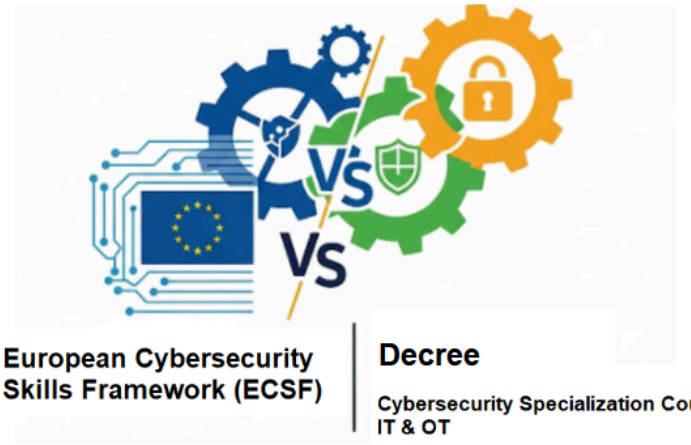

European Competencies and Contents of the IT/OT Cybersecurity Specialization Courses

2025-2026

index

1. Objective and Scope of the Comparison Document

Enisa is the European Cybersecurity Agency, and it has defined the roles and profiles of cybersecurity technicians needed to cover the cybersecurity field in companies and organizations. The main objective of this framework is to create a common understanding between individuals, employers, and training program providers in EU Member States.

12 profiles have been defined along with their titles, missions, tasks, skills, knowledge and competencies that we could group into different groups, some management profiles (CISO) and regulations, risk manager profiles, incidents and threats, technical profiles of architecture design, technical auditing, forensics or pentesting and trainer and researcher profiles

The **Tknika cybersecurity group analyzed these profiles and compared them with the existing decrees** that regulate cybersecurity specialization courses in the IT and OT fields, comparing the profiles' mission, tasks, skills, and knowledge with the competencies, learning outcomes, and content of the different modules.

2. Presentation of ENISA and the European Cybersecurity Competence Framework (ECSF)

2.1. ENISA

ENISA (European Union Agency for Cybersecurity) is the European Union's cybersecurity agency. It was established in 2004 and is based in Athens and Heraklion, Greece. It is the official body responsible for **improving cybersecurity in the European Union** . Its main mission is to help Member States, European institutions, and the private sector **strengthen their capabilities** against cyber threats by promoting a common culture of digital security.

Main tasks of ENISA:

1. Strategic and technical advice
    - Advises the European Commission and national governments on cybersecurity policies.
    - She collaborates in the development and implementation of key legislation, such as the NIS2 Regulation and the Cyber Resilience Act.
2. Risk and policy management
    - Develops guides, standards, and best practices to manage technological and security risks.
    - Publishes competency frameworks, such as the ECSF (European Cybersecurity Skills Framework).
3. Training and awareness
    - Supports the training of professionals and promotes campaigns to increase public awareness of cybersecurity.
    - Organizes events such as the European Cybersecurity Month.
4. Support for CSIRTs
    - Collaborates with the Computer Security Incident Response Teams (CSIRT) of member countries.
    - Improves coordination in the event of cross-border cyberattacks.
5. Threat research and analysis
    - Publishes regular reports on trends in cyber threats, vulnerabilities, and emerging attacks.
    - Facilitates the sharing of cyber intelligence information between governments and businesses.
6. Cybersecurity Certification

- It oversees and coordinates the European Cybersecurity Certification Framework, which promotes common standards for ICT products, services, and processes.

2.2. European Cybersecurity Competence Framework (ECSF)

The European Cybersecurity Skills Framework (ECSF) is an initiative developed by ENISA (the European Union Agency for Cybersecurity) to establish a common language on the roles, skills and knowledge needed in the field of cybersecurity within Europe.

The ECSF is a structured model that defines and classifies cybersecurity professional roles, describing for each:

- Its main functions and tasks,
- The technical and non-technical skills required,
- The associated fundamental knowledge.

It is designed to align educational offerings, labor market needs, and public cybersecurity training policies.

Objectives of the ECSF:

A. Establish a common language between companies, educational institutions and public administrations.
B. Identify and classify professional roles in cybersecurity.
C. Facilitate the design of training programs and certifications based on the real needs of the sector.
D. Support career planning for professionals and recruitment for employers.
E. Bridging the cybersecurity talent gap in Europe.

Who is it for?

- Companies and employers: to define job descriptions and recruitment needs.
- Trainers and universities: to align educational programs with the labor market.
- Professionals: to guide the development of their skills and career.
- Politicians and regulators: to create coherent policies on digital skills.

Contents of the ECSF

The ECSF identifies 12 key professional roles in cybersecurity. Each comes with a detailed description of the duties, required skills, knowledge, and associated tools.

1. **Information Security Officer (** CISO **)**

   Leads the cybersecurity strategy and aligns policies and resources with business objectives.

2. **Cyber Incident Response**
   Detect, analyze, contain, and recover from incidents to minimize operational and reputational impact.
3. **Cyber Legal, Policy & Compliance Officer**
   Ensures compliance with security-related laws, regulations, and internal policies.
4. **Cyber Threat Intelligence** Specialist

   Collects and correlates information on actors, tactics, and campaigns to anticipate attacks.

5. **Cybersecurity Architect**
   Designs secure architectures, controls, and solutions that support business requirements.
6. **Cybersecurity Auditor**
   Evaluates the effectiveness of controls and makes recommendations to improve security posture.
7. **Cybersecurity Educator**
   Develops and delivers cybersecurity training, awareness, and capacity building programs.
8. **Cybersecurity Implementer**
   Integrates, configures, and maintains technical solutions (firewalls, IAM, EDR, etc.) in accordance with organizational policy.
9. **Cybersecurity Researcher**
   Conducts basic and applied research, generates innovation, and publishes results that expand the state of the art.
10. **Cybersecurity Risk Manager**
    Identifies, analyzes and treats cybersecurity risks to keep them within acceptable limits.
11. **Digital Forensics Investigator**
    Collects and analyzes digital evidence, documents findings, and presents them to stakeholders.
12. **Penetration Tester** Performs controlled penetration tests to discover vulnerabilities and recommend remediation measures.

Summary

The ECSF (European Cybersecurity Competence Framework) is a strategic EU tool to harmonize, professionalize, and strengthen the European cybersecurity ecosystem, helping to train, recruit, and develop the experts the continent needs to confront growing digital threats.

3. Presentation of the Specialization Course in Cybersecurity in Information Technology Environments

Royal Decree 479/2020, of April 7, establishing the Specialization Course in Cybersecurity in Information Technology Environments and setting out the basic aspects of the curriculum.

DECREE BOPV 83/2023, of June 6, establishing the curricula corresponding to the specialization course in Cybersecurity in Information Technology environments,

ID

Name : Cybersecurity in Information Technology Environments.

Level : Higher Vocational Training.

Duration : 900 hours

Professional Family : Information Technology and Communications (solely for the purposes of classifying Vocational Training courses).

Branch of knowledge : Engineering and Architecture.

ECTS credits : 43.

General competence:

The general competency of this specialization course consists of defining and implementing security strategies in information systems by conducting cybersecurity diagnostics, identifying vulnerabilities, and implementing the necessary measures to mitigate them by applying current regulations and industry standards, following quality, occupational risk prevention, and environmental protection protocols.

Professional modules.

Code	Professional Module	Time allocation

5021	Cybersecurity incidents	105
5022	Network and system bastioning	240
5023	Safe production launch	150
5024	Computer forensics	120
5025	Ethical hacking	150
5026	Cybersecurity regulations	60
E300	Basic fundamentals	75
	Total	900

4. Presentation of the Specialization Course in Cybersecurity in Operational Technology Environments

Royal Decree 478/2020, of April 7, establishing the Specialization Course in Cybersecurity in Operation Technology Environments

BOVP DECREE 83/2023, of June 6, establishing the curricula for the specialization course in Cybersecurity in Operational Technology Environments

ID

Title : Cybersecurity in Operational Technology Environments. **Level** : Advanced Vocational Training.
Duration : 900 hours.
Professional Family : Electricity and Electronics (solely for the purposes of classifying Vocational Training courses).
Branch of knowledge : Engineering and Architecture.
ECTS credits : 43.

General competence

The general competency of this specialization course consists of defining and implementing security strategies in organizations and industrial infrastructures by conducting cybersecurity diagnostics, identifying vulnerabilities, and implementing the necessary measures to mitigate them by applying current regulations and industry standards, following quality, occupational risk prevention, and environmental protection protocols.

Professional modules

Code	Professional Module	Time allocation
5027	Cybersecurity in industrial projects	150
5028	Secure industrial control systems	180
5029	Secure industrial communications networks	210
5030	Forensic analysis in industrial cybersecurity	240
5031	Comprehensive security	120
	Total	900

5. ANALYZE THE RELATIONSHIP BETWEEN PROFILES OF THE EUROPEAN FRAMEWORK AND THE PROFESSIONAL COMPETENCIES OF THE IT/OT DECREES

A comparative analysis has been carried out between the European Cybersecurity Competence Framework (ECSF) of ENISA and the curriculum content (Decree) of the Specialization Course in Cybersecurity in Information Technology Environments.

In each profile, the main tasks (Main task) have been related to the learning outcomes (RA) of each module, the key skills (Key Skills) with the personal and social professional competencies, and the key knowledge (Key knowledge) with the contents of each module.

- Main Task > Module (RA)
- Key skills > Personal and social professional skills
- Key knowledge > Modules (Contents)

5.1. ECSF Analysis & IT Decree

5.1.1. General perspectives

Following the study carried out—and before going into detail in subsequent sections—we will outline, as a general overview, to what extent we conclude that the ECSF profiles are addressed in our Decree.

ECSF	Main task(s)	Key skill(s)	Key knowledge	Total %
Decree	55%	54%	63%	58%

As we will see, the profiles with the highest scores are associated with more technical knowledge, while those with lower scores are more closely related to management or teaching roles, which is entirely understandable given the nature of the specialization courses.

5.1.2. More detailed information

The total score per profile (sum of tasks, skills, and knowledge) allows us to estimate alignment. Higher values indicate a greater alignment of the Decree with the European framework. Below is a table sorted by the percentage of total alignment by profile:

Profile	Main task(s)	Key skill(s)	Key knowledge	Total %
Penetration Analyst	81%	77%	88%	82%
Cybersecurity Risk Manager	75%	92%	65%	77%
Digital Forensic Investigator	88%	70%	73%	77%
Cybersecurity Implementer	70%	64%	75%	70%
Legal, Policy, and Cyber Compliance Officer	56%	53%	70%	60%
Cybersecurity Researcher	58%	64%	50%	58%
Cyber Incident Response Manager	61%	46%	63%	57%
Cybersecurity Auditor	38%	50%	72%	53%
Cybersecurity Architect	46%	40%	62%	49%
Director of Information Security	32%	41%	52%	42%
Cyber Threat Intelligence Specialist	46%	33%	42%	40%
Cybersecurity Educator	13%	19%	47%	26%

5.1.3. Classification according to alignment

Stronger Alignment: Technical and Practical Functions

The highest match rates are found in profiles focused on those that require greater technical knowledge that can be put into practice in the classroom.

Profile	Main task(s)	Key skill(s)	Key knowledge	Total %
Penetration Analyst	81%	77%	88%	82%
Cybersecurity Risk Manager	75%	92%	65%	77%
Digital Forensic Investigator	88%	70%	73%	77%
Cybersecurity Implementer	70%	64%	75%	70%

Moderate alignment: strategic and governance-oriented profiles

Several profiles show moderate levels of alignment; these profiles have been able to be addressed in detail in the classroom, but are more difficult to address in simulated environments like those used in the classroom.

Profile	Main task(s)	Key skill(s)	Key knowledge	Total %
Legal, Policy, and Cyber Compliance Officer	56%	53%	70%	60%
Cybersecurity Researcher	58%	64%	50%	58%
Cyber Incident Response Manager	61%	46%	63%	57%
Cybersecurity Auditor	38%	50%	72%	53%
Cybersecurity Architect	46%	40%	62%	49%

Bottom lineup: specialized or management profiles

As expected, the more specific profiles, those with a greater management component or those related to strategic outreach, have a lower level of alignment.

Profile	Main task(s)	Key skill(s)	Key knowledge	Total %

Director of Information Security	32%	41%	52%	42%
Cyber Threat Intelligence Specialist	46%	33%	42%	40%
Cybersecurity Educator	13%	19%	47%	26%

5.1.4. Conclusions

The data show that the Decree covers more than 50% of the details of the profiles defined by the ECSF in general. In detail, four profiles are strongly aligned (70% or more), five are moderately aligned (45% or more), and three are weakly aligned (less than 45%). Furthermore, of the 12 profiles, eight are aligned above 50%, and three are aligned above 75%.

We believe that, for a full-length specialization course, the data demonstrates that the curriculum is highly tailored and aligned with key technical functions in European cybersecurity.

5.2. ECSF Analysis & OT Decree

5.2.1. General perspectives

Following the study carried out—and before going into detail in subsequent sections—we will outline, as a general overview, to what extent we conclude that the ECSF profiles are addressed in our Decree.

ECSF	Main task(s)	Key skill(s)	Key knowledge	Total %
Decree	54%	56%	59%	56%

The data show varying levels of alignment between professional profiles and the needs of the OT environment. Functions with higher combined scores indicate stronger alignment with technical operations, while others stand out for their strategic components or thematic specialization.

5.2.2. Detailed information

The total score by role (sum of tasks, skills, and knowledge) allows us to estimate alignment. Higher values indicate greater fit with the OT field, both

technically and functionally. The total by role is shown below, sorted in descending order:

OT	Main task(s)	Key skill(s)	Key knowledge	Total %
Cybersecurity Risk Manager	94%	88%	75%	86%
Cybersecurity Implementer	83%	75%	68%	75%
Penetration Evaluator	78%	70%	77%	75%
Digital Forensic Investigator	58%	70%	52%	60%
Cybersecurity Architect	67%	48%	62%	59%
Cyber Incident Manager	59%	50%	65%	58%
Cybersecurity Researcher	52%	71%	45%	56%
Cyber Threat Intelligence Specialist	46%	48%	48%	47%
Director of Information Security	37%	47%	57%	47%
Legal, Policy, and Cyber Compliance Consulting	35%	34%	70%	46%
Cybersecurity Auditor	27%	38%	53%	39%
Cybersecurity Educator	6%	28%	41%	25%

5.2.3. Classification according to alignment

Stronger Alignment: Technical and Practical Functions

Roles with the highest total score, focused on implementation and operation in OT:

The highest match rates are found in profiles focused on those that require greater technical knowledge that can be put into practice in the classroom.

Cybersecurity Risk Manager	94%	88%	75%	86%
Cybersecurity Implementer	83%	75%	68%	75%
Penetration Evaluator	78%	70%	77%	75%

Moderate alignment: Strategic and governance-oriented

Roles with a mixed approach between technique and political management:

Several profiles show moderate levels of alignment; these profiles have been able to be addressed in detail in the classroom, but are more difficult to address in simulated environments like those used in the classroom.

Digital Forensic Investigator	58%	70%	52%	60%
Cybersecurity Architect	67%	48%	62%	59%
Cyber Incident Manager	59%	50%	65%	58%
Cybersecurity Researcher	52%	71%	45%	56%
Cyber Threat Intelligence Specialist	46%	48%	48%	47%
Director of Information Security	37%	47%	57%	47%
Legal, Policy, and Cyber Compliance Consulting	35%	34%	70%	46%

Bottom lineup: Specialized or niche roles

Oriented to particular contexts, educational or auditory, with less OT weight in general:

As expected, the more specific profiles, those with a greater management component or those related to strategic outreach, have a lower level of alignment.

Cybersecurity Auditor	27%	38%	53%	39%
Cybersecurity Educator	6%	28%	41%	25%

5.2.4. Conclusions

The data show that the Decree covers more than 50% of the details of the profiles defined by the ECSF in general. In detail, three profiles are strongly aligned (70% or more), seven are moderately aligned (45% or more), and two are weakly aligned (less than 45%). Furthermore, of the 12 profiles, seven exceed 50% alignment, and three exceed 75%.

Most of the roles analyzed show good alignment with OT requirements, especially those focused on technical implementation, security architecture, and incident response. Mixed profiles between technical and political management would fall somewhere in between, while profiles focused on education, policy, or forensic analysis have a more limited contribution, although relevant in specific contexts.

This difference in IT values is logical given the different nature of the facilities. In the OT area, architecture, incident management, and risk management take priority, given that it's a production facility. Management and auditing are secondary.

We believe that, for a full-length specialization course, the data demonstrates that the curriculum is highly tailored and aligned with key technical functions in European cybersecurity.

6. TABLES OF RELATIONSHIP BETWEEN PROFILES AND DECREE

CHIEF INFORMATION SECURITY OFFICER (CISO)

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	32%	37%
Key Skill(s)	41%	47%
Key Knowledge	52%	57%
	42%	47%

CYBER INCIDENT RESPONDER

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	61%	59%
Key Skill(s)	46%	50%
Key Knowledge	63%	65%
	57%	58%

CYBER LEGAL, POLICY & COMPLIANCE OFFICER

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	56%	35%
Key Skill(s)	53%	34%
Key Knowledge	70%	70%
	60%	46%

CYBER THREAT INTELLIGENCE SPECIALIST

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	46%	46%
Key Skill(s)	33%	48%
Key Knowledge	42%	48%
	40%	47%

CYBERSECURITY ARCHITECT

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	46%	67%
Key Skill(s)	40%	48%
Key Knowledge	62%	62%
	49%	59%

CYBERSECURITY AUDITOR

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	38%	27%
Key Skill(s)	50%	38%
Key Knowledge	72%	53%
	53%	39%

CYBERSECURITY EDUCATOR

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	13%	6%
Key Skill(s)	19%	28%
Key Knowledge	47%	41%
	26%	25%

CYBERSECURITY IMPLEMENTER

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	70%	83%
Key Skill(s)	64%	75%
Key Knowledge	75%	68%
	70%	75%

CYBERSECURITY RESEARCHER

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	58%	52%
Key Skill(s)	64%	71%
Key Knowledge	50%	45%
	58%	56%

CYBERSECURITY RISK MANAGER

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	75%	94%
Key Skill(s)	92%	88%
Key Knowledge	65%	75%
	77%	85%

DIGITAL FORENSICS INVESTIGATOR

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	88%	58%
Key Skill(s)	70%	70%
Key Knowledge	73%	52%
	77%	60%

PENETRATION TESTER Penetration tester

CONCEPT	MATCH RATE IN IT Decree	MATCH RATE IN Decree OT
Main Task(s)	81%	78%
Key Skill(s)	77%	70%
Key Knowledge	88%	77%
	82%	75%

Summary table %

	ITEM					OT			
	Main task(s)	Key skill(s)	Key knowledge	Total %		Main task(s)	Key skill(s)	Key knowledge	Total %
Chief Information Security Officer (CISO)	32%	41%	52%	42%		37%	47%	57%	47%
Cyber Incident Response	61%	46%	63%	57%		59%	50%	65%	58%
Head of Cyber Policy, Compliance and Legal Affairs	56%	53%	70%	60%		35%	34%	70%	46%
Cyber Threat Intelligence Specialist	46%	33%	42%	40%		46%	48%	48%	47%
Cybersecurity Architect	46%	40%	62%	49%		67%	48%	62%	59%
Cybersecurity auditor	38%	50%	72%	53%		27%	38%	53%	39%
Cybersecurity Educator	13%	19%	47%	26%		6%	28%	41%	25%
Cybersecurity Implementer	70%	64%	75%	70%		83%	75%	68%	75%
Cybersecurity researcher	58%	64%	50%	58%		52%	71%	45%	56%
Cybersecurity Risk Manager	75%	92%	65%	77%		94%	88%	75%	85%
Digital Forensic Investigator	88%	70%	73%	77%		58%	70%	52%	60%
Penetration tester	81%	77%	88%	82%		78%	70%	77%	75%

Profiles (ECSF) % IT

ITEM	Main task(s)	Key skill(s)	Key knowledge	Total %
Penetration Analyst	81%	77%	88%	82%
Cybersecurity Risk Manager	75%	92%	65%	77%
Digital Forensic Investigator	88%	70%	73%	77%
Cybersecurity Implementer	70%	64%	75%	70%
Legal, Policy, and Cyber Compliance Officer	56%	53%	70%	60%
Cybersecurity Researcher	58%	64%	50%	58%
Cyber Incident Response Manager	61%	46%	63%	57%
Cybersecurity Auditor	38%	50%	72%	53%
Cybersecurity Architect	46%	40%	62%	49%
Director of Information Security	32%	41%	52%	42%
Cyber Threat Intelligence Specialist	46%	33%	42%	40%
Cybersecurity Educator	13%	19%	47%	26%

Profiles (ECSF) % OT

OT	Main task(s)	Key skill(s)	Key knowledge	Total %
Cybersecurity Risk Manager	94%	88%	75%	86%
Cybersecurity Implementer	83%	75%	68%	75%
Penetration Evaluator	78%	70%	77%	75%
Digital Forensic Investigator	58%	70%	52%	60%
Cybersecurity Architect	67%	48%	62%	59%
Cyber Incident Manager	59%	50%	65%	58%
Cybersecurity Researcher	52%	71%	45%	56%
Cyber Threat Intelligence Specialist	46%	48%	48%	47%
Director of Information Security	37%	47%	57%	47%
Legal, Policy, and Cyber Compliance Consulting	35%	34%	70%	46%
Cybersecurity Auditor	27%	38%	53%	39%
Cybersecurity Educator	6%	28%	41%	25%

7. Literature

Enisa **:** https://www.enisa.europa.eu/

The European Cybersecurity Competence Framework (ECSF)

https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Basque Institute of Vocational Training Knowledge IVAC EEI

https://ivac-eei.eus/es/

COURSE IN CYBERSECURITY IN INFORMATION TECHNOLOGY ENVIRONMENTS

https://ivac-eei.eus/es/familias-profesionales/informatica-y-comunicaciones-ifc/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-la-informacion.html

COURSE IN CYBERSECURITY IN OPERATIONAL TECHNOLOGY ENVIRONMENTS

https://ivac-eei.eus/es/familias-profesionales/electricidad-y-electronica-ele/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-operacion.html

➢ ANNEX I: Complete list of profiles & Decree

The level of compliance (RATE) has been quantified in the decree of each "Detail" of the ECSF taking into account the following scale: 0% - 25% - 50% - 75% - 100 %

1-Chief Information Security Officer

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task	Define, implement, communicate, and maintain cybersecurity objectives, requirements, strategies, and policies aligned with business strategy to support organizational objectives.	M1:RA1(Ea);M2:RA 3(Ef)	50%	M1:RA1(Ea,Eb, Ed),RA2(Ec.Ed); M2:RA5(Ed)	50%
	Prepare and present the cybersecurity vision, strategies, and policies for approval by the organization's senior management and ensure their execution.		0%	M4:RA1(Ef,Eg)	25%
	Monitor the implementation and improvement of the Information Security Management System (ISMS)		0%	M1:RA4(Ea,Ec, Ef);M5:RA5(Ea, Eb,Ec,Ee)	25%
	Educate senior management on cybersecurity risks and threats and their impact on the organization.	M1:RA1(Eb,Ec);M2: RA3(Ea),RA10(Ea)	75%	M5:RA2(Ea,Ed, Eg)	25%
	Ensure senior management approves the organization's cybersecurity risks.	M2:RA3(Ec);M6:RA 2(Ec)	50%	M5:RA5(Ed,eE)	25%
	Develop cybersecurity plans		0%	M1:RA1(Ee),RA 3(EC)	75%
	Develop relationships with authorities and communities related to cybersecurity	M1:RA3(Ee); M6:RA1(Ee)	50%	M5:RA2(Ef,Eg); RA3(Ec,Ed)	50%
	Report cybersecurity incidents, risks, and findings to senior management.	M1:RA2(Ec,Ed,Ee),R A5(Eb)	50%	M4:RA1(Ef),RA 4(Ef)	50%
	Monitor progress in cybersecurity	M1:RA2(Eb,Ed);M2: RA7(Eh); M3:RA7(Ed);M5:RA 1(Ei)	100%	M3:RA9(Ea,Ed, EE)	100%

	Secure resources to implement the cybersecurity strategy	M2:RA3(e)	25%	M1:RA2(Ea,Eb)	25%
	Negotiate the cybersecurity budget with senior management		0%	M1:RA2(Ed,Ef)	0%
	Ensure organizational resilience to cyber incidents	M1:RA4(Ea,Eb,Ed)	50%	M4:RA6(Mib,Ec,Eg)	50%
	Manage the continuous development of capabilities within the organization		0%	M5:RA1(Ea,Ee), RA2(Ee,Ef)	25%
	Review, plan, and allocate adequate cybersecurity resources		0%	M1:RA2(Eb,Ed)	0%
	Level of compliance		32%		38%
Key skill(s)	Evaluate and improve an organization's cybersecurity posture	AC	25%	Ca,Cb	35%
	Analyze and implement cybersecurity policies, certifications, standards, methodologies, and frameworks.	Ce, Ck	75%	Cb,Cg	75%
	Analyze and comply with laws, regulations, and legislation related to cybersecurity.	Ca,Cl,Cm	100%	Ck	100%
	Implement cybersecurity recommendations and best practices	Cb,Cc	100%	Cj,Ch	100%
	Manage cybersecurity resources		0%	Cl,Cm	25%
	Develop, defend, and lead the execution of a cybersecurity strategy	Cb,Cc	25%	Cm,Cn	25%
	Influencing an organization's cybersecurity culture	Ca,Cl	25%	Cn	25%
	Design, implement, monitor, and review the Information Security Management System (ISMS), either directly or by leading its outsourcing.		0%	Ch,Cc	25%
	Review and improve security documents, reports, SLAs, and ensure security objectives are met.		0%	Cc, Ck	25%
	Identify and resolve cybersecurity-related issues	Cf,Ci	100%	Ci,Cm	75%
	Establish a cybersecurity plan	Ca,Cc	50%	Cd,Ca	50%
	Communicate, coordinate and cooperate with internal and external stakeholders	Cñ	50%	Cg,Cn	50%
	Anticipate necessary changes in the organization's information security strategy and formulate new plans	DC	50%	Ce,Cf	50%
	Define and apply maturity models for cybersecurity management		0%	Cf	25%
	Anticipate future cybersecurity		0%	This	50%

	threats, needs, and challenges				
	Motivate and encourage people	Cñ	50%	Cm	25%
	Level of compliance		41%		48%
Key knowledge	Cybersecurity policies	M2:RA3(C4),RA6(C9),RA9(C8);M7:RA2(C3)	100%	M2:RA5(C1,C2,C3);M5:RA1(C1,C2,C3),RA2(C1,C2,C3,RA3(C1,C2,C3)	100%
	Cybersecurity standards, methodologies and frameworks	M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5)	100%	M3:RA2(C10);M5:RA5(C1,C2,C3)	100%
	Cybersecurity recommendations and best practices	M2:RA3(C5,C7);M6:RA5(C3);	50%	M3:RA7(C1,C5,C6);M5:RA5(C1,C3)	100%
	Laws, regulations and legislation related to cybersecurity	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	100%	M5:RA5(C2,C3)	50%
	Cybersecurity-related certifications		0%	M1:RA2(C1,C2,C4);M5:RA5(C3)	0%
	Requirements of an ethical cybersecurity organization	M6:RA1(C1)	25%	M2:RA1(C1,C3);M5:RA5(C1,C3)	25%
	Cybersecurity maturity models		0%	M1:RA1(C1,C5)	25%
	Cybersecurity procedures	M1:RA4(C1),RA5(C1);M2:RA3(C7),RA7(C17)	100%	M1:RA5(C2,C3);M4:RA6(C1,C5)	100%
	Resource management		0%	M1:RA2(C1,C3);M5:RA1(C3)	25%
	Management practices		0%	M1:RA2(C2,C3);M5:RA5(C1,C2,C3)	25%
	Risk management standards, methodologies and frameworks	M2:RA3(C1);M3:RA5(C2);M6:RA2(C3)	100%	M5:RA5(C1,C2,C3)	75%
	Level of compliance		52%		57%

2- Cyber Incident Responder Cyber incident response

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Contribute to the development, maintenance and evaluation of the Incident Response Plan	M1:RA5(Ea)	25%	M4:RA6(Ea,Eb),M5:RA5(Ea,Eb,Ec,Ee)	25%
	Develop, implement, and evaluate procedures related to incident management	M1:RA4(Ea,Eb),RA5(Ea)	50%	M4:RA6(Ea,Eb,Ec,Ee)	50%
	Identify, analyze, mitigate, and	M1:RA2(Mib),RA3(Ea,Ed),R	100%	M4:RA1(Ec,Ed)	100%

	communicate cybersecurity incidents	A5(Mib,Ec,Ed,Ee)		,RA6(Ea,Ef,Eg)	
	Evaluate and manage technical vulnerabilities	M2:RA3(Ea),RA4(Eb,Ec,Ed,Ee),RA9(Eg,Eh);M3:RA6(Ec); M5:RA1(Ef,Eh),RA2(Eb,Ed,Ee,Eg),RA3(Eb,Ee,Ef),RA5(Ed,Ee,Ef,Eg)	100%	M3:RA8(Ea,Ed,Ee)	100%
	Measuring the effectiveness of cybersecurity incident detection and response	M1:RA2(Mib,Ed),RA3(Mib,Ef),RA4(Ea,Mib,Ed),	100%	M3:RA9(EA;Ed,Ee)	75%
	Evaluate the resilience of cybersecurity controls and mitigation actions taken after a cybersecurity incident or data breach.	M1:RA4(Ea,Eb)	25%	M4:RA6(Mib,Ec,Eg)	25%
	Adopt and develop incident handling testing techniques	M1:RA2(Eb,Ec,Ed),RA3(Ed), R4(Ea,Ec)	100%	M4:RA6(Ee,Ef)	75%
	Establish procedures for analyzing incident results and preparing incident handling reports.	M1:RA2(Ee),RA5(E*)	75%	M4:RA4(Ea,Ec,Ed)	75%
	Document the analysis of incident results and incident management actions	M1:RA5(Ea)	25%	M4;RA5(Ef)	75%
	Cooperate with Secure Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs)	M1:RA5(Ed)	25%	M5:RA5(Ef,Eg)	25%
	Cooperate with key personnel to report security incidents in accordance with the applicable legal framework.	M1:RA3(Eb,Med)	50%	M4:RA6(Ef.Eg)	25%
	Level of compliance		61%		59%
Key skill(s)	Practice all technical, functional, and operational aspects of the cybersecurity incident. Handling and response	Cf	75%	Cc, Cd, Cm, Cj, Cn	75%
	Collect, analyze, and correlate cyber threat information from multiple sources	Cb	75%	Ca, Ch, Ci, Cg	75%
	Work on operating systems, servers, clouds, and relevant infrastructures.		0%	Cb, Cf, Ch	0%
	Working under pressure	Cñ	75%	Cb, Cf, Ch	75%
	Communicate, present and	Cñ	50%	Cl,Cm	50%

	inform relevant stakeholders				
	Manage and analyze log files		0%	Cc, Ck, Cn	25%
	Level of compliance		46%		50%
Key know ledge	Incident management standards, methodologies and frameworks		0%	M4:RA1(C2,C3, C4);M5:RA5(C 1,C3)	50%
	Recommendations and best practices for incident management	M1:RA4(C6)	75%	M3:RA10(C1,C 2,C3);M4:RA6(C1,C2,C4,C6)	75%
	Incident management tools	M1:RA2(C2,C3,C4)	50%	M3:RA9(C1,C2);M4:RA2(C7,C 9)	50%
	Communication procedures for incident management	M1:RA3(C5),RA4(C3),RA5(C *)	100%	M4:RA6(C4,C5, C6);M5:RA5(C 3,C5)	75%
	Operating system security	M7:RA3(C1,C2)	75%	M2:RA6(C1,C4);M3:RA11(C2, C3)	75%
	Computer network security	M2:RA1(C*),RA3(C*),RA6(C *);M7:RA1(C1,C2,C3)	100%	M3:RA5(C1,C2, C4),RA6(C1,C3)	100%
	cyber threats	M1:RA3(C4);M2:RA3(C1);M 3:RA5(C2)	100%	M3:RA8(C5,C6);M4:RA2(C2,C 6,C7)	100%
	Cybersecurity attack procedures	M5: RA2(C4,C5), RA3(C6,C7,C8), RA5(C6), RA6(C4)	100%	M3:RA8(C3,C4);M4:RA6(C2,C 6)	100%
	Vulnerabilities of computer systems	M2:RA10(C10);M3:RA6(C2, C6);M5:RA3(C6,C9),RA5(C5, C6,C7)	100%	M4:RA2(C7,C9)	100%
	Cybersecurity-related certifications		0%	M1:RA2(C2,C3);M5:RA5:C1,C 3)	0%
	Laws, regulations and legislation related to cybersecurity	M6:RA3(C1,C2,C3),RA4(C*), RA5(C8)	100%	M5:RA5(C2,C3)	100%
	Operation of Secure Operations Centers (SOC)	M2:RA7(C19)	25%	M3:RA9(C1,C2);M4:RA6(C1,C 5,C6)	25%
	Operation of Computer Security Incident Response Teams (CSIRT)		0%	M4:RA6(C3,C4, C5)	0%
	Level of compliance		63%		65%

3- Cyber Legal, Policy & Compliance Officer Responsible for Legal Affairs, Policies and Cyber Compliance

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Ensure compliance and provide legal advice and guidance on privacy and data protection rules, laws, and regulations.	M2:RA4(E*);M3:RA6(Ef);M4:RA4(Ee);M6:RA4(E*)	100%	M5:RA5(Ea,Eb,Ec,Ee)	50%
	Identify and document compliance gaps	M1:RA1(Ee);M6:RA1(Ea,Ec,Ed,Ee);RA2(Ed);RA3(Ec),RA4(Ed)	100%	M5:RA3(Ea,Eb,Ef),RA5(Ed,Ee)	75%
	Conduct privacy impact assessments and develop, maintain, communicate, and train on privacy policies and procedures.	M1:RA1(Eb,Ec,Ed); M6:RA3(Eb),RA4(Ec)	75%	M5:RA1(Ee,Ef,Eg),RA2(Eb,Ee,Eg)	50%
	Enforce and uphold the organization's privacy and data protection program	M1:RA1(Ea); M6:RA4(Ea,Eb,Ec,Ed,Ee,Ef)	100%	M5:RA1(Ec,Ef),RA5(Eb,Ed,Ee)	50%

	Ensure that owners, holders, controllers, processors, subjects, partners and internal or external entities are informed about their data protection rights,	M6:RA4(E1)	25%	M5:RA2(Ea,Ed,Eg),RA5(Ee,Ef)	25%
	Act as a key point of contact to handle queries and complaints regarding data processing.	M6:RA4(Ee)	25%	M4:RA1(Ea,Ef,Eg),RA3(Ef,Eg)	25%
	Assist in the design, implementation, auditing, and compliance testing activities to ensure cybersecurity and privacy compliance.	M1:RA1(Ee);M6:RA4(Ec)	50%	M4:RA1(Eb,Ec,Ee),RA3(Ec,Ee)	25%
	Oversee audits and training activities related to data protection	M1:RA1(Ec,Ed,Ee)	50%	M5:RA3(Ed,Ef,Eg),RA4(Ea,Ec)	25%
	Cooperate and share information with authorities and professional groups	M1:RA5(Ee)	25%	M5:RA2(Ef,Eg)	25%
	Contribute to the development of the organization's cybersecurity strategy, policy, and procedures.	M1:RA1(Ec)	25%	M1:RA1(Ea,Eb,Ed)	25%
	Develop and propose staff awareness training to achieve compliance and foster a data protection culture within the organization.	M6:RA1(Ec),RA3(Ed)	50%	M5:RA2(Ee,Eg), RA3(Ea,Eb)	25%
	Manage the legal aspects of information security responsibilities and the ability to engage with third parties to address legal, regulatory, and policy requirements.	M6:RA1(Ee),RA4(Ea)	50%	M5:RA5(Mib,Ec, Ee)	25%
	Level of compliance		56%		35%
Key skill(s)	Comprehensive understanding of business strategy, models, and products, and the ability to address legal, regulatory, and policy requirements.	Ca, Cj	50%	Ca, Ck	25%
	Conduct work-life practices on data protection and privacy issues involved in the implementation of	Cd,Ce	100%	Ca, Cd, Ck	25%

	organizational, financial, and business strategy processes.				
	Lead the development of appropriate cybersecurity and privacy policies and procedures that complement business needs and legal requirements;	AC	25%	Ca, Cb, Cj, Cl	25%
	Conduct, monitor, and review privacy impact assessments using recognized standards, frameworks, methodologies, and tools.	Cj	50%	Ca, Cc, Ch, Cj	25%
	Explain and communicate data protection and privacy issues to stakeholders and users.	Cñ	50%	Cl,Cm	50%
	Understand, practice, and adhere to ethical requirements and standards.		0%	Cl	25%
	Understand the implications of legal framework changes on the organization's cybersecurity and data protection strategy and policies.	Ca,Cm	75%	Ca, Ck	25%
	Collaborate with other team members and colleagues.	Cñ	75%	Cm,Cl	75%
	Level of compliance		53%		34%
Key knowledge	Laws, regulations and legislation related to cybersecurity	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	100%	M4:RA6(C5,C6); M5:RA5(C3)	100%
	Cybersecurity standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M2:RA3(C1);M5:RA5(C1,C3)	100%
	Cybersecurity policies	M2:RA3(C4),RA9(C8)	50%	M1:RA4(C3,C5); M2;RA5(C1,C3)	75%
	Requirements, recommendations and best practices for legal, regulatory and legislative compliance	M2:RA3(C3,C5);M6:RA5(C3)	75%	M5:RA1(C1,C2), RA5(C2,C3)	50%
	Privacy Impact Assessment Standards, Methodologies, and Frameworks	M6:RA4(C3,C4)	25%	M4:RA2(C5,C7); M5:RA5(C1,C3)	25%
	Level of compliance		70%		70%

4- **Cyber Threat Intelligence** Specialist

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Develop, implement, and manage the organization's cyber threat intelligence strategy.	M1:RA4(Ea,Ec),RA5(Ea)	50%	M1:RA1(Ea,Eb,Ed);M5:RA5(Ea,Ec,Ee)	50%
	Develop plans and procedures to manage threat intelligence	M1:RA4(Ea,Ec),RA5(Ea)	50%	M5:RA5(Eb,Ed,Ef)	50%
	Translating business requirements into intelligence requirements		0%	M1:RA1(Ea,Ec,Ee)	25%
	Implement threat intelligence collection, analysis, and production of actionable intelligence and its dissemination to security stakeholders.		0%	M4:RA2(Ea,Ec,Ef)	25%
	Identify and assess cyber threat actors attacking the organization	M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb)	100%	M3:RA8(Ea,Eb,Ed)	75%
	Identify, monitor, and evaluate the tactics, techniques, and procedures (TTPs) used by cyber threat actors by analyzing open-source and proprietary data and information.	M1:RA2(Mib,Ec,Ed,Ee)	50%	M3:RA7(Ea,Ec),RA8(Ee,Eg)	50%
	Produce actionable reports based on threat intelligence data	M4:RA1(Ef),Ra3(Ec),RA5(Eh),RA6(Ea,Eb),M5:RA2(Eg),RA3(Ef)	100%	M4:RA4(Eb,Ec,Ed)	75%
	Develop and advise on mitigation plans at the tactical, operational, and strategic levels.	M1:RA4(Ea);M5:RA2(For example),RA3(For example),RA5(For example)	100%	M5:RA5(Ed,Ee)	100%
	Coordinate with stakeholders to share and consume intelligence on relevant cyber threats	M1:RA3(Ee)	25%	M5:RA2(Ef,Eg)	25%
	Leverage intelligence data to support and assist with threat modeling, risk mitigation recommendations, and cyber threat hunting.	M1:RA4(Ea),M6:RA3(Eb)	50%	M4:RA3(Mib,Ed,Ee),RA6(Ea,Eg)	50%

	Articulate and communicate intelligence openly and publicly at all levels		0%	M4:RA1(Ex.)	0%
	Convey the appropriate security severity by explaining risk exposure and its consequences to non-technical stakeholders.	M2:RA3(Ec,Ee)	25%	M4:RA4(Ea, Ef)	25%
	Level of compliance		46%		46%
Key skill(s)	Collaborate with other team members and colleagues.	Cñ	75%	Cl,Cm	75%
	Collect, analyze, and correlate cyber threat information from multiple sources	Cb	50%	Ca, Cb, Cc, Ch	75%
	Identify threat actors' TTPs and campaigns	Cb	25%	Ca,Cb	50%
	Automate threat intelligence management procedures		0%	Cg,Cl	0%
	Perform technical analysis and reporting	Cf	75%	Cc, Ck	100%
	Identify non-cyber events with implications for cyber activities		0%	Ca,Cd	50%
	Threats, actors and TTP of the model	Cb	25%	Ca,Cc	25%
	Communicate, coordinate and cooperate with internal and external stakeholders	Cñ	50%	Cm,Cn	50%
	Communicate, present and inform relevant stakeholders	Cm	25%	Cc, Ck	50%
	Use and apply CTI platforms and tools		0%	Cg, Ch	0%
	Level of compliance		33%		48%
Key knowledge	Operating system security	M7:RA3(C1,C2)	25%	M2:RA6(C1, C4);M3:RA11(C2,C3)	25%
	Computer network security	M2:RA3(C5,C6),RA6(C1)	50%	M3:RA5(C1, C2),RA6(C3)	100%
	Cybersecurity controls and solutions	M1:RA2(C2,C3,C4)	50%	M2:RA4(C3, C4);M3:RA10(C3,C5)	50%
	Computer programming	M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*)	100%	M2:RA2(C2, C6)	75%
	Cyber Threat Intelligence (CTI) Sharing Standards, Methodologies, and Frameworks		0%	M4:RA6(C1, C3,C5)	0%
	Responsible information disclosure	M1:RA3(C5)	25%	M4:RA6(C4,	25%

	procedures			C5)	
	Cross-domain and cross-border knowledge related to cybersecurity		0%	M1:RA1(C1, C4)	25%
	cyber threats	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	100%	M3:RA8(C3, C5);M4:RA2(C2,C6)	100%
	Cyber threat actors	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	100%	M3:RA9(C1, C2)	100%
	Cybersecurity attack procedures	M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6)	100%	M3:RA8(C4, C6)	100%
	Advanced Persistent Threats (APT)		0%	M4:RA3(C5)	25%
	Tactics, techniques, and procedures (TTPs) of threat actors		0%	M4:RA4(C4, C5)	25%
	Cybersecurity-related certifications		0%	M5:RA5(C3)	0%
	Level of compliance		42%		50%

5- Cybersecurity **Architect**

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Design and propose a secure architecture to implement the organization's strategy	M2:RA3(Ee),RA10(Eb)	50%	M1:RA1(Ea,Ee),RA3(Eb,Ec,Ed); M5:RA5(Eb,Ec,Ed)	50%
	Develop the organization's cybersecurity architecture to address security and privacy requirements.	M6:R4(Cc),RA5(Eg)	50%	M5:RA4(Ec,Ed),RA5(Ea,Ee)	75%
	Prepare architectural documentation and specifications.	M2:RA3(Ee)	25%	M4:RA4(Eb,Ed,Ef)	100%
	Present the high-level security architecture design to stakeholders		0%	M4:RA4(Ea,Ec,Ef)	50%
	Establish a secure environment throughout the development lifecycle of systems, services, and products	M2:RA6(Ef),RA10(Ef)	50%	M2:RA6(Ea,Eb,Ee)	75%
	Coordinate the development, integration, and maintenance of cybersecurity components, ensuring compliance with cybersecurity specifications.	M2:RA10(Ex.)	25%	M2:RA7(Eb,Ed,Eg)	50%
	Analyze and evaluate the cybersecurity of the organization's architecture.	M1:RA1(Ee),M2:RA3(Eb);M3:RA8(Ee)	100%	M3:RA3(Ea,Eb,Ed,Ee)	100%
	Ensure the security of solution architectures through security reviews and certification.		0%	M5:RA5(Ea,Ed,Ee)	25%
	Collaborate with other teams and colleagues	M4:RA1(Eg),RA3(Ed),RA4(Ef),RA5(Ei)	100%	M5:RA2(Ef,Eg)	100%
	Evaluate the impact of cybersecurity solutions on the design and performance of the organization's architecture.		0%	M3:RA7(Ec,Ee,Ef)	25%
	Adapt the organization's architecture to emerging threats	M1:RA2(Ea),M2:RA3(Ea),RA10(Ea)	75%	M1:RA4(Ea,Ed,Ef)	75%
	Evaluate the implemented architecture to maintain an adequate level of security	M2:RA3(Ee),RA6(Ea);M3:RA5(Eb)	75%	M5:RA5(Ec,Ee,Ef)	75%
	Level of compliance		46%		67%
Key skill(s)	Perform user and business security requirements analysis	Cb	50%	Ca, Cb, Cd	50%
	Develop architectural and functional	DC	50%	Cc, Ck	50%

	cybersecurity specifications				
	Decompose and analyze systems to develop security and privacy requirements and identify effective solutions	Cf	50%	Ca, Cg, Ch	50%
	Design systems and architectures based on cybersecurity principles of security and privacy by design and by default	Cc,Ce	75%	Cb,Cj	75%
	Guide and communicate with implementers and IT/OT staff	Cñ	25%	Cl,Cm	25%
	Communicate, present and inform relevant stakeholders		0%	Cc, Ck	25%
	Propose cybersecurity architectures based on stakeholders' needs and budgets		0%	Ca,Cb	25%
	Select appropriate specifications, procedures, and controls	Cc,Ce	100%	Cj,Cg	100%
	Develop resilience to points of failure throughout the architecture	CD	50%	Ce,Cn	50%
	Coordinate the integration of security solutions		0%	Cd,Cj	25%
	Level of compliance		40%		48%
Key knowledge	Cybersecurity-related certifications		0%	M1:RA2(C2,C3);M5:RA5(C3)	0%
	Cybersecurity recommendations and best practices	M2:RA3(C5);M6:RA5(C3)	50%	M2:RA5(C1,C3);M3:RA7(C1,C2)	50%
	Cybersecurity standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M2:RA3(C4);M5:RA5(C3)	100%
	Analysis of cybersecurity-related requirements		0%	M1:RA1(C2,C5)	25%
	Secure Development Lifecycle		0%	M1:RA4(C3)	50%
	Security architecture reference models	M2:RA6(C6);M3:RA7(C1)	50%	M3:RA2(C1,C6)	50%
	Technologies related to cybersecurity	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	100%	M2:RA2(C3);M3:RA5(C1,C4)	100%
	Cybersecurity controls and solutions	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(	100%	M2:RA4(C4);M3:RA10(C2,C5)	100%

		C1,C6,C8);M3:RA2(C3)			
	Cybersecurity risks	M2:RA3(C1),M3:RA5(C2);M6:RA2(C3)	100%	M2:RA3(C4);M5:RA5(C2,C3)	100%
	cyber threats	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	100%	M3:RA8(C1,C5);M4:RA2(C2,C7)	100%
	Trends in cybersecurity	M2:RA7(C1)	25%	M3:RA2(C8,C10)	50%
	Requirements, recommendations and best practices for legal, regulatory and legislative compliance	M2:RA3(C3,C5); M6:RA5(C3)	50%	M5:RA1(C2)	50%
	Legacy cybersecurity procedures	M6:RA1(C1,C3), RA3(C*),RA5(C3,C4,C5,C6,C7,C8)	100%	M1:RA5(C1,C2)	100%
	Privacy Enhancing Technologies (PET)	M2:RA4(C1,C2); M6:RA4(C3,C4)	75%	M5:RA5(C3)	25%
	Privacy by Design Standards, Methodologies, and Frameworks	M6: RA4(C2), RA5(C2, C4, C6, C7, C8)	75%	M5:RA5(C1,C3)	25%
	Level of compliance		62%		62%

6- Cybersecurity Auditor Cybersecurity Auditor

	Detail	HE	IT RATE	Old Testament	OT RATE
Main	Develop the organization's audit	M1:RA1(Ee);M2:RA	50%	M1:RA5(Ef,Eg);	25%

task(s)	policy, procedures, standards, and guidelines.	2(Ec)		M5:RA5(Eb,Ee)	
	Establish the methodologies and practices used for systems auditing.	M3:RA7(Ec),M5:RA2(Ei),RA4(Eb)	75%	M2:RA3(Ea,Ec);M5:RA3(Ec,Ef)	50%
	Establish the target environment and manage audit activities	M3:RA7(Ec),M5:RA2(Ei),RA4(Eb)	75%	M4:RA1(Ee,Eg);M5:RA1(Ef,Eg)	50%
	Define the scope of the audit, the objectives and the criteria for auditing	M6:RA2(Ec)	25%	M2:RA5(Ed,Ee);M5:RA4(Ed,Ef)	25%
	Develop an audit plan that describes the audit frameworks, standards, methodology, procedures, and tests.		0%	M1:RA3(Ed,Eh);M3:RA10(Ea,Ec)	0%
	Review the assessment objective, security objectives, and requirements based on the risk profile	M2:RA3(Ec,Ee),RA8(Ee);M3:RA5(Eb,Ed),RA6(Eb)	100%	M1:RA1(Ec,Ee);M2:RA3(Eb,Ej)	50%
	Audit compliance with applicable laws and regulations related to cybersecurity	M1:RA1(Ee)	25%	M3:RA3(Ed,Ee);M5:RA5(Ee,Ed)	25%
	Audit compliance with applicable cybersecurity standards		0%	M1:RA5(Ec,Ee);M2:RA5(Ec,Ef)	0%
	Execute the audit plan and collect evidence and measurements	M1:RA3(Ea,Eb,Ec)	50%	M3:RA10(Eb,Ed);M4:RA2(E,Eg)	50%
	Maintain and protect the integrity of audit records	M2:RA8(Eh)	25%	M4:RA1(Ec,Ed);M5:RA5(Ef,Eg)	25%
	Develop and communicate conformity assessment, assurance, audit, certification, and maintenance reports.		0%	M2:RA4(Eb,Ed);M4:RA1(Ef,Eg)	0%
	Monitor risk remediation activities	M1:RA1(Ei)	25%	M3:RA8(Mib,Ef);M5:RA5(Ed,Ee)	25%
	Level of compliance		38%		27%
Key skill(s)	Organize and work systematically and deterministically based on evidence.	Cc,Ce	75%	Cc,Cg	75%
	Follow and practice audit frameworks, standards and methodologies.	Cc,Ce	75%	Ch,Ck	50%
	Apply audit tools and techniques	Cb,Cf	75%	Ca, Cb, Ci	50%
	Analyze business processes, evaluate and review software or	Cg	25%	Ca, Ch, Cj	25%

	hardware security, as well as technical and organizational controls.				
	Break down and analyze systems to identify weaknesses and ineffective controls	Cb,Cf	50%	Ck,Cm	25%
	Communicate, explain, and adapt legal and regulatory requirements and business needs.	Cm	25%	Cd,Cl	25%
	Collect, evaluate, maintain, and protect audit information	Cb,Cf	75%	Ca,Cm	50%
	Audit with integrity, being impartial and independent		0%	Cb,Cj	0%
	Level of compliance		50%		38%
Key knowledge	Cybersecurity controls and solutions	M1:RA2(C2,C3,C4); M2:RA5(C5),RA8(C1),RA10(C1,C6,C8); M3:RA2(C3)	100%	M2:RA4(C3,C4);M3:RA10(C2,C3,C5)	100%
	Requirements, recommendations and best practices for legal, regulatory and legislative compliance	M2:RA3(C3,C5);M6:RA5(C3)	75%	M5:RA5(C2,C3)	50%
	Monitoring, testing, and evaluating the effectiveness of cybersecurity controls	M1:RA2(C2,C4);M2:RA7(C13,C14,C18)	100%	M3:RA9(C1,C2);M5:RA5(C1,C2)	75%
	Standards, methodologies and conformity assessment frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M5:RA5(c3)	75%
	Audit standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M3:RA10(C3,C4);M4:RA6(C5,C6)	75%
	Cybersecurity standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M2:RA3(C4);M5:RA5(C3)	50%
	Audit-related certification		0%	M5:RA5(C3)	0%
	Cybersecurity-related certifications		0%	M1:RA2(C1,C2);M5:RA5(C3)	0%
	Level of compliance		72%		53%

7- Cybersecurity **Educator**

	Detail	HE	RATE	Old Testament	RATE
Main task(s)	Develop, update, and deliver cybersecurity and data protection curricula and educational materials for training and awareness based on the content, methods, tools, and needs of participants.		0%	M1:RA3(Eh); M5:RA5(Eb,Ee)	0%
	Organize, design, and deliver cybersecurity and data protection awareness activities, seminars, courses, and practical training.	M1:RA1(Ec,Ed,Ee)	50%	M2:RA4(Ed,Ee);M5:RA5(Ef,Eg)	25%
	Monitor, evaluate and report on the effectiveness of training		0%	M4:RA1(Ee,Ef),M5:RA3(Ef,Eg)	0%
	Evaluate and report on the learner's performance		0%	M5:RA5(Ef,Eg)	0%
	Finding new approaches to education, training and awareness-raising	M1:RA1(Ec,Ed,Ee)	50%	M1:RA5(Ee,Ef);M3:RA8(Ef,Eg)	25%
	Design, develop, and deliver cybersecurity simulations, virtual labs, or cyber field environments.		0%	M2:RA2(Ec.Ed);M4:RA3(Ec,Ef)	0%
	Provide guidance on cybersecurity certification programs for individuals		0%	M1:RA3(Eh,Ei);M5:RA5(Ee,Ef)	0%
	Maintain and continuously improve expertise; foster and enhance the continuous improvement of cybersecurity capabilities and capacity development.		0%	M2:RA3(Ej,Ee);M5:RA3(Eg,Ef)	0%
	Level of compliance		13%		6%
Key skill(s)	Identify cybersecurity awareness, training, and education needs	AC	50%	Ca,Cl	25%
	Design, develop, and deliver learning programs to meet cybersecurity needs.	Cm	25%	Ck,Cl	25%
	Develop cybersecurity exercises that include simulations using cyber-range environments.		0%	Cd,Cg	25%
	Provide training to obtain professional certifications in		0%	Ck,Cl	50%

	cybersecurity and data protection.				
	Use existing cybersecurity-related training resources		0%	Ca,Cl	0%
	Develop evaluation programs for awareness-raising, training and education activities.		0%	Ck,Cl	25%
	Communicate, present and inform relevant stakeholders	Cñ	25%	Cm,Cl	25%
	Identify and select pedagogical approaches appropriate for the target audience.	Cñ	25%	Ck,Cl	25%
	Motivate and encourage people	Cñ	50%	Cl,Cm	50%
	Level of compliance		19%		28%
Key knowledge	Standards, methodologies and pedagogical frameworks		0%	M5:RA1(C1)	0%
	Development of cybersecurity awareness, education, and training programs	M1:RA1(C3,C4)	25%	M1:RA4(C7); M5:RA1(C3)	25%
	Cybersecurity-related certifications		0%	M1:RA2(C2); M5:RA5(C3)	0%
	Cybersecurity education and training standards, methodologies, and frameworks		0%	M5:RA5(C1,C3)	0%
	Laws, regulations and legislation related to cybersecurity	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	100%	M5:RA5(C3)	100%
	Cybersecurity recommendations and best practices	M2:RA3(C5,C7);M6:RA5(C3)	50%	M2:RA5(C3); M3:RA7(C2,C5)	50%
	Cybersecurity standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	100%	M5:RA5(C3)	75%
	Cybersecurity controls and solutions	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	100%	M2:RA4(C3,C4);M3:RA10(C3,C5)	75%
	Level of compliance		47%		41%

8- Cybersecurity **Implementer**

	Detail	HE	IT RATE	Old Testament	OT RATE

Main task(s)	Develop, implement, maintain, update, and test cybersecurity products	M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(Ed,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),Ra7(Ec,Ed);M4:RA2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),RA3(Ec,Ee),RA4(E*),RA5(Ec,Ed,Ee,Ef),RA6(Ea,Ec,Ed)	100%	M1:RA3(Ec,Ef);M5:RA5(Ef,Eg)	100%
	Provide cybersecurity-related support to users and customers		0%	M2:RA4(Ec,Ed);M5:RA5(Ee,Ef)	50%
	Integrate cybersecurity solutions and ensure their proper functioning		0%	M1:RA3Ec,Ei);M3:RA4(Eg,Eh)	50%
	Configure systems, services, and products securely	M2:RA4(Ea,Eb,Ec,Ed,Ee),Ra5(Ee),RA6(Ef),RA7(Ea,Eb,Ec,Ed,Ee,Eh,Ei),Ra8(Ec,Eg,Eh),Ra9(Eb,Ed),RA10(Ed);M3:RA6(Ei),RA8(Ec);M5:RA2(Ea)	100%	M2:RA6(Ed,Ee);M5:RA4(Ec,Ef)	100%
	Maintain and update the security of systems, services and products.	M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(Ed,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),Ra7(Ec,Ed);M4:RA2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),R	100%	M1:RA4(Mib,Ef);M5:RA3(Mie,Eg)	100%

		A3(Ec,Ee),RA4(E*),RA5(Ec,Ed,Ee,Ef),RA6(Ea,Ec,Ed)			
	Implement cybersecurity procedures and controls	M1:RA4(Ea),RA5(Ea);M3:RA8(Ef);M6:RA1(Ec),RA5(Ee,Ef)	100%	M2:RA3(Ef,Eh);M5:RA1(Eg,Eg)	100%
	Monitor and ensure the performance of implemented cybersecurity controls	M1:RA2(Eb,Ec,Ed)	25%	M3:RA7(Ed,Ee);M5:RA3(Ef,Eg)	50%
	Document and report on the security of systems, services and products	M1:RA2(Ee),RA4(Ee);M3:RA8(Ef);M4:RA1(Ed),RA5(Ee),RA6(Ec)	100%	M2:RA4(Eb,Ed);M4:RA1(Ed,Ef)	100%
	Work closely with IT/OT staff on cybersecurity-related actions	M2:RA10(E*)	75%	M1:RA1(Eb,Ed);M2:RA1(Ef,Eg)	75%
	Deploy, apply, and manage patches to products to address technical vulnerabilities	M2:RA4(Eb,Ec,Ed,Ee),RA10Eg,Eh);M3:RA6(Ec);M5:RA2(Ee),RA3(Ee),RA5(Ed,Ee,Ef),	100%	M2:RA6(Ea,Ed);M3:RA8(Ea,Eb)	100%
	Level of compliance		70%		83%
Key skill(s)	Communicate, present and inform relevant stakeholders	Cñ	25%	Cm, Ck	25%
	Integrate cybersecurity solutions into the organization's infrastructure	Cd, Ce, Cg, Ch	100%	Cj,Cb	100%
	Configure solutions according to the organization's security policy	CD	25%	Cf. Ch.	100%
	Evaluate the security and performance of solutions	Cf,Ci	50%	Cc, Cd	50%
	Develop code, scripts and programs	Cg	75%	Cl,Ce	75%
	Identify and resolve cybersecurity-related issues	Cf,Ci	100%	Cm,Cg	100%
	Collaborate with other team members and colleagues.	Cñ	75%	Cn,Cl	75%
	Level of compliance		64%		75%
Key knowledge	Secure Development Lifecycle	M3:RA8(C*)	50%	M1:RA1(C1,C5),RA4(C3)	50%
	Computer programming	M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*)	100%	M2:RA2(C2,C6)	75%

	Operating system security	M7:RA3(C1,C2)	25%	M2:RA6(C1,C4);M3:RA11(C2,C3)	25%
	Computer network security	M2:RA3(C5,C6), RA6(C1)	50%	M3:RA5(C1,C2,C4),RA6(C1,C3)	75%
	Cybersecurity controls and solutions	M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	100%	M2:RA4(C4),M3:RA10(C2,C3,C5)	100%
	Offensive and defensive security practices	M5:RA1(C4),RA2(C*),RA3(C*)	100%	M3:RA8(C3,C5);M4:RA6(C2,C6)	50%
	Secure coding recommendations and best practices	M3: RA5(C1,C2,C3,C4), RA6(C1,C3,C4,C5,C6,C7,C8,C9,C10,C11), RA7(C1,C2,C3,C4,C5,C6), RA8(C1,C2,C3,C4,C5,C6,C7,C8,C9)	100%	M2:RA2(C2,C3)	75%
	Cybersecurity recommendations and best practices	M2:RA3(C5,C7); M6:RA5(C3);	75%	M5:RA5(C2,C3)	75%
	Standards, methodologies and testing frameworks	M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5)	100%	M3:RA9(C1,C2)	100%
	Test procedures	M5:RA1(C2,C3)	25%	M3:RA5(C1,C4)	25%
	Technologies related to cybersecurity	M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	100%	M2:RA2(C2);M3:RA5(C1,C4)	100%
	Level of compliance		75%		68%

9- Cybersecurity **Researcher**

	Detail	HE	IT RATE	Old	OT RATE

				Testament	
Main task(s)	Analyze and evaluate cybersecurity technologies, solutions, developments, and processes.	M1:RA2(Eb,Ec,Ed),RA3(Eb,Ec,Ed);M2:RA10(Ee,Eg);M5:RA6(Eb,Ec)	100%	M2:RA3(Ea,Ec); M5:RA5(Ed,Ef)	75%
	Carry out research, innovation and development work on topics related to cybersecurity	M1:RA2(Ed),RA3(Ed); M5:RA5(Ee,Ef)	100%	M1:RA3(Ec,Eh); M4:RA3(Ec,Ef)	75%
	Express and generate research and innovation ideas		0%	M5:RA5(Ee,Eg)	25%
	Advance the current state of the art in cybersecurity-related issues		0%	M1:RA1(Ed,Ee); M4:RA3(Ed,Eg)	25%
	Contribute to the development of innovative solutions related to cybersecurity.	M3:RA4(Ee),RA5(Eb,Ec),RA6(E*),RA7(Ec,Ed)	100%	M3:RA8(Ef,Eg); M5:RA3(Ef,Eg)	75%
	Conduct experiments and develop proofs of concept, pilots, and prototypes for cybersecurity solutions.	M5:RA2(E*),RA3(E*),RA5(E*)	100%	M2:RA3(Ej,Eh); M4:RA2(Ee,Eg)	75%
	Select and apply frameworks, methods, standards, tools, and protocols, including creating and testing a proof of concept to support projects.	M5:RA2(E*),RA3(E*),RA5(E*)	100%	M1:RA3(Ed,Ei); M3:RA10(Ea,Ed)	100%
	Contribute to cutting-edge cybersecurity business ideas, services, and solutions.		0%	M1:RA5(Ef,Eg); M5:RA5(Eg,Eh)	0%
	Contribute to the development of cybersecurity-related capabilities, including awareness, theoretical training, practical training, testing, mentoring, supervision, and exchange.	M1:RA1(Ec,Ed,Ee);M5:RA2(E*),RA3(E*),RA5(E*)7	100%	M1:RA5(Ef,Eg); M5:RA5(Eg,Eh)	100%
	Identify cross-sector achievements in cybersecurity and apply them in a different context or propose innovative approaches and solutions		0%	M1:RA5(Eg,Ef); M5:RA5(Eg,Ef)	0%

	Lead or participate in innovation processes and projects, including project management and budgeting.		0%	M2:RA1 (Ef,Eg); M3:RA2 (Ef,Eg)	0%
	Publish and present scientific papers and research and development results	M1:RA5(Eb,Ec,Ed,Ee), M4:RA1(Ef,Eg),RA3(Ed) ,RA4(Ef),RA5(Ei)	100%	M1:RA3 (Ed,Eh); M5:RA5 (Ee,Ef)	75%
	Level of compliance		58%		52%
Key skill(s)	Generate new ideas and transfer theory into practice.	Cn	25%	Ca,Cl	75%
	Break down and analyze systems to identify weaknesses and ineffective controls	Cb, Cf, Ci	100%	Cb,Ch	100%
	Decompose and analyze systems to develop security and privacy requirements and identify effective solutions	Ce,Cf	75%	Cc, Cd, Cf	75%
	Monitor new developments in cybersecurity-related technologies	Cg, Ck	75%	Ce,Cl	75%
	Communicate, present and inform relevant stakeholders	Cñ	25%	Ck,Cm	25%
	Identify and resolve cybersecurity-related issues	Cf,Ci	75%	Cm,Cg	75%
	Collaborate with other team members and colleagues.	Cñ	75%	Cn,Cm	75%
	Level of compliance		64%		71%
Key know ledge	Research, development and innovation (R&D&I) related to cybersecurity	M6:RA1(Cd)	25%	M1:RA1 (C1,C4); M4:RA2 (C7,C9)	25%
	Cybersecurity standards, methodologies and frameworks	M1:RA4(C1);M2:RA3(C 6);M3:RA5(C2,C4),RA6 (C4);M6:RA5(C2,C5)	100%	M2.RA3(C4);M5: RA5(C3)	100%
	Legal, regulatory and legislative requirements on the release or use of cybersecurity-related technologies	M4:RA4(C2);M6:RA4(C *),RA5(C3,C6,C7,C8)	100%	M5:RA5 (C2,C3)	75%
	Multidisciplinary aspect of cybersecurity		0%	M1:RA1 (C2,C5); M5:RA1 (C1,C3)	0%
	Responsible information disclosure procedures	M1:RA3(C5)	25%	M4:RA6 (C4,C5)	25%

	Level of compliance	50%		45%

10- **Cybersecurity Risk** Manager

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Developing a cybersecurity risk management strategy for an organization	M2:RA3(Ec,Ee), M3:RA5(Eb);M 6:RA4(Ee)	100%	M1:RA1(Ed,Ee); M5:RA5(Ea,Ec)	100%
	Manage an inventory of the organization's assets	M5:RA3(Eb),RA 5(Eb)	50%	M1:RA1(Mib,Ec);M2:RA3(Mib,E c)	100%
	Identify and assess threats and vulnerabilities related to the cybersecurity of ICT systems	M1:RA2(Eb,Ec, Ed);M2:RA3(Ea) ,RA7(Ef);M3:RA 5(Ea,Eb)	100%	M2:RA3(Ec,Ed); M3:RA8Ea,Eb)	100%
	Identification of the threat landscape, including attacker profiles and estimation of attack potential.	M1:RA2(Mib,Ec ,Ed,Ee)	50%	M4:RA2(Ef,Eg); M5:RA5(Ee,Eg)	75%
	Evaluate cybersecurity risks and propose the most appropriate risk treatment options, including security controls and risk mitigation and prevention that best address the organization's strategy.	M5:RA2(Eg),RA 3(Ef),RA5(Eg)	75%	M1:RA3(Ed,Eh); M5:RA5(Ed,Ef)	75%
	Monitor the effectiveness of cybersecurity controls and risk levels	M1:RA2(Eb,Ed); M2:RA7(Eh);M 3·:RA7(Ed);M5: RA1(Ei)	100%	M3:RA7(Ed,Ee); M5:RA3(Ef,Eg)	100%
	Ensure all cybersecurity risks are kept at an acceptable level for the organization's assets.	M2:RA3(Ec,Ee)	25%	M5:RA5(Ee,Ef)	100%
	Develop, maintain, report, and communicate comprehensive risk management cycle guidelines and ensure compliance with regulations and standards.	M2:RA3(Ec,Ee), M3:RA5(Eb);M 6:RA4(Ee)	100%	M1:RA3(Ei,Eh); M4:RA1(Ef,Eg)	100%
	Level of compliance		75%		94%
Key skill(s)	Implement cybersecurity risk management frameworks, methodologies, and tools. guidelines and ensure compliance with regulations and standards	Ce, Cf, Ci	100%	Ca, Cb, Cj, Cn	100%
	Analyze and consolidate the organization's quality and risk management practices.	Ce, Cf, Ci, Cp	100%	Cg,Cñ	100%

	Empower business asset owners, executives, and other stakeholders to make risk-based decisions to manage and mitigate risks.	Ce, Cf, Ci	100%	Cm,Cl	100%
	Building a cybersecurity-aware environment	Ce, Cf, Ci	100%	Ce,Cc	100%
	Communicate, present and inform relevant stakeholders	Cñ	75%	Ck,Cm	25%
	Propose and manage risk sharing options	Ce, Cf, Ci	75%	Cd,Ch	100%
	Level of compliance		92%		88%
Key know ledge	Risk management standards, methodologies and frameworks	M2:RA3(C1); M3:RA5(C2);M 6:RA2(C3)	25%	M2:RA3(C3);M5 :RA5(C1)	50%
	Risk management tools	M6:RA2(C3)	25%	M2:RA3(C7);M3 :RA3(C2)	50%
	Risk management recommendations and best practices	M2:RA3(C1);M 3:RA5(C2),M6: RA2(C3)	100%	M5:RA5(C2)	100%
	cyber threats	M1:RA3(C4);M 2:RA3(C1);M3: RA5(C2)	100%	M2:RA3(C2)	100%
	Vulnerabilities of computer systems	M2:RA10(C10); M3:RA6(C2,C6) ;M5:RA3(C6,C9),RA5(C5,C6,C7)	100%	M3:RA8(C1)	100%
	Cybersecurity controls and solutions	M1:RA2(C2,C3, C4);M2:RA5(C5),RA8(C1),RA10 (C1,C6,C8);M3: RA2(C3)	100%	M2:RA4(C5,C6)	100%
	Cybersecurity risks	M2:RA3(C1); M3:RA5(C2);M 6:RA2(C3);	25%	M1:RA2(C3);M5 :RA5(C3)	75%
	Monitoring, testing, and evaluating the effectiveness of cybersecurity controls	M1:RA2(C2,C4) ;M2:RA7(C13,C 14,C18)	75%	M1:RA4(C5);M3 :RA9(C2)	75%
	Cybersecurity-related certifications		0%	M5:RA5(C3)	0%
	Technologies related to cybersecurity	M1:RA2(C2,C3, C4);M2:RA5(C5),RA8(C1),RA10 (C1,C6,C8);M3: RA2(C3)	100%	M1:RA3(C4);M2 :RA1(C3)	100%
	Level of compliance		65%		75%

11- Digital Forensics Investigator

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Develop digital forensic investigation policies, plans, and procedures	M4:RA1(Ea,Eb, Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb), RA4(Ea,Eb,Ec), RA5(Ea,Eb,Ec,E d,Ee,Ef,Eg)	100%	M4:RA1(Ea,Ed); M5:RA5(Ec,Ef)	75
	Identify, recover, extract, document, and analyze digital evidence	M4:RA1(Ea,Eb, Ee),RA3(Ea),RA 5(Ea,Eb,Ec,Ed,E f)	75%	M3:RA9(Ea,Ed); M4:RA2(Eb,Ec)	75
	Preserve and protect digital evidence and make it available to authorized stakeholders	M4:RA1(Ea,Eb, Ee),RA3(Ea),RA 5(Ea,Eb,Ec,Ed,E f)	75%	M4:RA1(Ec,Ee); M5:RA1(Ef,Eg)	25
	Inspect environments for evidence of unauthorized and illegal actions.	M4:RA1(Ea,Eb, Ee),RA3(Ea),RA 5(Ea,Eb,Ec,Ed,E f)	75%	M3:RA8(Mib,Ee);M4:RA3(Ea,Ec)	50
	Document, report, and present the findings and results of digital forensics in a systematic and deterministic manner.	M4:RA1(Ef,Eg), RA3(Ec,Ed),RA4 (Ef),RA5(Eh,Ei), RA6(E*)	100%	M2:RA4(Eb,Ed); M4:RA1(Ef,Eg)	75
	Select and customize forensic testing, analysis, and reporting techniques for actors	M4:RA1(Ea,Eb, Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb), RA4(Ea,Eb,Ec), RA5(Ea,Eb,Ec,E d,Ee,Ef,Eg)	100%	M1:RA3(Eh,Ei): M4:RA2(Ed,Ef)	50
	Level of compliance		88%		58.33
Key skills	Work ethically and independently, without internal or external influences or prejudices. actors	Ch,Co	75%	Cl,Cn	25
	Collect information while preserving its integrity	Ch	75%	Ci, Ck	75
	Identify, analyze, and correlate cybersecurity events	Ch	75%	Ca, Cb, Ch	75
	Explain and present digital evidence in a simple, straightforward, and easy-to-understand manner.	Cm	50%	Cc, Ck	100
	Prepare and communicate detailed and reasoned research reports.	Cm	75%	Cc,Cj	75

	Level of compliance		70%		70
Key know ledge	Digital Forensics Recommendations and Best Practices	M4:RA1(C2,C4),RA4(C3)	75%	M4:RA1(C2),RA4(C6)	50
	Digital forensic investigation standards, methodologies, and frameworks	M4:RA1(C4),RA3(C1,C2),RA4(C3)	100%	M4:RA1(C3)	50
	Digital forensic analysis procedures	M4:RA1(C7,C8,C10),RA2(C4,C5,C6,C7),RA3(C3),RA5(C3)	100%	M4:RA1(C6);M4:RA1(C3)	75
	Test procedures	M5:RA1(C2,C3)	50%	M4:RA2(C10)	50
	Procedures, standards, methodologies and frameworks for criminal investigation		0%	M4:RA2(C3),RA5(C4)	25
	Laws, regulations and legislation related to cybersecurity	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	100%	M5:RA5(C2,C3)	0
	Malware analysis tools	M4:RA2(C3)	50%	M4:RA1(C9,C10),RA6(C2,C6)	75
	cyber threats	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	100%	M4:RA3(C6)	50
	Vulnerabilities of computer systems	M2:RA10(C10);M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7)	100%	M3:RA8(C1,C5);M4:RA5(C2,C3)	75
	Cybersecurity attack procedures	M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6)	100%	M3:RA8(C5,C6)	75
	Operating system security	M7:RA3(C1,C2)	75%	M2:RA6(C3,C4);M3:RA11(C3,C4)	75
	Computer network security	M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3)	100%	M3:RA2(C10),RA10(C2)	75
	Cybersecurity-related certifications		0%	M5:RA5(C3)	0
	Level of compliance		73%		51.92

12- Penetration Tester Penetration Tester

	Detail	HE	IT RATE	Old Testament	OT RATE
Main task(s)	Identify, analyze, and evaluate technical and organizational cybersecurity vulnerabilities	M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb)	100%	M2:RA3(Ec,Ee);M3:RA8(Ea,Eb)	100%
	Identify attack vectors, discover and demonstrate the exploitation of technical cybersecurity vulnerabilities.	M2:RA10(Eh);M3:RA5(E*);M5:RA3(Ee),RA5(Ee,Ef)	100%	M3:RA8(Ec,Eg);M4:RA2(Eb,Ed)	100%
	Testing systems and operating compliance with regulatory standards	M2:RA3(Ef),M3:RA5(Ea,Eb);M6:RA5(Ef)	100%	M1:RA3(Eh,Ei);M5:RA5(Ee,Ef)	100%
	Select and develop appropriate penetration testing techniques	M5:RA1(Ee,Ef,Eg,Eh),RA2(Ea,Ec,Ed,Ee,Ef),RA3(Ea,Eb,Ec,Ed,Ee),RA4(E*),RA5(Ea,Eb,Ec,Ed,Ee,Ef),RA6(E*)	100%	M3:RA8(Ed,Ef);M4:RA3(Ee,Eg)	100%
	Organize test plans and procedures for penetration testing	M5:RA1(Ec),RA2(Ef),RA3(Eb),R5(Ea)	75%	M1:RA3(Ed,Eh);M5:RA5(Ec,Ef)	50%
	Establish procedures for analyzing and reporting penetration test results.	M5:RA2(Eg),RA3(Ef),RA5(Eg)	75%	M2:RA4(Ed,Ef);M4:RA1(Ef,Eg)	75%
	Document and report penetration test results to stakeholders	M1:RA3(Ee),RA4(Ee);M5:RA2(Eg),RA3(Ef),RA5(Eg)	100%	M2:RA4(Eb,Ed);M4:RA2(Mie,Ef)	100%
	Implement penetration testing tools and testing programs		0%	M3:RA8(Ee,Ef);M4:RA2(Eb,Ed)	0%
	Level of compliance		81%		78%
Key skill(s)	Develop codes, scripts and programs	Cg	75%	Ch, Ck, Cl	75%
	Perform social engineering	Cb	75%	Ca,Cd	75%
	Identify and exploit vulnerabilities	Cc, Cf, Ci	100%	Ch,Ci	100%
	Perform ethical hacking	Cf	100%	Cg,Cj	75%
	Think creatively and outside the box	Cn,Cñ	75%	Cm	75%
	Identify and resolve cybersecurity-related issues	Cf,Ci	75%	Cm	75%

	Communicate, present and inform relevant stakeholders	Cñ	25%	Cc, Ck	25%
	Use penetration testing tools effectively	Cb,Cf	100%	Cb,Cj	75%
	Perform technical analysis and reporting	Cf	75%	Cc,Cl	75%
	Break down and analyze systems to identify weaknesses and ineffective controls	Cb, Cf, Ci	100%	Ce,Cf	75%
	Review codes to assess their security	Cg	50%	Cb,Ck	50%
	Level of compliance		77%		70%
Key knowledge	Cybersecurity attack procedures	M5: RA1(C4), RA2(C4, C5), RA3(C5, C6, C7, C8, C9), RA4(C2), RA5(C3, C6)	100%	M3:RA8(C5); M4:RA6(C1,C2)	100%
	Information technology (IT) and operational technology (OT) devices	M2:RA10(C*)	75%	M2:RA1(C1,C2,C3)	75%
	Offensive and defensive security procedures	M5:RA1(C4),RA2(C*),RA3(C*)	100%	M3:RA8(C5,C6);M5:RA1(C3)	75%
	Operating system security	M7:RA3(C1,C2)	75%	M2:RA6(C3,C4);M3:RA11(C3,C4)	75%
	Computer network security	M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3)	100%	M3:RA10(C2,C4)	75%
	Penetration testing procedures	M5:RA1(C3,C4), RA2(C5),RA3(C*),RA4(C2,C3),RA5(C3,C5,C6),RA6(C4)	100%	M3:RA8(C4); M4:RA2(C10)	75%
	Penetration testing standards, methodologies, and frameworks	M5:RA1(C3,C4), RA2(C5),RA3(C*),RA4(C2,C3),RA5(C3,C5,C6),RA6(C4)	100%	M4:RA2(C9,C10)	75%
	Penetration testing tools	M2:RA10(C15); M3:RA6(C10),RA8(C8);M5:RA1(C7,C8),RA3(C6),RA5(C6),RA6(C*)	100%	M3:RA6(C3)	75%

	Computer programming	M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*)	100%	M3:RA5(C2,C3),RA8(C1,C2)	100%
	Vulnerabilities of computer systems	M2:RA10(C10); M3:RA6(C2,C6); M5:RA3(C6,C9), RA5(C5,C6,C7)	100%	M5:RA5(C2,C3)	100%
	Cybersecurity recommendations and best practices	M2:RA3(C5);M6:RA5(C3)	100%	M5:RA5(C3)	100%
	Cybersecurity-related certifications		0%		0%
	Level of compliance		88%		77%

Tknika

Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre