot project with 43 partners from 22 EU countries, focuses on designing, testing, and demonstrating governance structures for a future European Cybersecurity Competence Network [50]. The project aligns with CERN's concept and best practices and leverages the expertise of its partners. Within Work Package 6, “Cybersecurity Skills and Capability Building” [https://cybersec4europe.eu/work-packages/work-package-6-cybersecurity-skills-and-capability-building/], various deliverables related to cybersecurity professional education have been accomplished. These include a review of European Cyber Security Massive Open Online Courses (MOOCs), an education and training review of university-based European MSc programs in cybersecurity, the design of an education and professional framework, cybersecurity exercises, and the development of a European-based cybersecurity education and assessment framework [“D6.2 Education and Training Review.” https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf] [Karinsalo Anni, Halunen Kimmo, “Design of Education and Professional Framework.” CyberSec4Europe https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf] [“D6.4 Flagship 1.” https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf] [“D6.5 Flagship 2.” https://cybersec4europe.eu/wp-content/uploads/2022/04/D6.5-

Flagship-2-v1.3_submitted.pdf]. The overarching goal is to consolidate and enhance cybersecurity capabilities to safeguard European democracy and the integrity of the single digital market, with specific policy, technical, and innovation objectives.

2.4.4 Sparta

SPARTA ["SPARTA D9.1 Cybersecurity Skills Framework." https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf], an EU-funded cybersecurity project initiated in 2019, focuses on developing a comprehensive cybersecurity workforce skills framework and curriculum. The project aims to address the cybersecurity skills gap by tailoring the NIST's NICE framework [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf] to accommodate EU-specific considerations, particularly the General Data Protection Regulation (GDPR) [https://eur-lex.europa.eu/eli/reg/2016/679/oj]. The SPARTA Cybersecurity Skills Framework (S-CSF) maintains the structural representation of NICE but introduces adaptations to align with EU legal and regulatory landscapes. Notable modifications include incorporating the GDPR Data Protection Officer (DPO) role and adjusting Cyber Policy and Strategy Planner roles to Cyber Privacy Policy and Strategy Planner. S-CSF ensures conformity with EU regulations while retaining the knowledge, skills, and abilities outlined in the NICE framework.

2.4.5 ECHO

ECHO ["D2.6 ECHO CYBERSKILLS FRAMEWORK." Accessed: Apr. 05, 2023. [Online]. Available: https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf] is a pilot project of the European Commission focused on developing a common European cybersecurity strategy. Comprising 30 partners from diverse sectors, ECHO aims to strengthen the EU's cyber defense and technological sovereignty through collaboration. The project addresses various themes, including governance, multi-sector assessment, cybersecurity skills framework, security certification, federated cyber range, and an early warning system. The ECHO cybersecurity skills framework (ECHO-CSF) provides a model for ICT and cybersecurity professionals, aligning with the NIST NICE framework function groups. The curriculum includes four training programs, and ECHO's outputs, such as the cybersecurity skills framework and federated cyber ranges, resonate well with CyberSecPro's objectives. The curriculum is designed to enhance the competencies of IT professionals in detecting, containing, assessing, and responding to cyber-attacks, with specific training programs tailored for the health, energy, and maritime sectors [Infocomm Media Devevelopment Authority, "Skills Framework For ICT." https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html].

2.4.6 Cybersecurity education maturity assessment

As can be seen from the initiatives above, educational maturity for cyber security has been a matter of particular concern in the EU in recent years. It is evident that there is a gap between HEIs and industry, as well as in terms of vertically specialized expertise and knowledge sharing in the field of cyber security. This gap is also brought to light by ENISA with the current procurement it announced [https://www.enisa.europa.eu/procurement/cybersecurity-education-maturity-assessment], which underscores key needs in enhancing cybersecurity education across EU Member States. The initiative aims to identify and implement maturity models for assessing cybersecurity in education, emphasizing a structured approach to evaluating readiness levels. Additionally, the project seeks to analyze the cybersecurity education maturity across Member States, highlighting the importance of understanding the current landscape. Recognizing the diversity of needs, there is an explicit focus on identifying and addressing specific requirements in each Member State based on their maturity level. The overarching vision involves collaborative efforts with the European Commission and Member States to implement a roadmap for cybersecurity education, creating tailored educational materials to promote basic cybersecurity and cyber hygiene principles across various age groups. This comprehensive approach aims to foster closer coordination and exchange of best practices in cybersecurity awareness and education throughout the EU.

2.5 EU Challenges in Certifying Cybersecurity Training

In this chapter, the political and policy related, legal, technical, standard-related, human-related challenges for the harmonisation, interoperability and compliance of cybersecurity training in EU are presented.

2.5.1 General Challenges and EU efforts

Providing certifications in cybersecurity training involves addressing various challenges due to the dynamic nature of the field and the evolving threat landscape. Some of the common challenges in offering cybersecurity certifications include:

Rapidly Changing Technology**:** Cybersecurity is a field that experiences rapid technological advancements. Certification programs need to stay current with the latest technologies, tools, and methodologies to ensure that professionals are equipped with relevant and up-to-date skills.

Diverse Specializations**:** Cybersecurity encompasses a wide range of specializations, including penetration testing, incident response, risk management, and more. Developing certifications that cover this diverse spectrum while maintaining depth in each area can be challenging.

Emerging Threats and Techniques**:** New cyber threats and attack techniques continuously emerge. Certification programs need to adapt to cover these emerging threats and teach professionals how to defend against the latest attack vectors.

Hands-On Experience**:** Cybersecurity is a hands-on field, and professionals require practical experience to effectively address real-world challenges. Developing certification programs that incorporate realistic, hands-on scenarios and practical assessments can be challenging but is crucial for ensuring the practical skills of certified individuals.

Global Relevance**:** Cybersecurity is a global concern, and certification programs need to be relevant on a global scale. Ensuring that certifications are recognized internationally and align with global standards is a challenge for certification providers.

Recognised global Certification Bodies**:** The acknowledgment and integrity of certification bodies. The cost, legal and standardisation global frameworks are challenges in this category. Ensuring that certifications are accessible and affordable to a diverse group of learners is a challenge for certification providers.

Balancing Theory and Practical Skills**:** Certifications should strike a balance between theoretical knowledge and practical skills. Professionals need both a solid understanding of cybersecurity concepts and the ability to apply them in real-world scenarios.

Evolving Certification Standards**:** Certification bodies often need to adapt their standards to reflect the changing needs of the industry. This involves regularly reviewing and updating certification content and exam objectives to keep pace with industry developments.

Accessibility**:** The cost of obtaining certifications can be a barrier for some SMEs, MEs, individuals, especially in regions with limited resources. Ensuring that certifications are accessible and affordable to a diverse group of learners is a challenge for certification providers.

Credibility and Trust**:** Building and maintaining credibility and trust in certification programs is essential. This involves having a transparent and rigorous certification process, ensuring that certified professionals meet high standards of competence and ethical conduct.

The European Union (EU) has been actively engaged in promoting cybersecurity awareness, skills development, and training through various policies and initiatives. Here are some key aspects of EU policies for cybersecurity training:

- ***European Cybersecurity Strategy***: The European Commission has established a European Cybersecurity Strategy that outlines measures to enhance the EU's collective resilience against cyber threats. This strategy emphasizes the importance of building a strong and skilled cybersecurity workforce.
- ***NIS Directive*** **(Directive on Security of Network and Information Systems):** The NIS Directive is a legislative framework aimed at ensuring a high common level of network and information systems security across the EU. It encourages member states to establish national strategies for the security of network and information systems, including measures to improve the skills and competencies of cybersecurity professionals.
- ***European Cybersecurity Competence Centre*** **(ECCC):** The EU established the European Cybersecurity Competence Centre to enhance the EU's cybersecurity capabilities. The center is expected to play a role in coordinating and supporting cybersecurity training and education initiatives at the EU level.
- ***Digital Education Action Plan***: The Digital Education Action Plan, part of the European Commission's Digital Education Action Plan, aims to boost digital skills and competencies. While not specific to cybersecurity, it includes provisions for promoting digital literacy and skills, which are essential components of a comprehensive cybersecurity training strategy.
- ***European Cybersecurity Month (ECSM):*** The EU actively supports the European Cybersecurity Month, an annual campaign promoting cybersecurity awareness and education. The campaign includes various activities and events to raise awareness about the importance of cybersecurity and encourage individuals and organizations to enhance their cybersecurity knowledge.
- ***EU Funding Programs***: The EU allocates funds to support research, development, and innovation in the field of cybersecurity. These funds may also be used to support training programs, educational initiatives, and the development of cybersecurity skills. (e.g. DEP).
- ***European Skills Agenda***: The European Skills Agenda aims to ensure that people develop the skills they need for the jobs of today and tomorrow. While not exclusively focused on cybersecurity, it acknowledges the importance of digital skills and lifelong learning, which are relevant to the evolving cybersecurity landscape.
- ***Collaboration with Industry and Academia***: The EU encourages collaboration between industry, academia, and other stakeholders to address the skills gap in cybersecurity. Partnerships with educational institutions, training providers, and industry associations are seen as crucial for building a skilled cybersecurity workforce.
- ***European Cybersecurity Skills Framework (ECSF)***, as mentioned above, summarises the cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies, and interdependencies.
- *The **EU Cyber Solidarity Act*** includes activities related to cybersecurity trainings.
- Establishing a **European Cyber Shield** based on a network of Security Operations Centers (SOCs) across EU Member States to identify and respond to cyberattacks. ECSO's advocacy for an EU-level SOC network, as outlined in a paper, informed the European Commission's drafting of the Cyber Solidarity Act.
- The ***Cybersecurity Skills Academy*** which aims to create a framework that consolidates public and private initiatives focused on cybersecurity skills, similar to the existing Women4Cyber Academy. The platform will assist individuals aspiring for cybersecurity careers by providing access to courses, scholarships, and certifications.
- Additionally, there is an amendment proposed for the Cybersecurity Act to establish a certification scheme for "managed security services." Two Council Recommendations are also proposed to support Member States in enhancing digital skills, addressing the deficiency in a holistic government approach to digital education and the overall scarcity of digital skills in society, leveraging the European Year of Skills.

3 Standards, Schemas, Criteria and Scales

In this chapter, different certifying, authorities may have their own unique criteria, standards, and processes for certification. Candidates seeking certification should carefully review the requirements and guidelines provided by the specific certifying authority for the certification they are interested in pursuing. The various standards, principles and processes are presented and assessed.

3.1 Factors & Standards

Certification authorities usually use different certification factors including:

1. **Knowledge Domains:** They define the specific areas of knowledge and skills that candidates must possess to be eligible for certification. These knowledge domains are typically aligned with industry best practices and standards.

2. **Experience and Education:** Many certifications require a combination of practical experience and formal education in cybersecurity or related fields. The certifying authorities may specify the minimum requirements for experience and education that candidates must meet.

3. **Examination Process:** Certifications often involve passing an examination that assesses the candidate's knowledge and skills. The certifying authorities design and administer these examinations, which may be in the form of multiple-choice questions, practical assessments, or a combination of both.

4. **Continuing Education:** Some certifications have requirements for ongoing professional development. Certified individuals may need to earn continuing education credits or participate in regular recertification activities to maintain their certification status.

5. **Ethical and Professional Conduct:** Certifying authorities typically expect certified professionals to adhere to a code of ethics and maintain professional conduct in their cybersecurity practice.

Several standardisation bodies organisations are working in standards, e.g.:

- European Telecommunications Standards Institute (ETSI).
- European Committee for Standardization (CEN).
- European Committee for Electrotechnical Standardization (CENELEC).
- International Organization for Standardization (ISO).
- International Telecommunication Union (ITU).
- Institute of Electrical and Electronics Engineers, International Electrotechnical Commission (IEC).

Figure 1 shows the ISO/IEC standards for learning, education, and training namely:

- ISO/IEC TR 20748-2:2017, Information technology for learning, education and training - Learning analytics interoperability.
- ISO/IEC 23126:2021, Information technology for learning, education and training - Ubiquitous learning resource organization and description framework.
- ISO/IEC 19788-1:2011, Information technology Learning, education and training - Metadata for learning resources.
- ISO/IEC 24751:2008, Information technology - Individualized adaptability and accessibility in e-learning, education and training.
- ISO/IEC TR 23842-2:2020, Information technology for learning, education, and training - Human factor guidelines for virtual reality content.
- ISO/IEC WD 29187-1, Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET).
- ISO/IEC TS 20748-3:2020, Information technology for learning, education and training - Learning analytics interoperability.

- ISO/IEC 2382-36:2019, Information technology - Vocabulary Part 36: Learning, education and training.
- ISO/IEC 17024:2012, Conformity assessment - General requirements for bodies operating certification of persons.
- ISO/IEC TS 17027:2014, Conformity assessment - Vocabulary related to competence of persons used for certification of persons.

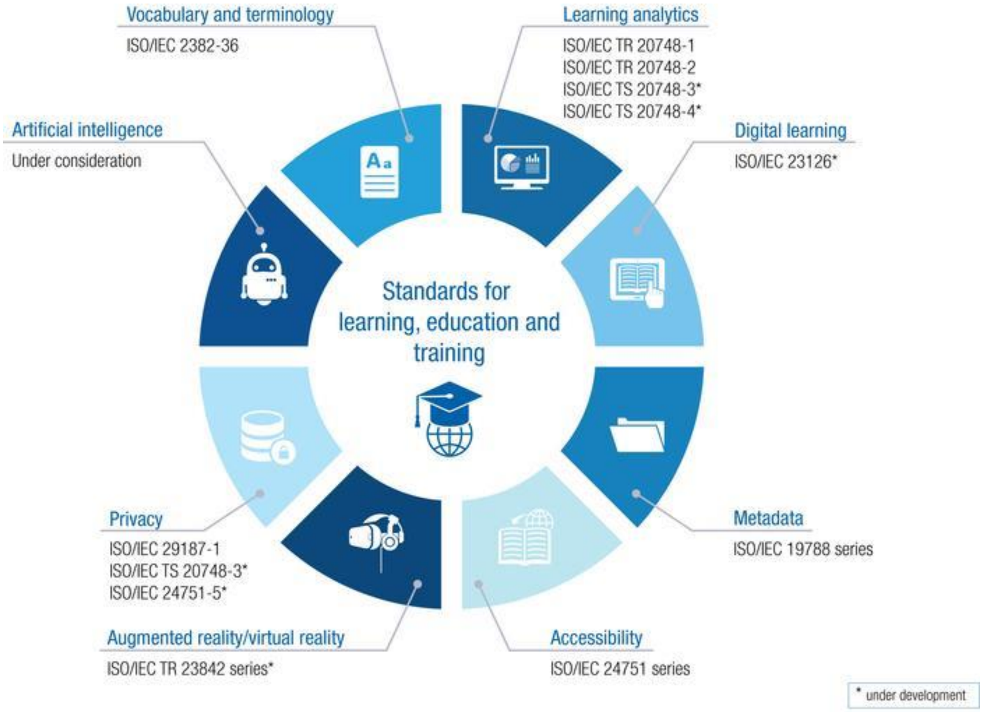


Figure 1. Standards for learning, education, and training[56]

The following service standards are available or in development. Although their titles specify “outside formal education”, most of the requirements they contain are equally valid in formal education.

- ISO 29993:2017, Learning services outside formal education – Service requirements.
- ISO 29991:2020, Language learning services - Requirements.
- ISO 29994:2021, Education and learning services - Requirements for distance learning.

The previous mentioned standards can be combined with the following new standards, which address various components of learning services.

- ISO 29992:2018, Assessment of outcomes of learning services – Guidance.
- ISO 29995:2021, Education and learning services – Vocabulary.

The possible options for learning service standards are also shown in *Figure 2*.

[56] https://www.iec.ch/blog/digital-learning-redefining-education

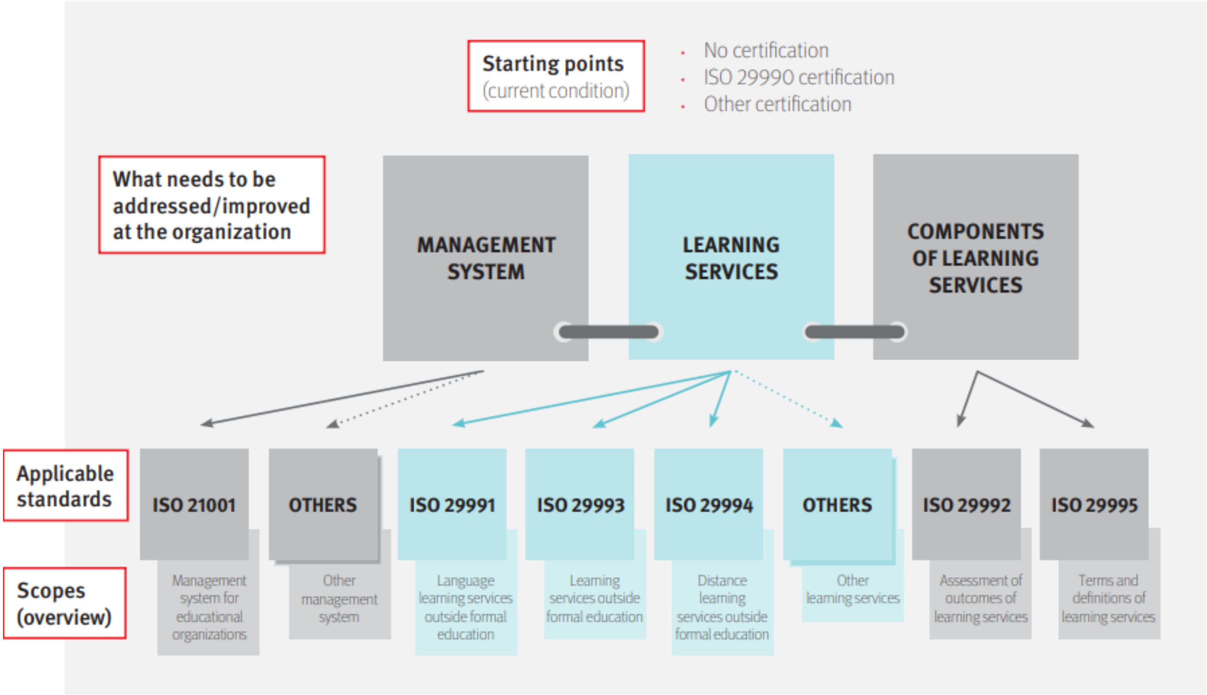

Starting points
(current condition)
No certification
ISO 29990 certification
Other certification
What needs to be addressed/improved at the organization
MANAGEMENT SYSTEM
LEARNING SERVICES
COMPONENTS OF LEARNING SERVICES
Applicable standards
Scopes (overview)
ISO 21001
OTHERS
ISO 29991
ISO 29993
ISO 29994
OTHERS
ISO 29992
ISO 29995
Management system for educational organizations
Other management system
Language learning services outside formal education
Learning services outside formal education
Distance learning services outside formal education
Other learning services
Assessment of outcomes of learning services
Terms and definitions of learning services

Figure 2. Possible options for standards for learning services57

3.2 Criteria & Schemas

3.2.1 Criteria for certifying cybersecurity professional trainings / modules

The criteria for certification of professional trainings, as previously assessed in Chapter 2, vary depending on the specific certification body or organization providing the training. However, there are some common elements and considerations that we identified:

***Relevance to Industry Standards*:** Professional training programs should align with industry standards and best practices. Certification bodies often ensure that the content and skills taught in the training are relevant to the current needs and expectations of the industry.

***Syllabus and Training material Quality*:** The syllabus/ training material of the training program should be comprehensive, well-structured, and cover the necessary topics targeting the sectors/objectives. It should provide a balance between theoretical knowledge and practical skills relevant to the profession.

Experienced Trainers: Certification programs typically require instructors or trainers with significant expertise and experience in the relevant field. Instructors should have a track record of success and be able to effectively communicate the material.

***Assessment and Evaluation*:** There should be a robust assessment mechanism in place to evaluate participants' understanding and application of the training content. This may include exams, practical assessments, or project work.

***Hands-On Experience*:** Practical, hands-on experience is a crucial aspect of professional training. Certification programs may require participants to apply their knowledge in real-world scenarios to demonstrate their practical skills.

[57] https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/ISO%2029990%20Briefing%20Notes.PDF

Duration and Intensity**:** The duration and intensity of the training program should be appropriate for the content being covered. Certification bodies may set standards for the minimum hours of instruction or the length of the training program.

Continuing Education and Renewal**:** Some certifications require individuals to engage in ongoing professional development to maintain their certification. This encourages professionals to stay current with industry trends and refresh their knowledge periodically.

Ethical Standards and Professional Conduct**:** Certification bodies often expect participants to adhere to ethical standards and professional conduct. This may include a commitment to honesty, integrity, and compliance with relevant laws and regulations.

Recognition and Accreditation**:** Certification programs that are recognized or accredited by relevant industry bodies or regulatory authorities may carry more weight. This recognition indicates that the program meets certain quality standards.

Accessibility and Inclusivity**:** Certification programs should be accessible to a diverse audience, and accommodations may be made for individuals with disabilities. Inclusivity in training materials and methods is an important criterion.

Feedback and Improvement**:** Certification bodies may consider feedback from participants to continuously improve the training program. This can involve regular evaluations of every module, reviews and updates to keep the content current and effective to the trainees and professions.

3.2.2 Cybersecurity Certification schemes for professional trainings

Referring to Chapter 2, based on the certification provided we can conclude that the term "cybersecurity scheme for training" can be broad, and it can refer to different aspects of cybersecurity training programs.

Some organizations or industry bodies develop cybersecurity certification schemes for training programs. These schemes outline the criteria and standards that training programs must meet to be recognized and certified. Certifications in cybersecurity often validate an individual's or organization's knowledge and skills in specific areas of cybersecurity.

A **general cybersecurity professional training scheme** may refer to a structured framework or curriculum or syllabus or modules designed to provide comprehensive training in various aspects of cybersecurity for specific sectors. This could include various modules needed in the market (or specific sectors) such as network security, threat detection, incident response, ethical hacking, and more.

Industry/Market-specific cybersecurity schemes may exist to set standards for a professional training program within a particular sector(s). These standards ensure that training aligns with industry/market sector best practices and addresses the unique challenges faced by organizations within that sector.

3.3 Scales

In this section, we describe the different scales/measurements/ which are used in the cybersecurity trainings (e.g., ECTS credits, mini credits, tokens, bonus, micro-credentials).

3.3.1 Credits in professional training modules and programmes

Credits in training programs/ modules typically refer to units or points awarded to participants upon completion of specific training activities. These credits serve as a measure of the individual's progress, achievement, or professional development. The types of credits can vary depending on the nature of the training and the accrediting or certifying body. Here are various types of credits commonly provided in professional trainings:

- **Continuing Education Units** (CEUs): CEUs are widely used in professional development and continuing education programs. One CEU is typically equivalent to ten hours of participation in an accredited program.

- **Continuing Professional Education** (CPE) Credits: CPE credits are commonly used in fields such as accounting, finance, and information technology. Professionals often need to earn a certain number of CPE credits annually to maintain their certifications.
- **Academic Credits**: Academic credits are associated with educational institutions and are often measured in semester hours or credit hours. They are commonly used in degree programs at colleges and universities. ECTS is widely used across European universities and has become a standard tool for facilitating the recognition of study achievements. It contributes to the harmonization and comparability of higher education systems within the European framework. CTS stands for European Credit Transfer and Accumulation System. It is a standard for comparing the study attainment and performance of students across the European Higher Education Area (EHEA) countries. ECTS facilitates the recognition of academic credits between different universities and countries, promoting student mobility and the flexibility of educational systems. The ECTS framework allows us to map credits to various factors, including learning objectives and learner outcomes. For instance, a network engineer might require less time to grasp cybersecurity infrastructure concepts due to their existing knowledge base. ECTS calculator can be found at: https://www.germangradecalculator.com/ects-calculator/.

  Key factors of ECTS include:

  - ✓ *Credit System*: ECTS operates on a credit system where academic programs are divided into individual course units or modules; each assigned a specific number of credits. Credits represent the workload required to complete a course successfully.
  - ✓ *Workload Definition*: One ECTS credit is generally equivalent to 25 to 30 hours of student workload, which includes lectures, seminars, independent study, exams, and other learning activities.
  - ✓ *Learning Outcomes*: ECTS emphasizes the definition of learning outcomes for each course or module. Learning outcomes describe what a student is expected to know, understand, and be able to do upon successful completion of a course.
  - ✓ *Grading Scale*: ECTS uses a standardized grading scale to assess student performance. The scale ranges from A (excellent) to F (fail), with corresponding grade descriptors. The grading scale may vary slightly among institutions, but the general principles are maintained.
  - ✓ *Transparency and Recognition:* ECTS promotes transparency and facilitates the recognition of academic qualifications across different European universities. This is particularly important for students participating in exchange programs or pursuing studies in multiple countries.
  - ✓ *Mobility:* ECTS is crucial for promoting student mobility within the EHEA. Students can transfer their ECTS credits earned at one institution to another, allowing for more flexible academic paths and enhancing the internationalization of higher education.
  - ✓ *Diploma Supplement:* Institutions often provide students with a Diploma Supplement, an official document accompanying a higher education diploma. The supplement includes details about the program, the institution, and the student's achievements in ECTS credits.

- **Certification Credits**: Some professional certifications require individuals to earn a certain number of credits to maintain or renew their certifications. These credits can be earned through participation in approved training programs or activities.
- **Training Hours**: Training hours simply measure the amount of time participants spend in training. This can be expressed in terms of contact hours, instructional hours, or total training time.
- **Skill-Based Credits**: Some training programs offer credits based on the acquisition of specific skills or competencies. Participants may earn credits for successfully demonstrating proficiency in certain areas.

- **Leadership Development Credits**: Leadership development programs may offer credits for activities that enhance leadership skills. These could include workshops, seminars, or coaching sessions focused on leadership development.
- **Technology-Specific Credits**: In the IT industry, training programs often provide credits related to specific technologies or platforms. For example, Microsoft or Cisco certification programs may offer credits for completing relevant courses.
- **In-Service Training Credits**: In-service training credits are often provided to employees as part of their ongoing professional development within an organization. The specific type of credits provided in a training program will depend on the goals and requirements of the training, as well as any industry or certification standards associated with the training.
- **Mini credits**: They could potentially refer to short courses or modules that offer a limited number of credits within a training program. These might be smaller units of study compared to standard courses, providing specific knowledge or skills in a condensed format.
- **Micro-credentials**[58,59]: Micro-credentials is the record of the **learning outcomes**, (i.e., the acquisition of specific skills or competencies) that a learner has acquired following **a small volume of learning**. These learning outcomes will have been assessed against transparent and clearly defined criteria. Learning experiences leading to micro-credentials are designed to provide the learner with specific knowledge, skills and competences that respond to societal, personal, cultural, or **labour market needs**. Micro-credentials are owned by the learner, can be shared and are portable. They may be standalone or combined into larger credentials. They are underpinned by quality assurance following agreed standards in the relevant sector or area of activity.

  Mandatory elements of micro-credentials include:
  - ✓ Identification of the learner
  - ✓ Title of the micro-credential
  - ✓ Country/Region of the issuer
  - ✓ Awarding body
  - ✓ Date of issuing
  - ✓ Learning outcomes
  - ✓ Notional workload needed to achieve the learning outcomes
  - ✓ Level (and cycle, if applicable) of the learning experience leading to the micro-credential (EQF, QF-EHEA), if applicable
  - ✓ Type of assessment
  - ✓ Form of participation in the learning activity

  Optional elements of micro-credentials include:
  - ✓ Prerequisites needed to enroll in the learning activity
  - ✓ Supervision and identity verification during assessment (unsupervised with no identity verification, supervised with no identity verification, supervised online or onsite with identity verification)
  - ✓ Grade achieved
  - ✓ Integration/stackability options (standalone, independent micro-credential / integrated, stackable towards another credential)
  - ✓ Further information.

Practical example of micro-credentials in professional training modules

	W	***L***	***C***	***A***	***Par***	***Pr***	

[58] https://www.etf.europa.eu/sites/default/files/2023-05/Micro-Credential%20Guidelines%20Final%20Delivery.pdf

[59] https://education.ec.europa.eu/education-levels/higher-education/micro-credentials

Module title*	**Workload (in hours; attendance plus study)**	**Level (Basic/Advanced)**	**Cycle** **(if repetitive, give the Nth time of repetition)**	**Assessment type (exercise, exam, project)**	**Participation type (online, physical)**	**Prerequisites**	**Micro-credentials**
Module_1	3+5	Basic	1	Exercise	Physical	No	1
Module_2	24+60	Basic	12	Exam	Physical	Yes	10
Module_3	3+9	Basic	2	Project	Physical	No	2
Module_4	3+15	Advanced	2	Project	Online	Yes	3

**Module_1 is a seminar; Module_2 is a course; Module_3 is a basic workshop; Module_4 is an advanced workshop*

The proposed **formula** used to calculate the volume of the **micro-credentials (MC)** in the table above is:

MC = W*0.1 + L : (B*0.1 | A*0.2) + C*0.1 + A : (Exe*0.1 | Exa*0,2 | Pro*0.3) + Par : (On*0.1 | Phy*0.2) + Pr : (Yes*0.2 | No*0.1)

Note: The micro-credentials (MC) sum must be rounded to the nearest integer.

4 CyberSecPro Proposed Scheme(s) for cybersecurity hands-on trainings

4.1 Principles and Standards to be used

As discussed in Chapter 3, certification authorities across Europe (and beyond) follow their own unique criteria, standards, and processes in the context of certification. CyberSecPro (CSP) has managed to collect and present in this document the state of the art and exploit this knowledge in order to propose its own certification schemas (as we shall see later in this chapter). The key factors and standards described earlier are presented below feeding into the CyberSecPro proposal for a certification scheme.

Factors	**CSP approach**
Knowledge domains	CSP defines 10 Knowledge Areas that the skills and competences acquired may be accredited. These knowledge areas are aligned with industry best practices and standards. These are: 1. Cybersecurity management 2. Human aspects of cybersecurity 3. Cybersecurity risk management 4. Cybersecurity policy, process and compliance 5. Network and communications security 6. Privacy and data protection 7. Cybersecurity threat management 8. Cybersecurity tools and technology 9. Penetration testing 10. Incident response
Experience and education	The CSP engages experienced trainers, i.e. professionals that pose the required expertise and are able to teach the training materials. Moreover, it certifies the hands-on experience of the trainees. There are no minimum requirements for experience and education that candidate trainees must meet.
Examination process	CSP delivers evaluation templates that may be used to evaluate participants’ understanding and application of the training content. In general, CSP identifies four types of assessment: (a) Knowledge-based assessments, (b) Performance-based assessments, (c) Attitudinal assessment, and (d) Behavioural assessments. The exams are in line with the identified learning outcomes per training module. The CSP certificates may be accompanied with ECTS points. Additionally, a Certificate of Attendance will be available for the trainee.
Continuing education	The CSP proposed certification schema does not foresee any type of requirements for ongoing professional development (i.e. earning continuing education credits or participate in regular recertification activities so as trainees to maintain their certification status). But, CSP takes care of continues refreshment of the knowledge delivered through monitoring industry trends.

Ethical and professional conduct	CSP proposed certification schema expects certified professionals to adhere to a code of ethics and maintain professional conduct in their cybersecurity practice.

Standards	**CSP approach**
ISO/IEC 27001	CSP proposed certification schemes which address the ISO/IEC 27001 standard through particular modules
ANAB/ISO/IEC 17024:2012	CSP proposed certification schemes which address the ISO/IEC 17024:2012 standard through particular modules
ISO 29993:2017	CSP proposed certification schemes which does not address the ISO 29993:2017 standard
ISO 9001:2015	CSP proposed certification schemes which does not address the ISO 9001:2015 standard

4.2 Criteria & Scales

4.2.1 Criteria

Relevance to Industry Standards:

EC-Council Global Services (EGS) comprises of advisory and technical teams with years of corporate, field, and consulting experience in the field of information security. EGS offers ISO/IEC 27001 Information Security Management System (ISMS) consultancy services to assist organizations in understanding their risk profile, identify the compliance gaps, and implement the controls required based on the standards and best practices.

EC-Council Global Services assists organizations in planning, creating, upgrading, and certifying a robust and effective ISMS which includes:

-- Conduct gap analysis to evaluate the current state of your information security programs.

-- Determine your current information security risk assessment of the ISMS controls area.

-- Development of written security policies/controls, ISMS procedures, and policy improvement.

-- Provide workshops and training.

-- Establish ISO 27001 best practices if security improvements are necessary.

-- Obtain ISO 27001 third-party certification.

Syllabus:

Introduction to Ethical Hacking

Foot Printing and Reconnaissance

Scanning Networks

Enumeration

Vulnerability Analysis

System Hacking

Malware Threats

Sniffing

Social Engineering

Denial-of-Service

Session Hijacking

Evading IDS, Firewalls, and Honeypots

Hacking Web Servers

Hacking Web Applications

SQL Injection

Hacking Wireless Networks

Hacking Mobile Platforms

IoT and OT Hacking

Cloud Computing

Cryptography

WAY OF DELIVERY:

Onsite

iWeek, Live, Online

iLearn,Self-paced video

Self-study,Certification

CEH Certified Ethical Hacker (ANSI) Application Process

Information Security and Ethical Hacking Overview

Reconnaissance Techniques

System Hacking Phases and Attack Techniques

Network and Perimeter Hacking

Web Application Hacking

Wireless Network Hacking

Mobile Platform, IoT, and OT Hacking

Cloud Computing

Cryptography

Certified Chief Information Security Officer (ANSI) Application process

Governance, Risk, Compliance

Information Security Controls and Audit Management

Security Program Management & Operations

Information Security Core Competencies

Strategic Planning, Finance, Procurement, and Third-Party Management

Certified Hacking Forensic Investigator (ANSI) Application Process

Forensic Science

Regulations, Policies and Ethics

Digital Evidence

Procedures and Methodology

Digital Forensics

Tools/Systems/Programs

Certified Network Defender (ANSI) Application Process

Network Defense Management

Network Perimeter Protection

Endpoint Protection

Application and Data Protection

Enterprise Virtual, Cloud, and Wireless Network Protection

Incident Detection

Incident Response

Incident Prediction

EC-Council Certified Incident Handler (ANSI) Application Process

Incident Response and Handling

Process Handling

Forensic Readiness and First Response

Email Security Incidents

Application Level Incidents

Network & Mobile Incidents

Insider Threats

Malware Incidents

Incidents Occurred in a Cloud Environment

Certification:

CEH (ANSI) - Certified Ethical Hacker (ANSI) Application Process

CEH (Practical) ANSI - Certified Ethical Hacker (Practical) Application Process

CCISO (ANSI) - Certified Chief Information Security Officer (ANSI) Application process

CHFI (ANSI) - Certified Hacking Forensic Investigator (ANSI) Application Process

CND (ANSI) - Certified Network Defender (ANSI) Application Process

ECIH (ANSI) - EC-Council Certified Incident Handler (ANSI) Application Process

CCSE - Certified Cloud Security Engineer Application Process

ECDE - EC-Council Certified DevSecOps Engineer Application Process

CCT - Certified Cybersecurity Technician

NDE - Network Defense Essentials

EHE - Ethical Hacking Essentials

DFE - Digital Forensics Essentials

ICS/SCADA Cybersecurity - ICS/SCADA Cybersecurity Application Process

CTIA - Certified Threat Intelligence Analyst Application Process

CASE .Net - Certified Application Security Engineer .Net, Java Application Process

CASE Java - Certified Application Security Engineer .Net, Java Application Process

CSA - Certified SOC Analyst Application Process

CSCU - Certified Secure Computer User

ECES - EC-Council Certified Encryption Specialist Application Process

EDRP - EC-council Disaster Recovery Professional Application Process

WAHS - Web Application Hacking Security Application Process

CPENT - Certified Penetration Tester Application Process

LPT (Master) - Licensed Penetration Tester (Master) Application Process

Accrediatation

American National Standards Institute (ANSI)

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), Certified Chief Information Security Officer (C|CISO), Certified Network Defender (C|ND), Computer Hacking Forensic Investigator (C|HFI), and EC-Council Certified Incident Handler (E|CIH) to meet the ANSI/ISO/IEC 17024 Personnel Certification Accreditation standard. EC-Council is one of a handful of certification bodies, whose primary specialization is information security, to be awarded this much sought-after quality standard.

Candidates who complete the EC-Council Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (C|HFI), Certified Network Defender (C|ND), Certified Chief Information Security Officer (C|CISO), and EC-Council Certified Incident Handler (E|CIH) certification will also have that extra credential meeting the requirements of the respective ANSI Certification Training Standards

Committee on National Security Systems (CNSS) & National Security Agency (NSA)

EC-Council was honored at the 13th Colloquium for Information Systems Security Education (CISSE) by the United States National Security Agency (NSA) and the Committee on National Security Systems (CNSS) when its Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (ECSA) and Licensed Penetration Tester (LPT) courseware was certified to have met the 4012 (Senior System Managers), 4013A (System Administrators), 4014 (Information Systems Security Officers), 4015 (Systems Certifiers) and 4016 (Information Security Risk Analyst) training standards for information security professionals in the federal government. The CNSS is a federal government entity under the U.S. Department of Defense that providesprocedures and guidance for the protection of national security systems.

Candidates who complete the EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (ECSA) or Licensed Penetration Tester (LPT) certification will also have that extra credential meeting the requirements of the respective CNSS 4011-4016 Federal Security Certification Training Standards.

Department of Defense (DoD)

EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (C|HFI), and Certified Chief Information Security Officer programs are formally integrated as baseline skill certification options for the U.S. Department of Defense (DoD) cyber workforce in several categories. Specifically, the C|CISO program is a recognized certification for the DoD IAM Level II, IAM Level III, and CSSP Manager, all specialized cyber management personnel classifications within the DoD’s information assurance workforce. C|HFI is now recognized as a baseline certification for CSSP Incident Responder and C|EH is now required for the DoD’s computer network defenders (CND’s) – CND Analyst, CND Infrastructure Support, CND Incident Responder, and CND Auditor.

GCHQ Certified Training (GCT)

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), Certified Security Analyst (ECSA), and Chief Information Security Officer (C|CISO), to meet the GCHQ Certified Training standard. This recognition is a feather in the cap for EC-Council’s much sought-after credentials, which are among the most comprehensive programs in the field of Vulnerability Assessment and Penetration Testing, and Information Security Leadership.

This affirms EC-Council’s commitment to offering high-quality certification programs that are developed to help arm information security professionals with the right skills to safeguard the cyber world and achieve successful professional roles.

National Infocomm Competency Framework (NICF)

EC-Council Certified Ethical Hacker (CEH) and Computer Hacking Forensic Investigator (CHFI) programs have been accepted into National Infocomm Competency Framework (NICF) Infocomm professionals competency requirement list. In addition to the inclusion, Infocomm professionals training to be certified for the EC-Council programs at NICF accredited training centers, will be entitled to receive partial funding from Critical Infocomm Technology Resource Program (CITREP) upon certification completion. NICF determines the skills and competencies; and develops training strategies for Infocomm professionals to build a niche Infocomm workforce in Singapore. CITREP is a training incentive program that assists Infocomm professionals with funding to gain recognized and specialized skills.

Department of Veterans Affairs

The Department of Veterans Affairs has included EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), and EC-Council Certified Security Analyst (ECSA) under its GI Bill® for the reimbursement of test fees for veterans and other eligible persons in accordance with the provisions of PL 106-4

Malaysian Military Cyber Security Warfare Department (KOMLEK)

The Malaysian Military Cyber Security Warfare Department (KOMLEK) has stipulated their military professionals to be CEH & CHFI Certified as part of their Cyber Warfare Training Program (CPS).

Distance Education Accrediting Commission (DEAC)

EC-Council University is accredited by Distance Education Accrediting Commission. DEAC is a private, non-profit organization that operates as a national accreditor of distance education institutions. Accreditation by DEAC covers all distance education activities within an institution and it provides a single source of nationally recognized accreditation. DEAC is listed by the U.S. Department of

Education as a nationally recognized accrediting agency as well as a acknowledged member of the Council for Higher Education Accreditation (CHEA).

Code of Ethics:

Students and alumni should:

-- Keep private and confidential information gained in own professional work, (in particular if it pertains to your client lists and client's personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without your client's prior consent.

-- Protect and respect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator. Disclose and report to appropriate persons or authorities' potential dangers to any e-commerce clients, the Internet community, or the public, as applicable.

-- Provide service in own areas of competence. You should be honest and forthright about any limitations of own experience and education. Ensure that the Certified Member is qualified for any project by an appropriate combination of education, training, and experience.

-- Never knowingly use software or process that is obtained or retained either illegally or unethically.

-- Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

-- Use and protect the property of your clients or employers only in ways which are properly authorized, and with the owner's knowledge and consent.

-- Avoid any conflict of interest. Disclose to all concerned parties, including (without limitation) your clients, employers, EC-Council any actual or potential conflicts of interest that cannot reasonably be avoided or escaped. For the purpose of clarity, if you have participated in Item writing for any of the EC-Council certification examinations, you will not be allowed to sit for the same certification examination. Further, if you wish to be EC-Council's Consultant, you must disclose your association with EC-Council's other products and/or services and/or your association with competing products and/or services.

-- Ensure good management for any project as a Certified Member.

-- Add to the knowledge of the e-commerce profession by constant study, share the lessons of own experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.

-- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in the Certified Member's knowledge and integrity.

-- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.

-- Not to associate with malicious hackers or engage in any malicious activities.

-- Not to purposefully compromise or allow the client's or organization's systems to be compromised in the course of the Certified Member's professional dealings.

-- Ensure all penetration testing activities are authorized and within legal limits.

-- Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.

-- Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.

-- Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.

-- Not to be in violation of any law of the land or have any previous conviction.

-- Make claims regarding certification only with respect to the scope for which the certification has been granted.

-- Not to use the certification in a manner as to bring EC-Council into disrepute.

-- Not to make misleading and/or unauthorized statement regarding the certification or EC-Council.

-- Discontinue the use of all trademarks as regard to the certification which contains any reference to EC-Council and/or EC-Council trademark or logo or insignia upon suspension/withdrawal of the said certification.

-- Return any certificates issued by EC-Council upon suspension/withdrawal of the certification.

-- Refrain from further promoting the certification in the event of the said certification is withdrawn or suspended.

-- Inform EC-Council without any undue delay of any physical or mental condition which renders the Certified Member incapable to fulfill the continuing certification requirements.

-- Maintain the certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that correspond with Certified member's particular certification.

-- To not to participate in any cheating incident, breach of security, misconduct or any other behavior that could be considered a compromise of the integrity or confidentiality of any EC-Council certification examination.

DEI&B

Culture

EC-Council University has people of all genders and all backgrounds in our company and our industry. EC-Council University fully supports the inclusion of people from all cultures, races, ethnicities, ages, genders, gender identities and expressions, sexual orientations, physical or mental abilities, and work-life situations. Our culture of inclusion emphasizes the health and well-being of everyone, regardless of background, so our workforce, community, and students feel included and able to perform at their best.

Talent

Recruiting – Developing – Leading

EC-Council University Group provides equal opportunities to all our employees and all eligible applicants for employment in our company. We do not discriminate on any ground, including race, caste, religion, color, ancestry, marital status, gender, sexual orientation, age, nationality, ethnic origin, disability, or any other category protected by applicable law.

Inclusive & Respectful Workplace

EC-Council University strives to create workplaces that are welcoming to all our employees. Everyone has the right to feel comfortable at work, and behavior that doesn't uphold our stated values will not be tolerated. As an employer, we are opposed to any form of bullying or harassment and are committed to providing a work environment that is free of such behavior. We expect that all our working relationships will be characterized by mutual trust and respect.

Code of Conduct

Commit to acting with integrity and maintaining the highest ethical standards.

Harassment Free Workplace

Create a positive environment for all, avoiding actions that create a hostile or offensive environment for others.

Diversity & Inclusion/Unconscious Bias

Diversity and Inclusion (D&I) is also pivotal to EC-Council University's internal organizational culture and success. EC-Council University strives to celebrate differences and aims to be recognized as a leader in D&I by ensuring that its environments are ready, respectful, and safe for everyone, everywhere, every time. This policy applies to all activities in which EC-Council University is engaged and includes all stakeholders, including learners, employees, visitors, and third parties. All employees and participants will be made aware of the policy and the resources that support its implementation.

Legal Compliance

Bribery and Corrupt Practices

EC-Council University is committed to ensuring that the EC-Council University Group meets its legal obligations and prevents, detects, minimizes, and eliminates all forms of corrupt practices. Our people hold themselves and our business to the highest legal and ethical standards. We will not be a party to corruption or bribery in any form.

Government, Regulators and Legislators

EC-Council University will seek to comply with all international, national, and local legislation affecting its operations. It will strive to follow the best practice in corporate governance & meet its tax obligations. It will not make any financial contributions or offer support to any political party.

4.2.2 Scales

In the CyberSecPro project, the training material can be provided in the following module types:

- Course (C),
- Workshop (W),
- Seminar (S),
- Cybersecurity exercise (CS-E),
- Summer School (SS),
- Hackathon (H),
- Other (O).

From these categories only the courses can follow the Academic Credits system described in section 3.3 of this deliverable, as they are characterized by a more academic manner and logic. This means that when the trainees complete a course, they earn the corresponding ECTS assigned to it by the trainer, based on the hours of student workload required.

All types of training material provided in the frame of this project will be accompanied by the duration of the module (Training Hours) as well as a Certificate of Attendance (CoA).

4.3 CyberSecPro Schemes

4.3.1 Objectives and requirements

During this project, we propose market-driven Industry/Market-specific cybersecurity schemes (see Chapter 3) that can be used for establishing a cybersecurity professional program and /or modules.

Based on the CSP partners work in D2.1, D2.3, D.3.1, we propose **structured frameworks for the**:

- Sector-agnostic curriculum for cybersecurity professional trainings **(CSP Scheme A)**
- Descriptions of the 12 sector-specific modules **(CSP Scheme B)**

- Syllabi of the 12 sector-specific modules **(CSP Scheme C)**

These schemes can be used by any training provider that wishes to develop a sectors-specific cybersecurity training program.

The CSP proposed schemes will help training providers to address the requirements for certifying their cybersecurity professional trainings, i.e.

- *Relevance to Industry Standards*: ensure that the content of the training material is relevant to the current needs and expectations of the market.
- *Syllabus and Training material Quality*: CSP syllabus/training material of the modules will comprehensive.
- *Experienced Trainers:* CSP trainers have a track record of success and are able to effectively communicate the material.
- *Assessment and Evaluation*: CSP evaluation templates (see D3.1) will be used to evaluate participants' understanding and application of the training content.
- *Hands-On Experience*: Practical, hands-on experience applies.
- *Duration and Intensity*: CSP modules duration is sufficient to illustrate and train the topics.
- *Continuing Education and Renewal*: CSP industry trends and refresh their knowledge periodically.
- *Feedback and Improvement*: regular evaluations of every module, reviews, and updates to keep the content current and effective to the trainees and professions.

4.3.2 CSP Scheme A: Sector-agnostic scheme for a professional cybersecurity training programme

Title	***Sector-agnostic scheme for a professional cybersecurity programme***
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	*Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O)*
Level *Training level: B (Basic), A (Advanced)*	A / B
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a professional training programme*	
12 sector(s)-specific cybersecurity modules	**1.** Cybersecurity Essentials and Management **2.** Human Factors and Cybersecurity **3.** Cybersecurity Risk Management and Governance **4.** Network Security **5.** Data Protection and Privacy Technologies **6.** Cyber Threat Intelligence **7.** Cybersecurity in Emerging Technologies **8.** Critical Infrastructure Security **9.** Software Security **10.** Penetration Testing **11.** Cyber Ranges and Operations **12.** Digital Forensics
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training programme. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as

	through practical exercises, simulations, or case studies. **Attitudinal assessments:** These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments:** These assessments measure the participant's actual behaviour in relation to cybersecurity. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the professional training programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* ***Analyse:*** *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* ***Identify:***	

(5)Network and Communications Security *(6) Privacy and Data Protection* ***Select:*** *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* ***Adapt:*** *(9)Penetration Testing* ***Apply:*** *(10)Incident Response*	
Pre-requisites	
Relevance to other Cybersecurity Skills Framework	e-CF, CyBOK, CONCORDIA, … (other)
Tools to be used *A list of tools that will be used for the operation of this training module*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS.*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Programme enrolment dates *Indicates the enrolment dates for the operation of this professional programme*	
Other important dates	

If applicable, any other important dates for this professional training programme (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.	

In the following sections, we will provide the descriptions/syllabi from D3.1 by parametrising them. After the operation (WP4) and evaluation (WP5) work-packages, we will update them and present the final ones in D5.4.

4.3.3 CSP Scheme B: Descriptions of the 12 professional training modules

4.3.4 Description of Training Module-1: Cybersecurity Essentials and Management in *<sector-name>*

The module provides a comprehensive overview of the essential concepts and principles of cybersecurity for <*sector-name*> leaders, managers, or technical cybersecurity beginners. The module provides foundation skills and knowledge including cybersecurity body of knowledge and management aspects of cybersecurity equipping participants in this sector with the knowledge and skills necessary to make a strategy to protect critical systems and data in the sector <*sector-name*>. The module covers a wide range of topics which address the sectorial needs of <*sector-name*>, including the cybersecurity body of knowledge, the different types of cybersecurity threats and vulnerabilities, the principles of cybersecurity risk management, ethical and professional practices, soft skills needed when working in teams and the basic cybersecurity controls.

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Cybersecurity Essentials and Management in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Cybersecurity Essentials in <*sector-name*> **2.** Cybersecurity Management in <*sector-name*> **3.** Cybersecurity for the Modern Workplace-Cybersecurity Essentials and Principles in <*sector-name*> **4.** A Comprehensive Overview of Cybersecurity Core Concepts in <*sector-name*> **5.** Mastering the Fundamentals of Cybersecurity in <*sector-name*> **6.** From Essentials to Management: Cybersecurity for Managers and Leaders in <*sector-name*> **7.** Essential Cybersecurity Skills for Managers and Leaders in <*sector-name*>

	8. Introduction to Information and Cyber Security in <*sector-name*> **9.** Introduction to Information Security Management in <*sector-name*> **10.** Management of Information Security in <*sector-name*>
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	This training module provides a foundational understanding of cybersecurity essentials and management, equipping participants with the knowledge and skills to manage information and cyber security in an <*sector-name*> organisation
Module description *Indicates the main purpose and description of the module*	The Cybersecurity Essential and Management in <*sector-name*> training module provides participants and trainees with the knowledge and skills necessary to manage the security of information assets in an organisation. The module covers a wide range of topics as described on the main topics. The module is designed to be more practical and hands-on, and participants will gain experience in applying the concepts they learn through a variety of exercises and activities
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a module*	By the end of the training, participants will be able to: • Demonstrate ethical and professional conduct in all aspects of information and cybersecurity management • Comprehend and articulate the key concepts and principles of information and cyber security • Understand the evolving cyber threat landscape and the diverse range of cyber attacks • Identifies the cybersecurity threats, vulnerabilities, and risks to an organisation • Recognises the human factor's role in cybersecurity breaches and risk mitigation strategies • Strategically aims to design and develop a robust information security governance framework and risk management aligned with organisational goals • Ability to design a secure information security architecture that safeguards critical assets • Ability to help and select appropriate security controls to protect against identified cybersecurity threats and risks

	• Helps the technical cybersecurity colleagues with appropriate security controls and measures to ensure data security and privacy • Develop an initial plan to effectively respond to cyber incidents, applying relevant information security concepts • Awareness raising within employees on cybersecurity best practices to foster a security-conscious culture • Foundation knowledge of compliance with and apply the legal and ethical aspects of cybersecurity within the organisation • Broad knowledge of applying security management standards and frameworks, such as ISO/IEC 27001, to enhance cybersecurity posture • Enhance soft skills, including teamwork, communication, problem-solving, critical thinking, leadership, and adaptability, to thrive in the cybersecurity domain • Document work-related activities, tasks, and outcomes effectively, and present them to various audiences and forums • Continuously reflect on and develop their own learning process and working-life skills to maintain professional competence
Main topics and content list *A list of main topics and key content*	• Ethical Conduct and Professionalism in <*sector-name*> • Ethical Conduct and Professionalism in <*sector-name*> • Foundational Knowledge of Cybersecurity in <*sector-name*> • Cybersecurity Body of Knowledge • Threats and vulnerabilities in <*sector-name*> • Human Factor Considerations in <*sector-name*> • Information Security Governance (ISG) and Information Security Risk Management (ISRM) in <*sector-name*> • Secure Architecture Design and Implementation in <*sector-name*> • Security Controls Selection and Implementation in <*sector-name*> • Data Security and Privacy by Design in <*sector-name*> • Security Auditing and Compliance in <*sector-name*> • Legal and Ethical Compliance in <*sector-name*> • Security Management Standards and Drameworks in <*sector-name*>

	- Soft Skills and Leadership Development in *<sector-name>* - Effective Communication and Documentation in *<sector-name>* - Self-Reflection and Continuous Learning in *<sector-name>*
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments:** These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments:** These assessments measure the participant's actual behaviour in relation to cybersecurity. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the professional training programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	

Knowledge area(s) *Mapping to the 10 selected knowledge areas* ***Analyse:*** *(1) Cybersecurity Management* *(2) Human Aspects of Cybersecurity* *(3) Cybersecurity Risk Management* *(4) Cybersecurity Policy, Process, and Compliance* ***Identify:*** *(5) Network and Communications Security* *(6) Privacy and Data Protection* ***Select:*** *(7) Cybersecurity Threat Management* *(8) Cybersecurity Tools and Technology* ***Adapt:*** *(9) Penetration Testing* ***Apply:*** *(10) Incident Response*	
Pre-requisites	
Relevance to other Cybersecurity Skills Framework	
Tools to be used *A list of tools that will be used for the operation of this training module*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates	

If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description	

4.3.5 Description of Training Module-2: Human Factors and Cybersecurity in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Human Aspects of Cybersecurity in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** The Human Dimension of Cybersecurity in <*sector-name*> **2.** Navigating Cyber Threats: The Human Element in <*sector-name*> **3.** Elements of Cyberpsychology in <*sector-name*> **4.** Humans in Cybersecurity **5.** Human-Centric Cyber Defence in <*sector-name*>
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	A, B
Module overview	This training module provides participants with the knowledge and skills

High-level module overview	necessary about human aspects of cybersecurity in <*sector-name*>, as well as the individual and organisational levels at the strategic, operational, and tactical levels
Module description *Indicates the main purpose and description of the module*	This course dives deep into the human elements of cybersecurity in <*sector-name*>, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants will gain insights into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations. It also emphasises the critical role of communication and collaboration at strategic, operational, and tactical levels. Participants will explore how effective communication across domains <*sector-name*> and decision-making processes can bolster cybersecurity efforts
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	**Knowledge:** ● Understand the psychological, social, and organisational factors influencing cybersecurity behaviours ● Recognize the importance of communication and collaboration in cybersecurity across <*sector-name*> domains ● Identify decision-making processes at strategic, operational, and tactical levels of cybersecurity in <*sector-name*> ● Identify Adversaries Profiles and Tactics in <*sector-name*> ● Measuring human-related threats and vulnerabilities in <*sector-name*> **Skills:** ● Develop and implement effective communication strategies for cybersecurity in <*sector-name*> ● Collaborate with cross-functional teams to address human aspects of cybersecurity in <*sector-name*> ● Analyse real-world cybersecurity incidents to identify human factors and communication breakdowns <*sector-name*> ● Categorise adversaries and analyse profiles **Competencies:** ● Lead and participate in strategic, operational, and tactical cybersecurity discussions ● Foster a culture of open communication and collaboration in cybersecurity ● Make informed cybersecurity decisions based on comprehensive understanding of human aspects ● Identify and mitigate human threats and vulnerabilities
Main topics and content list *A list of main topics and key content*	1. Ethical and professional practices in <*sector-name*> 2. Introduction to Human Aspects of Cybersecurity in <*sector-name*> 3. Psychological and Social Factors in Cybersecurity in <*sector-name*> 4. Human Vulnerabilities in Cybersecurity in <*sector-name*> 5. Organisational Culture, Communication, and Cybersecurity in <*sector-name*>

	6. Communication and Collaboration Across Domains in <*sector-name*> 7. Decision Making at Strategic, Operational, and Tactical Levels in <*sector-name*> 8. Training, Awareness, and Communication Programs in <*sector-name*> 9. Future Trends, Challenges, and the Role of Communication in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision	

Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	*(2) Human Aspects of Cybersecurity* *(7) Cybersecurity Threat Management*
Pre-requisites	
Relevance to other Cybersecurity Skills Framework	Cybersecurity Educator Chief Information Security Officer Cybersecurity Researcher Cybersecurity Risk Manager

Tools to be used *A list of tools that will be used for the operation of this training module*	CVSS4 calculator
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.6 Description of Training Module-3: Cybersecurity Risk Management and Governance in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The*	***CSP_00x_C_T***

purpose of this format is to apply the code to every place you use this module as part of the programme	
Module Title *The title of the training module*	**Cybersecurity Risk Management and Governance in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Information Security Risk Management **2.** Security Management **3.** Trust Management **4.** Risk Assessment and Management **5.** Enterprise Risk Management **6.** Risk Assessment and Mitigation **7.** Risk Control and Governance **8.** Risk Minimization Strategies **9.** Risk Analysis and Remediation **10.** Risk Mitigation and Compliance **11.** Strategic Risk Planning **12.** Risk Avoidance and Management **13.** Threat Management and Mitigation **14.** Risk Intelligence and Decision-Making
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	This module focuses on acquainting participants with the principles and requirements in relation to security and privacy of Information Systems (IS) in <*sector-name*>. The main phases of an ISMS (Information Security Management System) implementation are described as defined within ISO/IEC 27001. Risk Management and Risk Assessment methodologies are introduced based on standards and best practices. Security Management will involve the development of security reports (e.g. Risk Treatment Plan, Security Policy, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), Security Procedures).

Module description *Indicates the main purpose and description of the module*	This module aims at introducing the basic principles, standards, legislation, policies, rationale, and requirements of an Information Security Management System based on standards in <*sector-name*> (e.g. the ISO27000x family). Since risk management is part of the requirements of an Information Security Management System, this module also aims at providing the basic principles, phases, and methodologies for implementing it. Mitigation Actions (technical and non-technical) and Procedures will be introduced, assessed, and evaluated as well as development of security reports.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	By the end of the training, participants will have gained the following: **Knowledge:** ● Basic definitions related to Information Security Management Systems, and Information Security Governance in <*sector-name*> ● Risk Management in <*sector-name*> ● Basic phases and principles for an effective risk management methodology in <*sector-name*> ● Standards and Methodologies of Risk Management in <*sector-name*> ● Legal and Policies related to Risk Management in <*sector-name*> ● Measurements, Scales and Metrics of Risks in <*sector-name*> ● Technical and non-Technical Mitigation Actions in <*sector-name*> **Skills:** ● (applying) a suitable methodology for Information Security Risk Management and Risk Assessment. ● (analysing) Information Security Risk utilising different methodologies. ● (creating) policies, procedures and processes compliant to the requirements of the current version of standards (e.g. the 27000x family) in <*sector-name*>. ● Select and implement appropriate mitigation actions and controls. ● Develop Security Policy and Procedures. ● Develop BCS, DRP. ● Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards in <*sector-name*>. ● Analyse and consolidate organisation’s quality and risk management practices.

	● Enable business assets owners, executives, and other stakeholders to make risk-informed decisions to manage and mitigate risks in <*sector-name*> ● Enable employees to understand, embrace and follow the controls. ● Build a cybersecurity risk-aware environment. ● Communicate, present and report to relevant stakeholders. ● Propose and manage risk-sharing options. **Competencies:** ● Lead and participate in strategic, operational, and tactical cybersecurity discussions. ● Lead the design, development, operation, and improvement of an Information Security Management System. ● Support the organisation in the audits of an Information Security Management Systems.
Main topics and content list *A list of main topics and key content*	● Introduction to information security and cyber security including CIA triad. ● Risk management related standards in <*sector-name*>. ● The scope and purpose of an Information Security Management System. ● Information Security Risk Management definitions and principles. ● ISO Standards in <*sector-name*> basic structure. ● Threats and vulnerabilities in <*sector-name*>. ● Measurements and Metrics. ● Risk assessment, management processes, and methodologies in <*sector-name*>. ● Cybersecurity Maturity Models Requirements / Auditing practices. ● Security Reports.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews.

	Behavioural assessments: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance*	*(1) Cybersecurity Management* *(3) Cybersecurity Risk Management* *(4) Cybersecurity Policy, Process, and Compliance*

Identify: *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	
Pre-requisites	
Relevance to other Cybersecurity Skills Framework	chief information security officer (ciso) cyber legal, policy & compliance officer cybersecurity auditor cybersecurity risk manager
Tools to be used *A list of tools that will be used for the operation of this training module*	Mitigate, Risk calculators
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA)	

Indicates Yes or No (even in case of partial attendance)	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.7 Description of Training Module-4: Network Security in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Network Security in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Threats and network hardening **2.** Basic principles of network security **3.** Network security management **4.** Secure design and management of communication systems **5.** Cyber Network Defence **6.** Network Protection Strategies **7.** Secure Networking Practices **8.** Information Security Networking **9.** Cyber Defence for Networks

	10. Network Threat Prevention **11.** Securing Network Infrastructure **12.** Digital Network Defence **13.** Data Network Security **14.** Network Risk Management
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	This module will provide participants with the necessary knowledge to identify and address the possible security problems and threats associated with the emergence of various types of communication networks in <*sector-name*> and their implicit protocols. In this training process, participants will also learn how these protocols can be used to the benefit of attackers and what can be done to prevent their exploits. The module will also provide ways of post-attack policies in cases of a successful attack and measures to ensure privacy and anonymity of communication systems in <*sector-name*>.
Module description *Indicates the main purpose and description of the module*	This module's main objective is to provide a clear vision of the different types of communication systems, network structures, components and protocols involved in <*sector-name*>. This knowledge will be key not only to lay the necessary foundations on how attacks exploit network traffic and the components that make up communication networks in <*sector-name*>, but also to know how to identify potential and/or common threats in order to prevent them. Thus, this module covers a wide range of topics in <*sector-name*> with practical usefulness in multiple today's application scenarios and ecosystems such as IoT and their variants. This feature also obliges us to offer content not only with a theoretical approach but also with a mainly practical approach, where trainees will gain experience and skills by addressing a set of exercises and practical activities.
Learning outcomes and targets	By the end of the training, participants will have gained the following:

A list of knowledge, skills and competences achieved by the participants as a result of taking a training module	**Knowledge:** ● General knowledge of communication infrastructures and models, as well as the emergence of modern networks and technologies in <*sector-name*>. ● Knowledge of the most common vulnerabilities and threats in specific network systems in <*sector-name*> (in traditional networks, mobile networks, virtualized systems, or distributed systems) and their associated protocols. ● Knowledge of the most relevant security protocols, such as SSL/TLS and IPSec, and their importance for the protection of systems and communication networks in <*sector-name*>. ● Knowledge of the most relevant security mechanisms, such as firewalls and IDS/IPS, to protect network perimeters and access to private domains, such as corporate networks. ● Knowledge of the most relevant security mechanisms to protect the end-points of a communication, such as a client and a server, but also the interconnection elements between a client and a server. ● Knowledge of the most relevant security mechanisms to protect those advanced communication infrastructures such as mobile networks or virtualized systems. ● Knowledge of privacy and anonymity in network management, ensuring the protection of end-nodes and their location. **Skills:** ● Plan and design secure networks according to the most general recommendations and following good security practices in <*sector-name*>. ● Analyse communication scenarios and identify possible misconfigurations or vulnerabilities that could lead to security risks or threats in <*sector-name*>. ● Configure systems following basic security principles (e.g., user control, port control, etc.) in <*sector-name*>. ● Identify and apply those security elements or mechanisms that contribute to improving the security of a communication system in <*sector-name*>. **Competencies:** ● Know how to identify possible misconfigurations or errors that may lead to significant security risks. ● Lead the design, configuration, and deployments of communication systems in <*sector-name*>. ● Support the organisation in hardening its systems, and enhance secure communications in <*sector-name*>.

	● Knowledge of existing security technologies, mechanisms, and protocols, useful to protect any peer-to-peer communication. ● Knowledge of recommendations and best practices for securing end-nodes and interconnection elements. ● Knowledge of privacy weaknesses, and existing mechanisms to address threats in <*sector-name*>.
Main topics and content list *A list of main topics and key content*	**1.** Basic network fundamentals, architectures, and protocols. **2.** Common weaknesses and attacks of communication networks in <*sector-name*>. **3.** Main security protocols embedded in the traditional communication stack in <*sector-name*>. **4.** Perimeter defence and protection tools in <*sector-name*>. **5.** Security of end communication nodes and of interconnection systems in <*sector-name*>. **6.** Security in advanced network infrastructures in <*sector-name*>. **7.** Privacy and anonymity of communication networks in <*sector-name*>.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered	

Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:*	*(5) Network and Communications Security*

(10)Incident Response	
Pre-requisites	Basic knowledge of cybersecurity essentials in <*sector-name*> (Module 1), and experience with operating systems, network setups and protocols
Relevance to other Cybersecurity Skills Framework	Cyber threat intelligence specialist Cybersecurity architect Cybersecurity auditor Cybersecurity researcher Penetration tester
Tools to be used *A list of tools that will be used for the operation of this training module*	In addition to the presentations and materials of the training modules (e.g., use cases, examples, and relation of exercises), a set of tools will be applied to carry out the practical activities and exercises proposed during the training phase.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates,*	

face-to-face dates). More information will be provided in the module description	

4.3.8 Description of Training Module-5: Data Protection and Privacy Technologies in *<sector-name>*

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Data Protection and Privacy Technologies in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Privacy Technologies **2.** Privacy by Design **3.** Data Protection **4.** Data Privacy **5.** Privacy and Online Rights
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	This module will provide policies and practices for data protection in terms of security flaws and disastrous events in <*sector-name*>.

Module description *Indicates the main purpose and description of the module*	The main purpose of this module is to present the main types of encryption methods in <*sector-name*>with their pros/cons, display methods of anonymity in an organisation in <*sector-name*>, how to set up zero-knowledge infrastructure, in which scenarios cold storages are needed, who to provision security policies such as MFA, conditional access, how to be prepared potential social engineering attacks in <*sector-name*>, phishing attacks, create organised scarcity in terms of how security is implemented in a company/organisation, how to share data with anonymity in <*sector-name*>, create digital authorities, provide methods of reviving systems after a disastrous event in <*sector-name*>.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	● Architectural needs of each infrastructure in terms of privacy policies in <*sector-name*> ● Orthodox and global practices for security to protect data and privacy in <*sector-name*> ● Privacy related threats in <*sector-name*> ● Privacy assessment in <*sector-name*> ● Privacy controls, mitigation actions and procedures in <*sector-name*> ● Privacy technologies in <*sector-name*> CyBOK- related - Risk Management & Governance (https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf) - Security Operations & Incident Management (https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf) - Cryptography (https://www.cybok.org/media/downloads/Cryptography_v1.0.1.pdf) - Applied Cryptography (https://www.cybok.org/media/downloads/Applied_Cryptography_v1.0.0.pdf)
Main topics and content list *A list of main topics and key content*	● **Anonymisers in <*sector-name*>:** Hiding a user's real online identity (email address, IP address, etc.) and replacing it with a non-traceable identity (disposable / one-time email address, random IP address of hosts participating in an anonymising network, unlinkability, unobservability, pseudonyms, etc.). ● **Bogus online accounts:** Delink of real identity on the internet. ● **Obfuscation in <*sector-name*>.** Hiding personal information or sensitive data through computer algorithms and masking techniques. This technique can also involve adding misleading or distracting data or information so it's harder for an attacker to obtain the needed data(honeypots). ● **Conditional Access to Data & Infrastructure in <*sector-name*>:** Hierarchy and conditional access of the users and

	employees to data and infrastructure. MFA implementation methods. ● **Data Protection and Identity Management (IdM) in <*sector-name*>:** IdM, especially the difference between identity and identifier; Issues of overidentification; IdM architectures and the information flows therein. Related standards, especially ISO/IEC 24760 "A framework for identity management". ● **Location information and its privacy impact in <*sector-name*>**: Collection of location information, especially in cellular mobile telecommunication networks, and the uses of the data enabling movement profiles. Protection approaches against these attacks. ● **Enhanced privacy ID (EPID) in <*sector-name*>:** A digital signature algorithm supporting anonymity. Unlike traditional digital signature algorithms (e.g., PKI), in which each entity has a unique public verification key and a unique private signature key, EPID provides a common group public verification key associated with many unique private signature keys.[18] EPID was created so that a device could prove to an external party what kind of device it is (and optionally what software is running on the device) without needing to also reveal exact identity, i.e., to prove you are an authentic member of a group without revealing which member. It has been in use since 2008. ● **Methods of encryption in <*sector-name*>:** symmetric key cryptography, ECC, asymmetric key cryptography, hashing. ● **Zero-knowledge proof in <*sector-name*>:** A method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. ● **Digital Authorities & Ring Signatures in <*sector-name*>.** ● **Non-interactive zero-knowledge proofs in <*sector-name*>:** (NIZKs) are zero-knowledge proofs that require no interaction between the prover and verifier. ● **Blinding:** A cryptography technique by which an agent can provide a service to a client in an encoded form without knowing either the real input or the real output. ● **Differential privacy in <*sector-name*>**: An algorithm is constrained so that the results or outputs of a data analysis can't tell if a certain individual's information is being used to analyse and form the results. This technique focuses on large databases and hides the identity of individual "inputs" who might have private data and privacy concerns. ● **Pseudonymisation:** A data management technique that replaces an individual's identity or personal information with artificial identifiers known as Pseudonyms. This de-identification method enables contents and fields of information to be covered to deter attacks and hackers from obtaining important information. These Pseudonyms can be either placed in groups or for individual pieces of information. Overall, they serve to discourage information stealing while also maintaining data integrity and data analysis.[19]

	● **Federated learning in <*sector-name*>:** A machine learning technique that trains models across multiple distributed nodes. Each node houses a local, private dataset. ● **MFA methods** ● **Cold storages** ● **CSMs** ● Backup methods (offsite/onsite), OS snapshots, and provisioning data recovery methods for reviving the entity of the systems easily and fast
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	(6) *Privacy and Data Protection*
Pre-requisites	Basic IT training + suggested minimum know-how in above section
Relevance to other Cybersecurity Skills Framework	Cyber Incident Responder Cyber Legal, Policy & Compliance Officer

	Cybersecurity Architect Cybersecurity Auditor Cybersecurity Implementer
Tools to be used *A list of tools that will be used for the operation of this training module*	Laboratory with PCs, Servers, Presentation slides, CSMs, VPN setups, usage of "Cold storages", Openstack, Yubikeys, Licences for tools like DUO Security/Octa, platforms for provisioning changes on a mass scale (AZURE AD/Intune, Google Workspace, Data Security Assessment Tools, Amazon AWS demo platforms, Kerberos setup systems, etc…)
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.9 Description of Training Module-6: Cyber Threat Intelligence in <*sector-name*>

Code	***CSP_00x_C_T***

Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme	
Module Title *The title of the training module*	**Cyber Threat Intelligence in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Cybersecurity Intelligence Collaboration 2. Threat Intelligence Exchange 3. Security Threat Information Sharing 4. Cyber Threat Analysis and Collaboration 5. Intelligence-driven Cyber Defense 6. Threat Information Collaboration 7. Cybersecurity Intelligence Fusion 8. Collaborative Threat Mitigation 9. Intelligence-led Cybersecurity 10. Threat Sharing and Analysis
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	The module aims to provide learners with an overview of threat intelligence and management in <*sector-name*>. It allows the learners to analyse the known and unknown threats in <*sector-name*> and determine a course of action to tackle with them.
Module description *Indicates the main purpose and description of the module*	The module provides an understanding of the underlying properties and principles associated with cyber threats within an organisational setting in <*sector-name*>. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence. Upon completion of the module, the learners can adopt the knowledge and skill

	to analyse the threats in their organisational context.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge:** ● Demonstrate knowledge and understanding of threats in <*sector-name*>. ● Attacks and Attack actors in <*sector-name*>. ● Critically evaluate the cyber threats of an organisation in <*sector-name*> by following threat intelligence properties. **Skill and Competence:** ● Analyse the results of a threat assessment and provide recommendations. ● Able to perform vulnerability assessment and measure how it contributes to threat mitigation. ● Evaluate the necessity of threat hunting techniques and threat intelligence as protection mechanisms.
Main topics and content list *A list of main topics and key content*	● Cyber threats taxonomy and threat intelligence in <*sector-name*>. ● Vulnerabilities assessment techniques in <*sector-name*>. ● Threat modelling in <*sector-name*>. ● Threat hunting concept and standard in <*sector-name*>. ● Threat intelligence information sharing standard, reporting, and feed in <*sector-name*>. ● Security controls and standards in <*sector-name*>.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider	

Name(s) of training providers	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection*	*(1) Cybersecurity Management* *(7) Cybersecurity Threat Management* *(8) Cybersecurity Tools and Technology*

Select: *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	
Pre-requisites	Basic IT and security Knowledge
Relevance to other Cybersecurity Skills Framework	Cyber Incident Responder Cybersecurity Risk Manager Cyber Threat Intelligence Specialist Cybersecurity Implementer
Tools to be used *A list of tools that will be used for the operation of this training module*	Virustotal Phishtank Threatminer Mozilla observatory Threatfeeds Talos Malware bazaar CVSS v4.0 calculator
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate	

If applicable, the number of ECTS	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.10 Description of Training Module-7: Cybersecurity in Emerging Technologies in *<sector-name>*

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Cybersecurity in Emerging Technologies in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training*	**1.** Security Challenges in Emerging Technologies **2.** Protecting Emerging Tech: Cybersecurity Considerations **3.** Securing Future Technologies: Cyber Threats and Solutions **4.** Cyber Risks in Emerging Tech Landscapes **5.** Safeguarding Innovation: Cybersecurity in New Technologies

providers	**6.** Emerging Tech Security: Addressing Cyber Threats **7.** Cyber Defense for Emerging Technological Landscapes **8.** Ensuring Security in Cutting-Edge Technologies **9.** The Intersection of Cybersecurity and Emerging Tech **10.** Future Tech Security: Navigating Cyber Challenges
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	The module covers the usage of emerging technologies in <*sector-name*> for addressing cybersecurity issues.
Module description *Indicates the main purpose and description of the module*	The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by the integration of cutting-edge technologies in <*sector-name*>. As innovations arise, such as the Internet of Things (IoT), artificial intelligence (AI), blockchain, and 5G, the need for robust cybersecurity measures becomes paramount. This module aims at providing a comprehensive understanding of the cybersecurity landscape in <*sector-name*> within the context of emerging technologies.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	Upon completing the module, trainees should be well-equipped to address the cybersecurity challenges in <*sector-name*> posed by the integration of AI, Cloud, and IoT technologies. They should possess a strong foundation of knowledge, practical skills, and ethical considerations necessary for securing interconnected systems in modern IT environments. Trainees should be able to: ● Apply AI and machine learning techniques in <*sector-name*> to enhance cybersecurity practices, including threat detection and analysis. ● Gain knowledge of cloud computing fundamentals, securing cloud infrastructure, and managing identities in the cloud. ● Comprehend the security challenges associated with IoT in <*sector-name*>, including securing devices, networks, and addressing privacy concerns. ● Make ethical decisions regarding the use of AI, Cloud, and IoT

	in cybersecurity, considering privacy and societal implications in <*sector-name*>.
Main topics and content list *A list of main topics and key content*	● AI on cybersecurity in <*sector-name*> ● Anomaly detection techniques in <*sector-name*> ● Cloud security in <*sector-name*> ● IoT security in <*sector-name*> ● Data analysis for cybersecurity in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	*(8) Cybersecurity Tools and Technology*
Pre-requisites	Basic programming skills, particularly in languages commonly used in cybersecurity, such as Python.

Relevance to other Cybersecurity Skills Framework	Cyber Threat Intelligence Specialist Cybersecurity Researcher Digital Forensics Investigator
Tools to be used *A list of tools that will be used for the operation of this training module*	NFStream, Wireshark, Tshark, Python, Tensorflow, scikit-learn, PyOD
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.11 Description of Training Module-8: Critical Infrastructure Security in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Critical Infrastructure Security in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Protecting Vital Infrastructure: Security Measures **2.** Critical Systems Security: Safeguarding Infrastructure **3.** Securing Essential Services and Infrastructure **4.** Critical Infrastructure Protection: Security Strategies **5.** Infrastructure Resilience and Security **6.** Safeguarding Critical Assets: Infrastructure Security **7.** Security of Key Infrastructure Systems **8.** Defending Critical Infrastructure from Threats **9.** Infrastructure Security and Resilience Measures **10.** Ensuring Resilient Critical Infrastructure Security **11.** Hardening Critical Systems against Threats
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	All aspects of Critical Infrastructures Security (technological, policy, legal)

Module description *Indicates the main purpose and description of the module*	Definition and characteristics of Critical Infrastructures (CIs) will be identified, common threats and vulnerabilities of the CI technologies (ICT and OT) will be assessed and estimated based on existing standards and methodologies
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	A comprehensive understanding of the challenges, strategies, and best practices involved in securing critical infrastructure systems against various threats and vulnerabilities.
Main topics and content list *A list of main topics and key content*	● Introduction to Critical Infrastructure in <*sector-name*> ● Threat Landscape and Risk Assessment in <*sector-name*> ● Regulations and Standards in <*sector-name*> ● Security and Resilience in <*sector-name*> ● Privacy, Ethical, Legal, and Social Implications in <*sector-name*> ● Cybersecurity for Critical Infrastructure in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing*	*(1) Cybersecurity Management* *(2) Human Aspects of Cybersecurity* *(3) Cybersecurity Risk Management* *(4) Cybersecurity Policy, Process, and Compliance* *(6) Privacy and Data Protection* *(7) Cybersecurity Threat Management*

Apply: *(10)Incident Response*	
Pre-requisites	Basic IT training
Relevance to other Cybersecurity Skills Framework	CISO
Tools to be used *A list of tools that will be used for the operation of this training module*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.12 Description of Training Module-9: Software Security in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Software Security in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	
Module description *Indicates the main purpose and description of the module*	

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	
Main topics and content list *A list of main topics and key content*	● Software Security in <*sector-name*> ● Web & Mobile Security in <*sector-name*> ● Secure Software Lifecycle in <*sector-name*> ● Secure Software Development in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	

Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	(3) Cybersecurity Risk Management (4) Cybersecurity Policy, Process, and Compliance (5) Network and Communications Security (6) Privacy and Data Protection (7) Cybersecurity Threat Management (8) Cybersecurity Tools and Technology (9) Penetration Testing
Pre-requisites	Basic IT training, and suggested minimum know-how in above section

Relevance to other Cybersecurity Skills Framework	Cybersecurity Implementer
Tools to be used *A list of tools that will be used for the operation of this training module*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.13 Description of Training Module-10: Penetration Testing in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (*	***CSP_00x_C_T***

S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme	
Module Title *The title of the training module*	**Penetration Testing in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Ethical Hacking **2.** Security Assessment Testing **3.** Vulnerability Testing **4.** Red Teaming **5.** Security Audit and Testing **6.** White-Hat Hacking" **7.** Cybersecurity Penetration Testing **8.** Network Exploitation Testing **9.** Security Validation Testing **10.** Attack Simulation and Testing
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	The present course aims at providing on-hands training on devices for the <*sector-name*> stakeholders. During the activity a group of trainees will have the opportunity to practise simulated attacks. Most often observed attacks (including attacks via GNSS) are detailed and presented during the course.
Module description *Indicates the main purpose and description of the module*	The main purpose of this course is to describe potential threats and prepare the audience to face a potential attack on devices used by the <*sector-name*> community at a large scale.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	
Main topics and content list *A list of main topics and key content*	● Regulations in <*sector-name*> ● Radiofrequency Communications in <*sector-name*> ● Technologies of Jamming and spoofing in <*sector-name*> ● Past use cases and scenarios in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	

Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	(7) Cybersecurity Threat Management (3) Risk management
Pre-requisites	Basic IT training, and suggested minimum know-how in above section

Relevance to other Cybersecurity Skills Framework	Cybersecurity Educator Chief Information Security Officer Cybersecurity Researcher
Tools to be used *A list of tools that will be used for the operation of this training module*	Nmap Powershell Exploits Mimikatz Hashcat
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.14 Description of Training Module-11: Cyber Ranges and Operations in *<sector-name>*

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Cyber Ranges and Operations in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Offensive Practices **2.** Defensive Practices **3.** Hands-on Cybersecurity Training **4.** Computer and network security in Practice
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type*	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	Advanced hands-on network security educational scenarios including known services, and IoT devices in <*sector-name*>.
Module description *Indicates the main purpose and description of the module*	The current network security educational scenarios are interdisciplinary activities requiring background from various courses such as Computer networks, databases, and Web programming. The scenarios can be executed either collaboratively or competitively, in which case there will be two antagonistic teams: the blue team (defenders) vs the red team

	(attackers). During the scenarios the students will assume various roles such as network engineers, administrators, users, and attackers.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	· Gain interdisciplinary knowledge from Computer networks, databases, and Web programming. · Learn roles such as network engineers, administrators, users, and attackers. · Develop skills in building and managing web applications, including front-end and back-end technologies. · Acquire practical experience in setting up and managing a LAN using various hardware devices. · Understand the process of installing and configuring software on Raspberry Pi and other computers. · Gain expertise in network traffic analysis and security tools. · Perform simulated cyber-attack activities covering the entire attack lifecycle.
Main topics and content list *A list of main topics and key content*	▪ Web Application Development ▪ Web Server Setup and Raspberry Pi Configuration ▪ LAN Construction in <*sector-name*> and Raspberry Pi Roles ▪ Network Monitoring and Attack Simulation in <*sector-name*> ▪ Countermeasures, Testing, and Assessment in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cybersecurity. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	

Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	
Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:*	*(9) Penetration Testing* *(5) Network and Communications Security* *(10) Incident Response* *(8) Cybersecurity Tools and Technology*

(7)Cybersecurity Threat Management *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	
Pre-requisites	▪ Background knowledge in Computer networks, databases, and Web programming. ▪ Familiarity with basic hardware and software used in network security.
Relevance to other Cybersecurity Skills Framework	-Cybersecurity Educator, Cybersecurity Researcher, CISO,
Tools to be used *A list of tools that will be used for the operation of this training module*	▪ Software: HTML, CSS, JavaScript, MySQL, PHP, Apache, Raspbian, LAMP stack. ▪ Hardware: Computers, Raspberry Pi devices, Ethernet switches, WiFi access points. ▪ Network analysis tools: Wireshark, Tcpdump, Xplico, Dshell, etc.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation*	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates	

Indicates the enrolment dates for the operation of this training module	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.15 Description of Training Module-12: Digital Forensics in <*sector-name*>

Code *Code format: CSP00x_T_Sec where T is the type of module (S= seminar, C =course, W=workshop) and Sec is the type of market sector (e.g. M=maritime, E=energy) The purpose of this format is to apply the code to every place you use this module as part of the programme*	***CSP_00x_C_T***
Module Title *The title of the training module*	**Digital Forensics in <*sector name*>**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	**1.** Cyber Forensics **2.** Computer Forensics **3.** Digital Investigation and Analysis **4.** Electronic Forensics **5.** Cybercrime Forensics **6.** Forensic Computing **7.** Incident Response and Forensics **8.** Data Forensics **9.** Forensic Cybersecurity **10.** Information Forensics
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS),*	

Hackathon (H), Other (O). If other, please specify the specific type	
Level *Training level: B (Basic), A (Advanced)*	B, A
Module overview *High-level module overview*	The module introduces learners to digital forensics in <*sector-name*> to equip them with the knowledge and skills to undertake cybercriminal investigations that produce digital evidence that may prove a malicious activity.
Module description *Indicates the main purpose and description of the module*	This module aims to build learners' capacity to conduct cybercrime investigations in <*sector-name*>. It introduces the learner to digital forensics and techniques for conducting forensic examinations. The module also enables learners to examine digital evidence, including data acquisition and identification analysis and how digital evidence artefacts may enable intrusion investigation. To complement automated digital forensic tools, learners are introduced to base Python programming language, which can allow them to conduct forensic tasks such as simulation of attacks, evidence cloning, and port scanning.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a training module*	**Knowledge:** ● Knowledge of digital forensics methods, best practices and tools ● Knowledge of digital forensics analysis techniques ● Knowledge of digital forensics testing techniques ● Knowledge of criminal investigation methodologies and procedures ● Knowledge of malware analysis tools ● Knowledge of cyber threats and vulnerabilities ● Advanced knowledge of cybersecurity attacks tactics and techniques ● Knowledge of legal framework related to cybersecurity and data protection ● Knowledge of operating systems security ● Computer network security **Skills:** ● Work ethically and independently without bias ● Retrieve information while preserving its integrity ● Identifying, analysing, and correlating cybersecurity events ● Report and present digital evidence in an understandable way ● Produce detailed and objective investigative report
Main topics and content list *A list of main topics and key content*	▪ Introduction to digital forensics in <*sector-name*> ▪ Tools for digital forensics in <*sector-name*> ▪ Data/evidence acquisition in <*sector-name*> ▪ Legal aspects of digital forensics in <*sector-name*> ▪ Digital forensics analyses

	▪ Programming for digital forensics in <*sector-name*> ▪ Computing investigation and crime processing in <*sector-name*>
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in a variety of ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions. **Performance-based assessments:** These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies. **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cyber security. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews. **Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cyber security. They can be administered in a variety of ways, such as through observation, self-report, or peer-report.
Training Provider *Name(s) of training providers*	
Contact *Name(s) of the main contact person and their email address*	
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the programme)*	
Duration *Duration of the training*	
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website*	

Knowledge area(s) *Mapping to the 10 selected knowledge areas.* *Analyse:* *(1)Cybersecurity Management* *(2)Human Aspects of Cybersecurity* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance* *Identify:* *(5)Network and Communications Security* *(6) Privacy and Data Protection* *Select:* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *Adapt:* *(9)Penetration Testing* *Apply:* *(10)Incident Response*	*(1) Cybersecurity Management* *(10) Incident Response*
Pre-requisites	Basic IT training, and suggested minimum know-how in above section
Relevance to other Cybersecurity Skills Framework	Digital Forensics Investigator Cyber Incident Responder
Tools to be used *A list of tools that will be used for the operation of this training module*	
Language	

Indicates the spoken language and the language for the material and the assessment/evaluation	
Certification/Certificate *If applicable, the number of ECTS*	
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates *Indicates the enrolment dates for the operation of this training module*	
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description*	

4.3.16 CSP Scheme C: Syllabi of the 12 training modules

(In this section we will provide the syllabi as will be formulated in WP3, for each type of training module (course, seminar. Etc.) for Basic and Advance trainees in the knowledge areas selected by CSP. After the operation (WP4) and evaluation (WP5). We will update them and present the final ones in D5.4)

Penetration Testing

Cybersecurity Tools and Technology

Cybersecurity Management

Cybersecurity Threat Management

Cybersecurity Risk Management

Cybersecurity Policy, Process, and Compliance

Incident Response

Network and Communications Security

Privacy and Data Protection

Human Aspects of Cybersecurity "

4.3.17 Syllabus of the Training Module-1: Cybersecurity Essentials and Management for *<sector-name>*

Main topics	Suggested Content
Ethical Conduct and Professionalism in *<sector-name>*	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field in *<sector-name>*. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security in *<sector-name>*, its business activities, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals in *<sector-name>*, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security in *<sector-name>*. It will also discuss the ethical considerations that need to be considered when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request.
Foundational Knowledge of Cybersecurity in *<sector-name>*	**Introduction to information security:** This section will introduce the concept of information security and its importance to organisations. It will also discuss the different types of information assets that need to be protected, as well as the different threats and vulnerabilities that these assets face. **Introduction to cybersecurity:** This section will focus on the specific threats and vulnerabilities that exist in the cyber domain. It will also discuss the different types of cyber-attacks that can be launched, as well as the different ways to mitigate these attacks. **The CIA triad:** This section will discuss the three pillars of information security: confidentiality, integrity, and availability. It will explain what each pillar means and why it is important. **Other security models:** This section will discuss other security models that can be used to protect information assets. These models include the NIST Cybersecurity Framework, the ISO/IEC 27001

	standard, the COBIT framework, and any other framework that applies to <*sector-name*>.
Cybersecurity Body of Knowledge (CyBoK)	This topic will cover the general overview and foundation of the following key Body of Knowledge (BoK) as it applies to in <*sector-name*>. **Human, Organisational and Regulatory Aspects:** Risk Management & Governance: Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation. **Law & Regulation:** International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare. **Human Factors:** Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours. **Privacy & Online Rights:** Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems. **Attacks and Defences:** Malware & Attack Technologies: Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches. **Adversarial Behaviours:** The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers. **Security Operations & Incident Management:** The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence. Forensics The collection, analysis, & reporting of digital evidence in support of incidents or criminal events. **Systems Security:** Cryptography: Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them. **Operating Systems & Virtualisation Security:** Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems. **Distributed Systems Security:** Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multi-tenant data centres, & distributed ledgers.

	Formal Methods for Security: Formal specification, modelling, and reasoning about the security of systems, software, and protocols, covering the fundamental approaches, techniques and tool support. **Authentication, Authorisation & Accountability:** All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems. **Software and Platform Security:** Software Security: Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems. Web & Mobile Security: Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models. Secure Software Lifecycle: The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default. Infrastructure Security: Applied Cryptography The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems. Network Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security. Hardware Security Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness. Cyber-Physical Systems Security: Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures. Physical Layer & Telecommunications Security: Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.
Threats and Vulnerabilities in *<sector-name>*	**Introduction to threats and vulnerabilities:** This section will introduce the concept of threats and vulnerabilities and how they can impact an organisation's information assets. **Types of threats:** This section will discuss the different types of threats that can impact an organisation's information assets, such as malware, phishing, and social engineering. **Types of vulnerabilities:** This section will discuss the different types of vulnerabilities that can exist in an organisation's information

	systems, such as misconfigurations, outdated software, and poor password management. **Threat modelling:** This section will discuss the process of identifying and assessing threats to an organisation's information assets. **Vulnerability assessment:** This section will discuss the process of identifying and assessing vulnerabilities in an organisation's information systems.
Human Factors in Cybersecurity in <*sector-name*>	**Introduction of the human factors in security:** This section will introduce the concept of the human factor in cybersecurity and its importance. It will also discuss the different ways in which human behaviour can impact cyber security. **Human vulnerabilities:** This section will discuss the different types of human vulnerabilities that can be exploited by cyber attackers. These include things like social engineering, phishing, and password reuse. **Mitigating the human factor:** This section will discuss the different ways to mitigate the risks posed by human vulnerabilities. These include things like security awareness training, strong password policies, and two-factor authentication. **The role of management:** This section will discuss the role that management can play in mitigating the human factor in cybersecurity. This includes things like setting clear security policies and procedures, and providing employees with the resources they need to be secure. **Case studies:** This section will discuss some real-world examples of how the human factor has been exploited by cyber attackers. This can help to illustrate the importance of the human factor in cybersecurity and the need to take steps to mitigate the risks.
Information Security Governance (ISG) and Information Security Risk Management (ISRM) in <*sector-name*>	**Introduction to information security governance and risk assessment and management:** This section will introduce the concept of overarching framework of Information Security Governance (ISG) and how an organisation manages its information security risks. It establishes a vision and strategy for information security, develops and implements policies and procedures, creates a culture of information security, monitors, and measures information security performance, and continuously improves the information security program. Explores risk assessment and management and its importance. It will also discuss the different types of risks that organisations face. **Risk identification:** This section will discuss the process of identifying risks to an organisation's information assets. It will cover tools and techniques that can be used to identify risks. **Risk assessment:** This section will discuss the process of assessing the likelihood and impact of risks. It will cover tools and techniques that can be used to assess risks.

	Risk mitigation: This section will discuss the process of mitigating risks to an organisation's information assets. It will cover different types of risk mitigation controls. **Risk monitoring and updating:** This section will discuss the process of monitoring and updating risk assessments. It will cover how to ensure that risk assessments are kept up-to-date with the changing threat landscape.
Secure Architecture Design and Implementation in <*sector-name*>	**Introduction to Secure Architecture:** In this section students will learn and understand the role of secure architecture in an organisation. Some topics will include identifying the key principles and components of secure architecture recognizing the importance of security architecture in ICT infrastructures and risk management. **Secure Architecture Design and Implementation:** Subsequent sections will cover wide array of topic where student understand to design and develop secure architecture including defining security requirements and constraints, developing a secure architecture model, **Security by Design:** Equips participants with the knowledge and skills relevant to grasping the principles and benefits of security by design, secure software development, least privilege principles, and implementing security in entire lifecycle of organisational processes.secure coding practices
Security Controls Selection and Implementation in <*sector-name*>	**Introduction to security controls:** This section will introduce the concept of security controls and their importance in protecting information assets. **Types of security controls:** This section will discuss the different types of security controls, such as technical controls, administrative controls, and physical controls. **Designing and implementing security controls:** This section will discuss the process of designing and implementing security controls, taking into account the organisation's specific needs and risks. **Managing security controls:** This section will discuss the process of managing security controls, such as monitoring, testing, and updating them. **Evaluating the effectiveness of security controls:** This section will discuss the process of evaluating the effectiveness of security controls to ensure that they are meeting the organisation's needs. **Security control frameworks:** This section will discuss the different security control frameworks that can be used to guide the implementation and management of security controls.
Data Security and Privacy by Design in <*sector-name*>	**Introduction to data security and privacy by design:** This section will introduce the concept of data security and privacy by design, and why it is important.

	Fundamentals of data security: This section will cover the fundamental concepts of data security, such as confidentiality, integrity, and availability. **Privacy by design principles**: This section will discuss the seven privacy by design principles, which are: Proactive not reactive, Privacy as the default setting, Privacy embedded into design, Full functionality – positive-sum, not zero-sum, End-to-end security – full lifecycle protection, Visibility and transparency – keep it open, Respect for user privacy – keep it user-centric. **Data protection impact assessment:** This section will discuss the process of conducting a data protection impact assessment (DPIA), which is a tool to help organisations identify and mitigate privacy risks. **Data security controls:** This section will cover the different types of data security controls that can be used to protect data, such as encryption, access control, and data loss prevention. **Data privacy laws and regulations:** This section will discuss the different data privacy laws and regulations that organisations must comply with, such as the General Data Protection Regulation (GDPR). **Data security best practices:** This section will discuss some of the best practices for data security, such as implementing strong passwords, keeping software up to date, and having a backup plan.
Security Auditing and Compliance in <*sector-name*>	**Introduction to security auditing:** This section will introduce the concept of security auditing and its importance. It will also discuss the different types of security audits. **Security compliance:** This section will discuss the different laws and regulations that organisations must comply with in order to protect their information assets. **Planning and executing a security audit:** This section will discuss the process of planning and executing a security audit. It will also discuss the different tools and techniques that can be used to conduct a security audit. **Reporting on the results of a security audit:** This section will discuss the process of reporting on the results of a security audit. It will also discuss the different ways to communicate the results of a security audit to stakeholders. **Follow-up and remediation:** This section will discuss the process of following up on the results of a security audit and remediating any security vulnerabilities that are identified.
Legal and Ethical Compliance in <*sector-name*>	**Introduction to legal and ethical aspects of cybersecurity:** This section will introduce the concept of legal and ethical aspects of cybersecurity and its importance. It will also discuss the different laws and regulations that govern cybersecurity.

	Data privacy: This section will discuss the laws and regulations that govern data privacy, such as the General Data Protection Regulation (GDPR). **Intellectual property:** This section will discuss the laws and regulations that govern intellectual property, such as copyright and trademark law. **Cybercrime:** This section will discuss the different types of cybercrime, such as hacking, data theft, and ransomware attacks. **Ethical hacking:** This section will discuss the ethical hacking, which is the practice of testing an organisation's computer systems and networks to identify and fix security vulnerabilities. **Responsible disclosure:** This section will discuss the responsible disclosure, which is the practice of reporting security vulnerabilities to the organisation that owns the system or network. **Privacy by design:** This section will discuss the privacy by design, which is a framework for designing products and services with privacy in mind. **Security awareness and training:** This section will discuss the importance of security awareness and training for employees. **Incident response:** This section will discuss the process of responding to and recovering from cyber incidents. **Legal liability:** This section will discuss the legal liability that organisations face for data breaches and other cybersecurity incidents.
Security management standards and frameworks in <*sector-name*>	**Introduction to cybersecurity standards and frameworks:** This section will introduce the concept of cybersecurity standards and frameworks, and their importance. It will also discuss the different types of cybersecurity standards and frameworks in <*sector-name*>. **The EU Standards and Framework:** This section covers the key aspects of the various EU security standards and frameworks in <*sector-name*> including EU Cybersecurity Act, EU NIS Directive, the ENISA Cybersecurity Certification Framework and the ENISA The European Cybersecurity Skills Framework (ECSF) **ISO/IEC 27001:** This section will discuss the ISO/IEC 27001 standard, which is one of the most widely used cybersecurity frameworks. It will cover the key concepts of the standard, such as the risk management process, security controls, and documentation requirements. **NIST Cybersecurity Framework:** This section will discuss the NIST Cybersecurity Framework, which is another widely used cybersecurity framework. It will cover the key concepts of the framework, such as the five functions of cybersecurity, the risk management process, and the implementation tiers. **Other cybersecurity standards and frameworks:** This section will discuss other cybersecurity standards and frameworks, such as the

	Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). **The role of cybersecurity standards and frameworks in information and cyber security management:** This section will discuss the role of cybersecurity standards and frameworks in the overall information and cyber security management process. It will cover how to select the right standards and frameworks for an organisation, how to implement them, and how to measure their effectiveness.

4.3.18 Syllabus of the Training Module-2: Human Factors and Cybersecurity in <*sector-name*>

Main topics	Suggested Content
Ethical and professional practices in <*sector-name*>	**Introduction to ethics and professional conduct in cybersecurity**: This section will introduce the concept of ethics and professional conduct in cybersecurity, and discuss the importance of these principles in the field. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cybersecurity professionals, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security. It will also discuss the ethical considerations that need to be considered when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request. **Adversaries Profiles and Measurements:** Identify aspects, human traits, motives, and opportunities of the adversaries. Classify the profiles and measure the profile. Psychometrics will be overviewed.
Introduction to Human Aspects of Cybersecurity in <*sector-name*>	● **Definition and significance**: An overview of the human element's role and importance of the cybersecurity landscape. ● **Interplay between technology and human behaviour**: Exploring how human actions interact with and influence technological systems. ● **Cybersecurity landscape**: A brief look at the current state of cybersecurity threats and defences. ● **Common misconceptions**: Debunking myths related to the human aspect of cybersecurity.

	● **Cost of neglecting the human element:** Understanding the consequences of overlooking human factors of security. ● **Setting the stage:** Examining real-world incidents to highlight the consequences of human errors.
Psychological and Social Factors in Cybersecurity in <*sector-name*>	● **Understanding cognitive biases:** Understanding inherent biases that influence security decisions. ● **Social engineering techniques**: Exploring social engineering approaches used to deceive individuals. ● **Psychology behind phishing**: Understanding the psychological triggers exploited in phishing attacks. ● **Role of trust:** Examining how trust dynamics impact security behaviours. ● **Group dynamics**: Investigating how group interactions can influence individual security actions. ● **Emotional factors**: Gaining an understanding of how emotions like fear and curiosity affect cybersecurity decisions.
Human Vulnerabilities in Cybersecurity in <*sector-name*>	● **Cataloguing common errors**: Listing frequent human mistakes that lead to security breaches. ● **Insider threats**: Differentiating between intentional malicious actions and unintentional human errors within an organisation. ● **Impact of stress and fatigue**: Understanding how physical and mental strain can compromise security decisions. ● **Challenge of maintaining vigilance**: Discussing the difficulty of staying consistently alert to security threats in. ● **Case studies**: Analysing real incidents to understand the role of human vulnerabilities. ● **Mitigation strategies:** Identifying solutions to reduce risks associated with human vulnerabilities.
Organisational Culture, Communication, and Cybersecurity in <*sector-name*>	● **Organisational values:** Exploring how a company's core values influence its security posture. ● **Ripple effect:** Understanding how a single decision can have widespread implications for an organisation's security. ● **Leadership's role**: Understanding how different leadership styles influence setting communication standards and security priorities. ● **Feedback loops**: Discussing the significance of continuous feedback in improving cybersecurity measures. ● **Proactive security culture**: Strategies to cultivate an anticipatory approach to threats. ● **Overcoming resistance**: Addressing challenges in changing established culture and security practices.
Communication and Collaboration Across Domains in <*sector-name*>	● **Effective communication:** Understanding factors of successful communication in cybersecurity. ● **Challenges in collaboration:** Identifying obstacles in inter-domain cooperation and their solutions. ● **Building bridges**: Strategies to enhance collaboration across domains. ● **Role of mediators**: Understanding the importance of

	intermediaries in facilitating effective communication. ● **Case studies:** Analysing instances of successful and failed collaborations. ● **Communication tools:** Having an oversight of platforms and tools that aid in effective communication.
Decision Making at Strategic, Operational, and Tactical Levels in <*sector-name*>	● **Layers of decision-making:** Understanding the different levels of decision-making in cybersecurity. ● **Interdependence of decisions**: Understanding how decisions at one level can influence actions at other levels. ● **Communication channels:** Discussing appropriate communication methods for each decision-making level. ● **Balancing speed and accuracy**: Strategies to make timely yet informed decisions. ● **Role of data**: Emphasising the importance of data-driven decision-making. ● **Case studies:** Analysing real-world decisions made during cybersecurity incidents.
Training, Awareness, and Communication Programs in <*sector-name*>	● **Impactful training:** Designing effective targeted cybersecurity training programmes that meet participant needs. ● **Continuous education**: The importance of continued professional development in adapting to evolving threats. ● **Tailored training**: Customising training programmes targeted groups. ● **Feedback:** The significance of integrating feedback to improve training modules. ● **Measuring effectiveness**: Techniques to assess the success and impact of training initiatives. ● **Leveraging technology:** Using modern technological tools to enhance training experiences.
Future Trends, Challenges, and the Role of Communication in <*sector-name*>	● **Anticipating threats:** Predicting upcoming cybersecurity challenges. ● **Emerging technologies:** Understanding how new technological trends will shape human interactions and communication patterns. ● **Interdisciplinary collaboration:** Understanding and leveraging the growing need for cooperation across various fields in cybersecurity. ● **Remote workforces:** Preparing for security challenges posed by decentralised teams and workforces. ● **AI and automation:** Exploring the influence of artificial intelligence on human behaviour in cybersecurity. ● **Staying ahead:** Strategies to remain updated in a rapidly evolving cybersecurity environment.

4.3.19 Syllabus of the Training Module-3: Cybersecurity Risk Management and Governance in <*sector-name*>

Main topics	Suggested Content
Introduction to Information Security in <*sector-name*>	This topic covers the basic terms and definitions that the participants should be acquainted with to facilitate better / uniform understanding. The terms introduced in this section are derived from various standards (e.g., ISO/IEC), initiatives (e.g., NIST, ENISA) and guidlines, standards, legal and EU policies related to security management will be presented and analysed.
The ISO/IEC family of standards in <*sector-name*>	As part of this topic, various standards are explored (e.g., the ISO 27k family). This overview includes vocabulary and basic principles, standards containing requirements (e.g., ISO/IEC 27001:2022, ISO 27799:2019, ISO 27006), standards providing guidance and best practices on controls (e.g., ISO/IEC 27002:2022, ISO 27035-1), and others.
The scope and purpose of an ISMS in <*sector-name*>	Within this topic, information is provided on what is an ISMS and which are the benefits and objectives of its implementation. Within this topic, the differences between the implementation of individual controls and the implementation of an ISMS are demonstrated.
The PDCA cycle in <*sector-name*>	This topic describes the Plan-Do-Check-Act cycle and the relationship between the phases and the Information Security Management System. The advantages and alternatives of this approach are also discussed.
The requirements of ISO 27001 - clauses 4-10 in <*sector-name*>	This topic discusses in depth the requirements of the clauses of ISO 27001. Through a series of examples and exercises, participants are guided through the implementation steps and mandatory requirements of an Information Security Management system. The topics discussed include elements like context, Information Security Policy, Role and Responsibilities, audits, change management, objectives, management review, monitoring and measurement and corrective actions. Within this topic the mandatory minimum documentation related to an ISO/IEC 27001:2022 implementation, is presented and discussed.
Information Security Risk Management definitions and principles in <*sector-name*> Threats and vulnerabilities in <*sector-name*> ISO 27005 and ISO 31000 basic structure	This topic introduces the key component of an Information Security Management System - risk management. Specifically, the basic terms related to risk management are introduced as well as the phases proposed by international standards (i.e. ISO 31000 and ISO 27005) as needed for an effective implementation of information security risk management. The phases of a risk management process are explained, and an exercise is performed to cover the following phases: Context - Risk identification - Risk Analysis - Risk Evaluation - Risk Treatment.

	The phases of recording and reporting, monitoring and review and communication are described.
Threat Models, Technical Vulnerabilities, and Measurements in <*sector-name*>	Technical and non-technical threats and vulnerabilities will be analysed. The various metrics systems (e.g. CVE, CVSS4, CWE) will be presented and illustrated with various examples.
Other Risk Assessment methodologies and tools in <*sector-name*>	This topic introduces a list of risk assessment methodologies and tools. Exercises are carried out using a specific methodology and a tool. Comparisons are made between the approaches and results. The ENISA interoperability framework is described and discussed.
The Annex A of ISO/IEC 27001:2022 in <*sector-name*>	This topic describes the concept behind the Annex A controls and risk management. The structure of the controls (in themes) and the usage of attributes is described. Examples of controls (one per theme) will be incorporated in an implementation exercise taking into consideration the guidance of ISO/IEC 27002. Non-technical mitigation actions will be presented.
Security Policies and Procedures in <*sector-name*>	The development of security policy, BCP, DRP and procedures based on standards will be covered in this section. The human element in the risk assessment process will be analysed.
Certificates and certification in <*sector-name*>	This topic introduces the concept of certification; conformity assessment related standards and methodologies
Cybersecurity Maturity Models and Open Issues in <*sector-name*>	Cybersecurity Maturity models have been introduced for Cybersecurity in the last 10 years. Some of them have already been incorporated in laws or are being presented as best practices for organisations. This topic presents the history and rationale of the maturity models in cybersecurity. Specific examples of cybersecurity maturity models are presented, and their usage is explained through relevant exercises. Cyber Security challenges in managing the risks of the emerging technologies will be analysed.

4.3.20 Syllabus of the Training Module-4: Network Security in <*sector-name*>

Main topics	Suggested Content
Basic network fundamentals, architectures, and protocols in <*sector-name*>	**Emergence of networks - from the Internet to advanced network ecosystems**: This topic will provide an overview of the most important technological developments and their influence on the growth of networks and connectivity; from the origin of the Internet to the emergence of more advanced communication networks, such as IoT and mobile networks.

	The aim is to highlight the relevance of networks for society, discussing how IoT devices can change the security landscape and emphasising the complexity that the new interconnection ecosystems may bring. **Introduction to Internet infrastructures and native protocols:** This topic will review the basic knowledge of networking and the main communication structures (e.g., OSI model, TCP/IP model) together with their native protocols and mechanisms. This will help to lay the foundation for the other topics introduced in this particular module, and specific for cybersecurity, such as the influence of ICMP for verifying the liveness of a node within a network, routing, Network Address Translation (NAT), etc. **Current network architectures:** This section will explore the diverse network architectures, their basic constructions and the benefits and drawbacks that these may bring to the new ecosystems. In this networks spectrum, we will consider the general implications that may bring the wired networks (Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN)), wireless (WLAN and WMAN), mobile networks (Global System for Mobile Communication (GSM) and following networks like 3G - 6G), and the use of virtualized systems such as SDN for large ecosystems. **Existing interconnection devices:** Beyond the network architectures defined in the previous point, it is also essential to know the use and function of the interconnection devices, as this knowledge will help to lay the foundations and clarify the knowledge (especially in attack and hardening modes).
Common weaknesses and attacks in communication networks in <*sector-name*>	**Main vulnerabilities and bad practices:** This topic will highlight the relevance of designing and deploying secure networks following basic hardening principles. It will detail an overview of the main vulnerabilities and/or weaknesses committed by experts, administrators and users in communications systems and related environments, and consider existing standards, recommendations and/or best practices that help to mitigate or avoid such problems. **Threat models and common attacks:** This topic will address ways of modelling potential network threats in various communication environments (whether based on TCP/IP or other protocols, and whether fixed-line-based, wireless or mobile networks), and including profiles and interests of attackers. In this regard, formal methods, such as the typical Dolev-Yao model, will be considered, and the most common attacks and their general countermeasures will be addressed as particular examples of these situations, including distributed denial of services, botnet, malware exploitation, infection of network systems, movement profiles, etc. **Typical offensive tools**: To complement the objectives of the previous point, a set of offensive tools will be presented to show their technical capabilities that can jeopardise the confidentiality, integrity and availability of a system and of its users. In this case, we could consider from existing frameworks, such as Metasploit, to hacking tools included in the different Linux distributions. **Demonstration of attacks, replication, testing, mitigation, post-attack remedies**: This topic will cover the use of Wireshark, visualisation of

	attack demonstrations, attack replication, exploration of test mitigation methods, recommendations for network configurations (virtual and/or physical), and post-attack policies.
Main security protocols embedded in the traditional communication stack in *<sector-name>*	**Application-layer security:** This topic will address all those security protocols deployed at the application layer, such as Secure Shell (SSH), Domain Name System (DNS) Security, Pretty Good Privacy (PGP) or Secure Multipurpose Internet Mail Extensions (SMIME), etc. **Transport-layer security:** This topic will address all those security protocols deployed at the transport layer, and consider those with support in Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). In particular, we will explore the Transport Layer Security (TLS) protocol, highlighting the benefits of the latest versions and their main applicability. We will also detail UDP security protocols such as Datagram Transport Layer Security (DTLS) and Quick UDP Internet Connections (QUIC), their main functions and features. **Network-layer security:** This topic will also contemplate all those security protocols deployed at the network layer, such as IPSec, and how these can be essential to build Virtual Network Privates (VPNs). **Link-layer security:** This topic will also contemplate all those security measures deployed at the link layer, and particularly looking at the protection of wireless networks. For the latter, we will take into account the existing security protocols for the key management in specific networks such as WiFi, confidentiality and integrity, as well as authentication, authorisation and accounting, e.g., making use of the Extensible Authentication Protocol (EAP) under the IEEE 802.1X Port-based Authentication.
Perimeter defence and protection tools in *<sector-name>*	**Network segmentation:** This topic will cover all those security mechanisms that ensure the segmentation/isolation of networks. This ranges from the use of diode communication to virtual LANs (VLANs), application proxies or gateways, firewalls and demilitarised zones, commonly known as DMZs. **Virtual private networks:** This topic will show a spectrum of existing solutions to create VPNs, either from the link level to the network and transport level, highlighting the relevance of the IPSec protocol, as well as its different tunnelling modes (ESP, AH and IKE, and transport and tunnel). **Intrusion detection and prevention:** This topic will include the most typical mechanisms of intrusion detection and prevention together with their main components, their detection methods (comparing their strengths and weaknesses against specific types of attacks such as advanced persistent threats), and exploring the most typical existing detection tools such as snort or suricata. **Deception and feedback:** As an extension of the previous point, this topic will also address the main deception mechanisms applied to capture malicious actions and feed existing prevention mechanisms. This will involve providing an overview of existing strategies and available tools, as well as their implications within a corporate network.

	Network security monitoring: It is also essential to highlight the relevance of collecting multiple data from multiple endpoints and locations to explain the progress and emergence of a potential threat within a broader context, such as distributed systems and IoT. Therefore, this section will highlight the main components that help to explain at a high level the progress of a threat within a network, and the relevance that SIEM (Security Information and Event Management) systems could have in this regard.
Security of end communication nodes and of interconnection systems in *<sector-name>*	**Protection of the final elements of the communication:** In any client-server communication it is also essential to protect the final elements involved in such communication, in this case, the nodes acting as client and server. Therefore, this section will present the main vulnerabilities concentrated on these elements, and in relation to port control, services and firewalls of the operating system, and web security. **Hardening of the interconnection elements:** The protection of intermediary elements is also essential to ensure secure communication between a client and a server. Therefore, this topic will present some general recommendations on how to maintain proper and controlled access on routers, taking into account per-user control and closing unnecessary or insecure ports.
Security in advanced network infrastructures in *<sector-name>*	**Introduction to distributed and advanced networks:** This topic will present the different communication models beyond the typical TCP/IP-based one, such as those based on cloud/edge networks, decentralised systems such as blockchain, and virtualized systems such as SDN, as well as their main security issues. **Distributed/decentralised networks, and their security measures:** In addition to introducing the characteristics of this type of networks, such as IoT/IIoT or blockchain, and their main drawbacks from a security point of view, existing protection measures for the access control will be addressed. **Mobile telecommunication infrastructures, and their security measures**: This topic will contemplate the role of the GSM and following mobile technologies; security and privacy models and assumptions, issues with cell-based communication and the corresponding routing and movement profiles. Likewise, this section will explore the main security issues and features of mobile networks like SIM based authentication and network access via challenge-response protocols. **Virtualised network infrastructures, and their security measures:** Beyond wired and wireless systems, it is possible to find other types of networks based on virtualized communications such as SDNs. In this sense, it is essential to consider the most relevant security threats and the main measures to protect not only the virtual communications but also the virtualized environment.
Privacy and anonymity in communication networks in *<sector-name>*	**Introduction to anonymous communications:** This topic will detail the threat model and the most common attacks against node privacy (location privacy), as well as present the main principles and properties of

	anonymity in such systems. **Anonymity strategies:** This topic will be devoted to presenting the different protection mechanisms, considering those based on randomization and rooting, such as The Onion Router (TOR). **Location tracking and movement profiles:** This section will explore the various mechanisms and methods of location tracking as well as movement profiling endangering anonymity in communication networks.

4.3.21 Syllabus of the Training Module-5: Data Protection and Privacy Technologies in <*sector-name*>

Main topics	Suggested Content
Ethical and professional practices	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security. It will also discuss the ethical considerations that need to be taken into account when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request.
Data Protection and Identity Management (IdM)	Introduction into IdM, especially the difference between identity and identifier; Issues of overidentification; IdM architectures and the information flows therein. Related standards, especially ISO/IEC 24760 “A framework for identity management”.
Location information and its privacy impact	Collection of location information, especially in cellular mobile telecommunication networks, and the uses of the data enabling movement profiles.Protection approaches against these attacks.
Seminars on implementing security policies and architectures	Providing architectural knowledge depending on the scenario for cryptography, privacy policies, anonymization, avoidance of (movement) profiling, good security, and privacy practices.

4.3.22 Syllabus of the Training Module-6: Cyber Threat Intelligence in <*sector-name*>

Main topics	Suggested Content
Cyber threats taxonomy and threat intelligence in <*sector-name*>	Cyber threats and types of threats Attacks and Mitigations Attack actors Introduction to malware taxonomy: Vectors of infection, Software-Borne threats, Payload functionality Static and dynamic malware analysis, malware spread Advanced persistent threat
Legal Instruments and Standards in <*sector-name*>	Relevant EU cybersecurity legislation EU cybersecurity standards
Vulnerabilities assessment techniques in <*sector-name*>	Basic of vulnerability, vulnerability groups, vulnerability exploitation, Zero Day Exploit Vulnerability types Vulnerability database and entries Common vulnerability scoring system- 3.1 and 4.0 Vulnerability exploitation
Threat modelling and hunting in <*sector-name*>	Threat modelling Threat modelling techniques- STRIDE, DREAD, Attack tree, Kill chain Report on threat modelling Important of threat hunting, human vs tool centric, threat hunting methodology Threat hunting maturity model MITRE ATT&CK Framework
Threat intelligence information sharing standard and reporting, threat feed in <*sector-name*>	Cyber threat intelligence- concept, properties, types , process Indicator of compromise- host and network based Threat feed platform and sharing Data Security
Security controls in <*sector-name*>	Goals of security control, security control types, security control functions, Access control properties, patch management, CIS Critical

	Security Controls

4.3.23 Syllabus of the Training Module-7: Cybersecurity in Emerging Technologies in *<sector-name>*

Main topics	**Suggested Content**
AI on cybersecurity in <*sector-name*>	The section explores the reciprocal influence of AI and cybersecurity. It will cover the three dimensions in which AI and cybersecurity intersect, covering challenges and opportunities from the offensive and defensive aspects. Examples will include adversary penetration testing and emerging challenges of adversarial AI through a blend of theoretical and practical exercises. It covers various facets of this intersection, including adversary penetration testing, intrusion detection systems (IDS), Security Information and Event Management (SIEM) systems, and the emerging challenge of adversarial AI. Through a blend of theoretical knowledge and practical exercises, students gain a comprehensive understanding of how AI can be applied defensively and offensively in cybersecurity, focusing on building expertise in AI-driven penetration testing, enhancing IDS and SIEM with AI, and defending against adversarial AI attacks.
Anomaly detection techniques in <*sector-name*>	**Introduction to Anomaly Detection:** In this section, we will delve into the concept of anomalies, examining their nature as unexpected deviations from the norm. We'll explore anomaly detection’s significance and diverse applications, emphasising different types such as point anomalies, contextual anomalies, and collective anomalies. Throughout the session, we'll also address the challenges inherent in anomaly detection, fostering a comprehensive understanding of this critical aspect of cybersecurity. **Machine Learning-Based Method:** In this section, we focus on machine learning-based methods and explore various anomaly detection approaches based on supervised and unsupervised machine learning algorithms. We will discuss the evaluation metrics crucial for assessing the effectiveness of these methods, including precision, recall, and F1-score. Through this content, participants will gain insights into the practical applications and considerations associated with deploying machine learning models for anomaly detection. **Time Series Anomaly Detection**: In this section, we will explore the complexities associated with detecting anomalies in time series data. We will investigate fundamental techniques such as moving averages and exponential smoothing as well as the Seasonal-Trend decomposition using Loess (STL) method. Moreover, we'll introduce advanced approaches, including Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN)-based methods tailored for analysing time series data. **Anomaly Detection in Real-World Applications:** We will present real use-case scenarios using data from various sources such as IoT devices,

	network traffic logs and similar.
Cloud security in *<sector-name>*	This section is designed to provide trainees with a deep understanding of the unique challenges and best practices associated with securing cloud computing environments. As organisations increasingly migrate their data and services to the cloud, there is a growing need for professionals who can ensure the security and compliance of cloud-based infrastructures. This module covers cloud security concepts, strategies, and technologies to prepare students for the complexities of safeguarding data and applications in the cloud.
IoT security in *<sector-name>*	This section is designed to provide trainees with a comprehensive understanding of the principles, strategies, and best practices for securing modern networks and the Internet of Things (IoT) ecosystems. In an increasingly interconnected world, the security of networks and IoT devices is paramount. This module covers the fundamentals of network security and delves into the unique challenges posed by IoT devices, preparing students to protect critical data and infrastructure.
Data analysis for cybersecurity in *<sector-name>*	This section is designed to equip trainees with the knowledge and skills needed to harness the power of data analytics and machine learning in the context of cybersecurity. In today's rapidly evolving threat landscape, organisations rely on data-driven insights to detect and respond to cyber threats effectively. This module explores various data analysis techniques and tools, emphasising their application to cybersecurity scenarios.

4.3.24 Syllabus of the Training Module-8: Critical Infrastructure Security in *<sector-name>*

Main topics	Suggested Content
Ethical and professional practices	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security. It will also discuss the ethical considerations that need to be considered when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the

	General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request.
Introduction to Critical Infrastructure in <*sector-name*>	▪ Definition and significance of critical infrastructure ▪ Sectors and examples of critical infrastructure (energy, transportation, water, etc.) ▪ Interdependencies between various critical systems
Threat Landscape and Risk Assessment in <*sector-name*>	▪ Identifying threats and vulnerabilities to critical infrastructure ▪ Risk assessment methodologies specific to critical systems ▪ Understanding cyber, physical, and natural threats
Regulations and Standards in <*sector-name*>	▪ Overview of regulatory frameworks and standards (e.g., NIST, ISO, ENISA, ETSI guidelines) ▪ Compliance requirements for critical infrastructure security
Security and Resilience in <*sector-name*>	▪ Risk treatment plan and Security Policy ▪ Disaster Recovery Plan ▪ Business Continuity Plan
Ethical, Legal, and Social Implications in <*sector-name*>	▪ Ethical considerations in critical infrastructure security ▪ Legal aspects and privacy concerns ▪ Social impacts and community resilience
Cybersecurity for Critical Infrastructure in <*sector-name*>	▪ Cyber threats to critical systems ▪ Network security, including firewalls, intrusion detection systems, and encryption ▪ Incident response and recovery plans for cyber attacks

4.3.25 Syllabus of the Training Module-9: Software Security in <*sector-name*>

Main topics	Suggested Content
Ethical and professional practices	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals, such as confidentiality, integrity, and availability.

	Introduction to legal and ethical aspects of information security: This section will discuss the laws and regulations that govern information security. It will also discuss the ethical considerations that need to be taken into account when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request.
Software Security in <*sector-name*>	**Introductory definition and terms** - The CIA triad - Security - Vulnerability - Security failure - Bugs / Implementation vulnerabilities **Categories of vulnerabilities** - Memory management vulnerabilities - Structured output generation vulnerabilities - Race condition vulnerabilities - API vulnerabilities - Side-channel vulnerabilities **Prevention of vulnerabilities** - Language design and type systems - API design - Coding practices **Detection of vulnerabilities** - Static detection - Dynamic detection **Mitigating exploitation of vulnerabilities** - Runtime detection of attacks - Automated software diversity - Limiting privileges - Software integrity checking
Web & Mobile Security in <*sector-name*>	**Fundamental concepts and approaches** - Appification - Webification - Application stores - Sandboxing - Permission dialog based access control - Web PKI and HTTPS - Authentication - Cookies - Passwords and alternatives

	- Frequent software updates **Client side vulnerabilities and mitigations** - Phishing & clickjacking - Client side storage - Physical attacks **Server side vulnerabilities and mitigations** - Injection vulnerabilities - Server side misconfigurations & vulnerable components
Secure Software Lifecycle in *<sector-name>*	**Motivation** **Prescriptive secure software lifecycle processes** - Secure software lifecycle processes - Comparing the secure software lifecycle models **Adaptations of the secure software lifecycle** - Agile software development and DevOps - Mobile - Cloud computing - Internet of Things (IoT) - Road Vehicles - ECommerce / Payment card industry **Assessing the secure software lifecycle** - The Software Assurance Maturity Model (SAMM) - The Building Security In Maturity Model (BSIMM) - The Common Criteria (CC) **Adapting a secure software lifecycle**
Secure Software Development in *<sector-name>*	**Software design risk management** - Threats, vulnerabilities, and impact analysis - Risk calculation - Countermeasures definition **Secure coding practices** - Input validation - Output encoding - Error handling and logging - Secure API usage - Common coding vulnerabilities mitigation **Third-party dependencies validation** - Libraries, frameworks, and components validation **Secure configuration management** - Servers, frameworks, and system components secure configuration **Security testing** - Vulnerability assessment

	- Penetration testing - Code reviews **Data protection** - Encryption algorithms - Secure key management - Role-based access control (RBAC) - Least privilege principles **Sensitive data protection** - Personally Identifiable Information (PII), Personal Health Information (PHI), and Payment Card Industry (PCI) data - Passwords, API keys, tokens, and credentials

4.3.26 Syllabus of the Training Module-10: Penetration Testing in <*sector-name*>

Main topics	Suggested Content
Ethical and professional practices	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security. It will also discuss the ethical considerations that need to be considered when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose confidential information or when to comply with an illegal request.
Regulations in <*sector-name*>	
Radiofrequency Communications in <*sector-name*>	
Technologies of Jamming and	

spoofing in <*sector-name*>	
Past use cases and scenarios in <*sector-name*>	

4.3.27 Syllabus of the Training Module-11: Cyber Ranges and Operations in <*sector-name*>

Main topics	Suggested Content
Web Application Development	**Front-End Development:** Students build the front-end of the web application using HTML, CSS, and JavaScript. **Back-End Development:** Creation of the back-end with a MySQL database and PHP or another programming language. **Initial Concept and Design:** Discussing and planning the overall functionality and design of the web application.
Web Server Setup and Raspberry Pi Configuration	**Web Server Installation**: Installing and configuring Apache on a Raspberry Pi. **LAMP Stack Setup**: Setting up Linux, Apache, MySQL, PHP (LAMP stack), and phpMyAdmin on Raspberry Pi for web hosting. **Operating System Installation**: Students install Raspbian on Raspberry Pi devices.
LAN Construction in <*sector-name*>, and Raspberry Pi Roles	**Building a LAN**: Using Ethernet switches and WiFi access points to construct a LAN. **Raspberry Pi as DNS/DHCP Server**: Configuring the second Raspberry Pi to serve as a DNS and DHCP server with dnsmasq. **Raspberry Pi as Malicious Actor**: Preparing the third Raspberry Pi to simulate a malicious threat actor, including cloning the web application's front-end and writing/installing malware.

Network Monitoring and Attack Simulation in *<sector-name>*	**Security Tool Installation**: Setting up network monitoring and security tools such as Wireshark, firewall, nmap, IP scanner. **Attack Simulations**: Students conduct reconnaissance, enumeration, and various attacks (DNS poisoning, ARP poisoning, DoS attacks, SQL injection, CSRF, XSS, etc.). **Traffic Analysis and Recognition**: Recording and analyzing network traffic to recognize and understand the attacks.
Countermeasures, Testing, and Assessment in *<sector-name>*	**Implementing Countermeasures**: Students develop and apply strategies to counter the simulated attacks. **Solution Testing**: Testing the effectiveness of their security solutions. **Wrap-Up and Conclusions**: Discussion and analysis of the exercises, what was learned, and areas for improvement. **Student and Scenario Assessment**: Evaluating student performance and obtaining feedback on the educational scenario from students and instructors.

4.3.28 Syllabus of the Training Module-12: Digital Forensics in *<sector-name>*

Main topics	Suggested Content
Introduction to digital forensics in *<sector-name>*	Understand the fundamentals of general forensic science and digital forensics; Benefits of digital forensics; Digital forensics process
Tools for digital forensics in *<sector-name>*	Hardware and software tools; Tools selection and validation; Digital forensics quality assurance
Data/evidence acquisition in *<sector-name>*	Understanding data storage formats and digital evidence; Acquisition tools, and determination of best acquisition methods; Validation of data acquisitions
Legal aspects of digital forensics in *<sector-name>*	Understanding the legal aspects of digital forensics and their impact on digital forensics
Digital forensics analyses	Malware analysis; Volatile memory analysis; Timeline analysis; Intrusion analysis;

Programming for digital forensics in <*sector-name*>	Understanding Python programming for digital forensics; Use of Python base programming for performing tasks such as simulation of attacks, port scanning, website cloning, load generation and testing of a website, wireless network scanning, transmission of traffic in the network etc.
Computing investigation and crime processing in <*sector-name*>	Digital forensics process model: Introduction to cybercrime scenes; Scene and evidence documentation; Chain of custody; Forensic evidence cloning; Integrity of evidence; reporting;

Annex A: Glossary and Terms

Term	Abbreviation	Definition(s)	Reference	Example(s)	Notes/ Remarks
Security Concepts					
Accountability	-	the state of being answerable (in response) for assigned actions and decisions.	ISO/IEC 27000:2018		
Attack	-	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.	ISO/IEC 27000:2018	Attack on a SCADA software (cyber), attack on a cruise terminal (physical).	
Attack path (attack model/attack pattern/attack vector)	-	1. Attack path: Steps that a threat takes or may take to plan, prepare for, and execute an attack [API standard 780]. 2. Attack pattern: abstracted approach utilized to attack software [ISO/IEC TR 20004:2015]. 3. Attack vector: path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome [ISO/IEC 27032:2012].	1. API standard 780, 2. ISO/IEC TR 20004:2015 , 3. ISO/IEC 27032:2012	attack path to compromise a CCTV system of an enterprise: compromise an e-mail account to gain access to an employee's workstation of an enterprise and after take advantage of a CCTV server that is installed in the workstation operating system	

Attack Potential (means, skills, opportunities)	-	(1) Measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation. (2) Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.	1. ISO/IEC 15408-1:2009 (CC) 2. ISO/IEC 27032:2012		- Attack potential can be estimated *Basic* or *Enhanced-basic* or *Moderate* or *High*. - 'Attack potential' is used to prove or deny the TOE security functionality remains in the secure state regardless if the vulnerability is identified or discovered.
Attacker (adversary/ threat agent)	-	1. Adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities [NIST SP 800-30 Rev 1, 2012]. 2. Attacker: an actor who attempts to gain access to behaviors or resources that are outside of the product's intended control sphere for that actor [MITRE glossary]. 3. Threat agent: entity that can adversely act on assets [ISO/IEC 15408-1:2009].	1. NIST SP 800-30 Rev 1, 2012, 2. MITRE glossary online available: https://cwe.mitre.org/documents/glossary, 3.. ISO/IEC 15408-1:2009	For instance, an attacker can be a disgruntled employee (insider), a hacktivist, a cybercriminal, a terrorist group, a pirate or a hijacker, a cyber vandal, a government/industry spy.	
Authenticity	-	Property that an entity is what it claims to be.	ISO/IEC 27000:2018		

Availability	-	Property of being accessible and usable on demand by an authorized entity.	ISO/IEC 27000:2018		
Common Vulnerabilities and Exposures	CVE	1. A nomenclature and dictionary of security-related software flaws. 2. A list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.	1. NIST SP 800-126 Rev. 2, 2. MITRE: online available: https://cve.mitre.org/	The confirmed vulnerability example of Microsoft Teams Remote Code Execution has the CVE (Id) "CVE-2020-17091"	(1) CVEs are designated by the CVE Numbering Authorities (CNAs), namely organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. The MITRE Corporation functions as Editor and Primary CNA. (2) NIST repository for vulnerabilities NVD is utilized to identify vulnerability on an asset. Useful links to search forCVEs: https://nvd.nist.gov/v

					uln,https://www.cvedetails.com/
Common Vulnerability Scoring System	CVSS	The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. It mainly consists of three metric groups: Base, Temporal, and Environmental.	FIRST CVSS v3.1 Specification, Rev.1 online available: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf , [MITRE] https://nvd.nist.gov/vuln-metrics/cvss	For instance, the confirmed vulnerability "CVE-2020-17091" Microsoft Teams Remote Code Execution has *Basic score metrics= 7.8* : Exploitability<AV= Local/AC=Low PR=None / UI=Required *Impact*<C= High I=High A=High *Temporal score metrics = 6.8 :* E= Unproven RL=Official fix RC=Confirmed	(1) CVSS is designed to measure the severity of a vulnerability. The score leverages Basic, Temporal and Environmental) CVSS is designed to measure the severity of a vulnerability. The score leverages Basic, Temporal and Environmental Metrics. (2) CVSS has been recognized as an international standard for scoring vulnerabilities.

Common Weakness Enumeration	CWE	A community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.	[MITRE] online availiable: https://cwe.mitre.org/	CWE-20 Improper Input Validation: the asset does not validate or incorrectly validates input that can affect the control flow or data flow of a program.When software fails to validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.	CWE is assigned by MITRE. This leads to a mapping of vulnerabilities to the related threats.
Confidentiality	-	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO/IEC 27000:2018		
Confirmed Vulnerability	-	Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the affected code has confirmed the presence of the vulnerability.	CVSS v3.1 NIST NVD (FIRST)	A confirmed vulnerability example is the vulnerability of Microsoft Teams Remote Code Execution, which was published on 11/11/2020.	

Control	-	1. Measure that maintains and/or modifies risk [ISO 31000: 2018; ISO/IEC 27000:2018]. 2. Controls include any process, policy, device, practice, or other actions which modify risk. It is possible that controls not always exert the intended or assumed modifying effect. [ISO/IEC 27000:2018]	1. ISO 31000: 2018 1.,2. ISO/IEC 27000:2018	Control – term used in [CSA, Art. 52.4]: “The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.” This term can be seen as equivalent to the Security Functional Requirements (SFRs) defined in ISO15408.	
Control objective	-	Statement describing what is to be achieved as a result of implementing controls.	ISO/IEC 27000:2018		
Cyber attack	-	An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.	NIST SP 800-30 Rev 1, 2012	Man-In the-Middle attack cinderella attack ransomware attack	

Exploitable Vulnerability	-	Weakness in the TOE *that can be used to violate the SFRs in the operational environment* for the TOE.	ISO/IEC 15408-1:2009 (CC)		
Impact	-	The result of an unwanted incident	ISO/IEC PDTR 13335-1		

Impact level	-	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.	NIST SP 800-37 Rev.2, 2018		
Information security	-	Preservation of the CIA triad (Confidentiality, Integrity and Availability) of information involving also the ensurance of other properties such as authenticity, accountability, non-repudiation, and reliability.	ISO/IEC 27000:2018		

Integrity	-	Property of accuracy and completeness.	ISO/IEC 27000:2018		
Level of risk	-	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.	ISO/IEC 27000:2018		
Likelihood of occurrence	-	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Determining the likelihood of threat events causing adverse impacts.	NISTIR 7621 Rev. 1, 2016, CNSSI 4009-2015, NIST SP 800-30 Rev 1, 2012		

Non-repudiation	-	Ability to prove the occurrence of a claimed event or action and its originating entities.	ISO/IEC 27000:2018		
Potential (uknown) Vulnerability	-	1. Potential: Suspected, but not confirmed, weakness 2. Uknown: There are reports of impacts that indicate a vulnerability is present, but that the cause of the vulnerability is unknown or they may differ on the cause or impacts of the vulnerability. Reporters are uncertain of the true nature of the vulnerability, and there is little confidence in the validity of the reports.	1. ISO/IEC 15408-1:2009 (CC), 2. CVSS v3.1 NIST NVD (FIRST)	An unknown/zero day vulnerability could be an adversary that sneaks in an asset through a backdoor that was left unlocked by accident.	Suspicion is by virtue of a postulated attack path to violate the SFRs. A sub-category of this is the "zero-day" vulnerability, which is related to a security flaw in the software that is known to the software vendor, but with no patch in place to fix the flaw.

Reliability	-	Property of consistent intended behaviour and results.	ISO/IEC 27000:2018		
Residual risk	-	Risk remaining after risk treatment. Residual risk can contain unidentified risk. It can also be referred to as “retained risk”.	ISO/IEC 27000:2018		
Residual Vulnerability	-	Weakness *that cannot be exploited in the operational environment for the TOE, but could be used to violate the SFRs* by an attacker with greater attack potential than is anticipated in the operational environment for the TOE.	ISO/IEC 15408-1:2009 (CC)		
Risk Assessment	RA	1. The overall process of risk identification, risk analysis and risk evaluation 2. the process of identifying, estimating, and prioritizing	1. ISO/IEC 27000:2018, 2. NIST SP 800-30		

		information security risks.	Rev.1, 2012		
Risk assessor	-	The individual, group, or organization responsible for conducting a risk assessment.	NIST SP 800-30 Rev.1, 2012		
Risk management	RM	1. A systematic performance of policies, procedures and practices management on communicating, consulting activities, establishing the context and controlling identifying, analysing, evaluating, treating, monitoring and reviewing risk. 2. Coordinated activities to direct and control an organization with regard to risk.	1. ISO/IEC 27000:2018 2. ISO 31000:2018		
Risk mitigation	-	Risk treatments that deal with negative consequences.	ISO/IEC 27000:2018		
Risk owner	-	Person or entity with the accountability and authority to manage a risk.	ISO/IEC 27000:2018		

Risk treatment	-	Process to modify risk.	ISO/IEC 27000:2018		
Security control	-	Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.	NIST SP 800-30 Rev.1, 2012 (FIPS 199, CNSSI No. 4009)		
Security impact analysis	-	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.	NIST SP 800-37 Rev.2, 2018		
Security Management	SM	Security management includes all the activities and practices implemented by organizations to manage security risks, threats, and impacts. These activities and practices should be coordinated in a systematic, and optimized manner.	ISO 28000:2007		
Security management objective	-	Specific outcome or achievement required of security in order to meet the security management policy. It is essential that such outcomes are linked either directly or indirectly to	ISO 28000:2007		

		providing the products, supply or services delivered by the total business to its customers or end users.			
Security management policy	-	Overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.	ISO 28000:2007		
Severity of vulnerability	-	The severity of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context-dependent.	NIST SP 800-30 Rev.1, 2012	CVSS 3.1	
Threat	-	Potential cause of an unwanted incident, which can result in harm to a system or organization.	ISO/IEC 27000:2018	Example are a signature spoofing by key theft on an e-mail operating system and buffer overflow in Local Command-Line Utilities on an admin operating system.	

Threat assessment	-	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	CNSS, 2015, NIST SP 800-30 Rev.1, 2012		
Threat level	-	The expected probability of occurrence of a threat to a cyber asset.	EU H2020-DS-2014-01 project "MITIGATE"		
Vulnerabilities Measurement/ Labelling	-	Vulnerabilities are defined in terms of an attribute and the method for quantifying it	ISO/IEC 27000:2018 , ISO/IEC/IEEE 15939:2017	- Common Vulnerabilities and Exposures - TOE-relevant CVE vulnerabilities - Common Weakness Enumeration - Common Vulnerability Scoring System - CVSS basic metric - CVSS temporal metric - CVSS environmental metric	

Vulnerability	-	1. Weakness in the TOE that can be used to violate the SFRs in some environment. 2. Weakness of an asset or control that can be exploited by one or more threats. 3. In the context of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service (functional) that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.	1. ISO/IEC 15408-1:2009 (CC) , 2. ISO/IEC 27000:2018 , 3. ISO/IEC 29147:2018	• Poor encryption in digital signatures. • Target Row Refresh (TRR), aka the TRRespass issue (CVE-2020-10255) • The DNS bugs (CVE-2020-11901)	A term 'vulnerability' is functioning in different context in ISO/IEC 15408 as it reflects the perspective of the TOE (*see line 94). - Multiple vulnerabilies can impact a supply chain as a whole, compromising multiple inteconnected assets by exploiting a series of assets' vulnerabilities. See more: "Hacking the Supply Chain" [https://i.blackhat.com/USA-20/Wednesday/us-20-Oberman-Hacking-The-Supply-Chain-The-Ripple20-Vulnerabilities-Haunt-Tens-Of-Millions-Of-Critical-Devices.pdf]

Vulnerability Analysis AVA_VAN	AVA_VAN	An assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs. It deals with the threats that an attacker will be able to discover flaws allowing unauthorised access to data and functionality, allowing the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users. Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE. Assessment of development vulnerabilities is covered by the assurance family AVA_VAN.	ISO/IEC 15408-3:2008 (CC)	Levelling is based on an increasing rigour of vulnerability analysis by the evaluator and increased levels of attack potential required by an attacker to identify and exploit the potential vulnerabilities. • AVA_VAN.1 Vulnerability survey (TOE Resistance against Basic Attack Potential); • AVA_VAN.2 (Unstructured) Vulnerability analysis (TOE Resistance against Basic AP); • AVA_VAN.3 Focused vulnerability analysis (TOE Resistance against Enhanced-Basic AP); • AVA_VAN.4 Methodical vulnerability analysis (TOE Resistance against Moderate AP); • AVA_VAN.5 Advanced methodical vulnerability analysis (TOE Resistance against High AP).	

Vulnerability Chain		Weaknesses existing in a group of assets that can be exploited by threats starting from an entry point in a successive manner which allows a progressive security impact or consequences to these assets that terminate(s) to a target point.	ANSI/API, 2013		
Vulnerability Severity Level	VSL	1. Qualitative severity rankings of “None” (0.0), "Low" (0.1-3.9), "Medium" (4.0-6.9), "High" (7.0-8.9), and “Critical” (9.0-10.0). 2. It measures the probability an attacker can successfully reach and exploit a specific vulnerability (either confirmed or unknown) taking into account temporal vulnerability characteristics and the impact according to the user’s environment to a specific asset.	1. CVSS v3.1, 2. EU H2020-ICT-02-2020 project "CYRENE" : CYRENE RCA Methodology		
Certification Concepts					

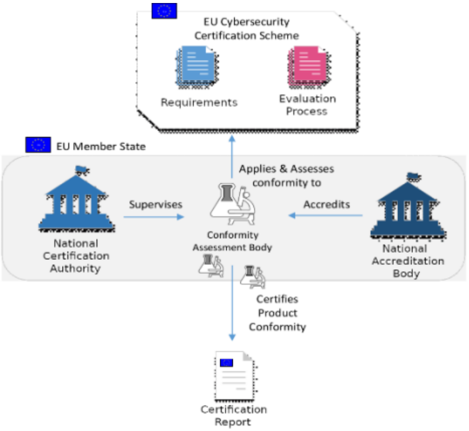
Accreditation	-	A third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities	Regulation (EC) No 765/2008 // ISO/IEC 17000:2020		
Accreditation Body		An authoritative body that performs accreditation	ISO/IEC 17000:2020		The authority of an accreditation body can be derived from government, public authorities, contracts, market acceptance or scheme owners
Assurance Level	-	A basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process	Regulation (EU) 2019/881 (EU Cybersecurity Act)		• Level 1: Little or no confidence; • Level 2: Some confidence; • Level 3: High confidence;

		concerned			
Attestation	-	An issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated	ISO/IEC 17000:2020		*Note 1*: The resulting statement, referred to in this document as a “statement of conformity”, is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, provide contractual or other legal guarantees. *Note 2:* First-party attestation and third-party attestation are distinguished by the terms declaration, certification and accreditation, but there is no corresponding term applicable to second-party attestation

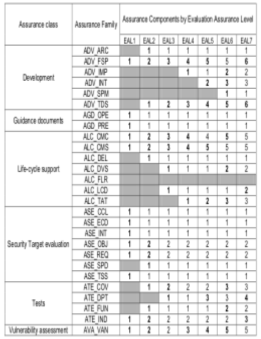
Attestation (scope of)	-	The range or characteristics of objects of conformity assessment covered by attestation	ISO/IEC 17000:2020		
Audit	-	A process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled	ISO/IEC 17000:2020		*Note 1*: The specified requirements are defined prior to performing an audit so that the relevant information can be obtained. *Note 2*: Examples of objects for an audit are management systems, processes, products and services. *Note 3*: For accreditation purposes, the audit process is called “assessment”.

Certification	-	A third-party attestation related to an object of conformity assessment, with the exception of accreditation. Also, a certification of a management system, such as the environmental management system, quality management system or information security management system of an organization, is one means of providing assurance that the organization has implemented a system for the management of the relevant aspects of its activities, products and services, in line with the organization’s policy and the requirements of the respective international management system standard. Also,	ISO/IEC 17000:2020 // ISO/IEC 17021-1:2015		
Certification scheme	-	Conformity assessment system related to management systems to which the same specified requirements, specific rules, and procedures apply.	ISO/IEC 17021-1:2015	EUCC, national schemes. (e.g. SOGIS-MRA, included NL (NLNCSA), FR (ANSSI), SE (FMV), DE (BSI).	

Common Criteria	CC	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.	ISO/IEC 15408-1:2009 (CC)		"Common Criteria" is the ISO/IEC 15408-1:2009.
Competence	-	The ability to apply knowledge and skills to achieve intended results	EN ISO 19011:2018		
Conformance claim		The conformance claim indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation.	Common Criteria for Information Security Conformity Evaluation (CC) (Part I: Introduction and general model (2017), v3.1 Rev. 5		
Conformity Assessment	CA	1. The process demonstrating whether specified requirements	1. Regulation (EC) No 765/2008		

		relating to a product, process, service, system, person or body have been fulfilled. 2. A procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled.	2. Regulation (EU) 2019/881 (EU Cybersecurity Act) 3. ISO/IEC 17000:2020	 EU Cybersecurity Certification Scheme Requirements Evaluation Process EU Member State Applies & Assesses conformity to Supervises Accredits National Certification Authority Conformity Assessment Body National Accreditation Body Certifies Product Conformity Certification Report	
Conformity Assessment Body	CAB	A body that performs conformity assessment activities including calibration, testing, certification and inspection	Regulation (EC) No 765/2008 // ISO/IEC 17000:2020	One that: • Applies and assesses conformity to EU Cybersecurity Certification Scheme. • Certifies product conformity by a certification report.	
Conformity Assessment System	-	The set of rules and procedures for the management of similar or related conformity assessment schemes	ISO/IEC 17000:2020		A conformity assessment system can be operated at an international, regional, national, sub-national, or industry sector level
Conformity assessment scheme / Conformity assessment programme	-	The set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment	ISO/IEC 17000:2020		*Note 1*: A conformity assessment scheme can be managed within a conformity assessment system. *Note 2*: A conformity

					assessment scheme can be operated at an international, regional, national sub-national, or industry sector level
Conformity Self-assessment	-	An action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.	Regulation (EU) 2019/881 (EU Cybersecurity Act)		
European Cybersecurity Certification Scheme	EUCC	A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.	Regulation (EU) 2019/881 (Cybersecurity Act)		It is an umbrella, which replaces SOG-IS. It covers the certification of ICT products, using the ISO/IEC 15408 (CC) and it is the foundation of a EU Cybersecurity certification framework. There are no examples of schemes according to ECCS yet - the EU is in the process of creating.

<table>
<tr>
<td><em>Evaluation Assurance Level</em></td>
<td>EAL</td>
<td>The definition of a scale for measuring assurance for component Targets of Evaluation (TOEs)</td>
<td>ISO/IEC 15408-3:2008
(CC)</td>
<td>
<table>
<tr><th>Assurance class</th><th>Assurance Family</th><th colspan="7">Assurance Components by Evaluation Assurance Level</th></tr>
<tr><th></th><th></th><th>EAL1</th><th>EAL2</th><th>EAL3</th><th>EAL4</th><th>EAL5</th><th>EAL6</th><th>EAL7</th></tr>
<tr><td>Development</td><td>ADV_ARC</td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ADV_FSP</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>5</td><td>6</td></tr>
<tr><td></td><td>ADV_IMP</td><td></td><td></td><td></td><td>1</td><td>1</td><td>2</td><td>2</td></tr>
<tr><td></td><td>ADV_INT</td><td></td><td></td><td></td><td></td><td>2</td><td>3</td><td>3</td></tr>
<tr><td></td><td>ADV_SPM</td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>1</td></tr>
<tr><td></td><td>ADV_TDS</td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>Guidance documents</td><td>AGD_OPE</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>AGD_PRE</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>Life-cycle support</td><td>ALC_CMC</td><td>1</td><td>2</td><td>3</td><td>4</td><td>4</td><td>5</td><td>5</td></tr>
<tr><td></td><td>ALC_CMS</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>5</td><td>5</td></tr>
<tr><td></td><td>ALC_DEL</td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ALC_DVS</td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td></tr>
<tr><td></td><td>ALC_FLR</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>ALC_LCD</td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td></tr>
<tr><td></td><td>ALC_TAT</td><td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>3</td></tr>
<tr><td>Security Target evaluation</td><td>ASE_CCL</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ASE_ECD</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ASE_INT</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ASE_OBJ</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td></td><td>ASE_REQ</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td></td><td>ASE_SPD</td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td></td><td>ASE_TSS</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>Tests</td><td>ATE_COV</td><td></td><td>1</td><td>2</td><td>2</td><td>2</td><td>3</td><td>3</td></tr>
<tr><td></td><td>ATE_DPT</td><td></td><td></td><td>1</td><td>1</td><td>3</td><td>3</td><td>4</td></tr>
<tr><td></td><td>ATE_FUN</td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td></tr>
<tr><td></td><td>ATE_IND</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>3</td></tr>
<tr><td>Vulnerability assessment</td><td>AVA_VAN</td><td>1</td><td>2</td><td>2</td><td>3</td><td>4</td><td>5</td><td>5</td></tr>
</table>
Table 1 — Evaluation assurance level summary
<em>Assurance Levels (ISO/IEC 15408-3:2008 (CC))</em></td>
<td></td>
</tr>
<tr>
<td><em>Inspection</em></td>
<td>-</td>
<td>The examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements</td>
<td>ISO/IEC 17000:2020</td>
<td></td>
<td><em>Note 1</em>: Examination can include direct or indirect observations, which can include measurements or the output of instruments.
<em>Note 2</em>: Conformity assessment schemes (4.9) or contracts can specify inspection as examination only</td>
</tr>
<tr>
<td><em>Protection Profile</em></td>
<td>PP</td>
<td>Implementation-independent statement of security needs for a TOE type.</td>
<td>ISO/IEC 15408-1:2009
(CC)</td>
<td></td>
<td>As a Protection Profile is not written for a specific product, in many cases only a general</td>
</tr>
</table>

					idea can be given of the available hardware/software/firmware. In some other cases, e.g. a requirements specification for a specific consumer where the platform is already known, (much) more specific information may be provided. All vendors must agree for the PP doc, which describes the security functions of the TOE, threats,etc.[https://www.commoncriteriaportal.org/pps/]
Security Assurance Requirements	SAR	A description of how assurance is to be gained that the TOE meets the SFRs	ISO/IEC 15408-1:2009 (CC)		
Security function	SF	Function that implement the security requirements.	ISO/IEC 15408 - 2:2008 (CC)		
Security Functional Requirements	SFR	A translation of the security objectives for the TOE into a standardised language	ISO/IEC 15408-1:2009 (CC)		

Security objective		1. Statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions. 2. Information security objective: Objectives that are set by the organization, consistent with the information security policy, to achieve specific results.	1. ISO/IEC 15408-1:2009 (CC) , 2. ISO/IEC 27000:2018		cf. EU Cybersecurity Act 2019/881 (Article 51) on Security objectives of European cybersecurity certification schemes
Security Requirements	ASE_REQ	The security requirements consist of two groups of requirements: a) the security functional requirements (SFRs) b) the security assurance requirements (SARs)	ISO/IEC 15408-1:2009 (CC)		
Target of Evaluation	TOE	A set of software, firmware, hardware and/or process possibly accompanied by guidance	ISO/IEC 15408-1:2009 (CC)	• A software application • An operating system; • A software application and an operating system; • A software application in combination with an operating system and a workstation; • An operating system in combination with a workstation; • A smart card integrated circuit; • The cryptographic co-processor of a smart card integrated circuit; • A Local Area Network including all terminals, servers, network equipment and software; • A database application excluding the remote client software normally associated with that database application; • A supply chain.	- TOE shall be the ICT product as a whole or the elements of the ICT product. - While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a

					combination of these. As far as ISO/IEC 15408 is concerned, the precise relation between the TOE and any IT products is only important in one aspect: the evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product.
Testing	-	The determination of one or more characteristics of an object of conformity assessment, according to a procedure	ISO/IEC 17000:2020		*Note 1*: The procedure can be intended to control variables within testing as a contribution to the accuracy or reliability of the results. *Note 2*: The results of testing can be expressed in terms of specified units or objective comparison

					with agreed references. *Note 3*: The output of testing can include comments (e.g. opinions and interpretations) about the test results and fulfilment of specified requirements
Validation	-	The confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements have been fulfilled	ISO/IEC 17000:2020		*Note 1*: Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use
Verification	-	The confirmation of truthfulness through the provision of objective evidence that specified requirements have been fulfilled	ISO/IEC 17000:2020		*Note 1*: Verification can be applied to claims to confirm the information declared with the claim regarding events that have already occurred or results that have already been obtained