Project Title	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training
Project Acronym	CYBERWISER.EU
Project Number	786668
Type of instrument	Innovation Action
Topic	DS-07-2017 Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
Starting date of Project	01/09/2018
Duration of the project	30
Website	www.cyberwiser.eu

D4.1 Training material, initial version

Work Package	WP4 Training material, scenarios and evaluation
Lead author	Gencer Erdogan (SINTEF)
Contributors	Dario Varano (UNIPI), Gianluca Dini (UNIPI), Gigliola Vaglini (UNIPI), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Liliana Ribeiro (EDP), José Ferreira Lourenço (EDP), Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT), Aida Omerovic (SINTEF), Ketil Stølen (SINTEF), Åsmund Hugo (SINTEF)
Peer reviewers	Rodrigo Diaz (ATOS), Valerio Vitangeli (FFSS)
Version	2.0
Due Date	15/02/2020
Submission Date	14/02/2020

Dissemination Level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the CYBERWISER project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786668.

Version History

Revision	Date	Editor	Comments
0.1	20/02/2019	Gencer Erdogan (SINTEF)	Initial version of the deliverable. Initial outline as well as initial set of courses for the Primer and Basic offering levels.
0.2	26/02/2019	Gencer Erdogan (SINTEF)	Updated course tables based on feedback in the WP4 status meeting 22.02.2019.
0.3	12/03/2019	Gencer Erdogan (SINTEF)	Initial complete description of courses in the Primer and Basic offering level.
0.4	22/03/2019	Dario Varano (UNIPI), Gianluca Dini (UNIPI), Gigliola Vaglini (UNIPI), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Liliana Ribeiro (EDP), Gencer Erdogan (SINTEF)	Updated Section 4.2 about course templates (UNIPI). Complete version of Section 3 (SINTEF).
0.5	26/03/2019	Gencer Erdogan (SINTEF)	Included text and supporting figure in Section 3.4. Updated the course descriptions in Section 4.
0.6	27/03/2019	Gencer Erdogan (SINTEF)	Updated course descriptions in Section 4 and included course description templates for the awareness courses.
0.7	29/03/2019	Gencer Erdogan (SINTEF)	Initial complete version of Section 2.2. Moved course templates to Section 2.1.
0.8	29/03/2019	Dario Varano (UNIPI), Gianluca Dini (UNIPI)	Added content for section 2
0.9	01/04/2019	Gencer Erdogan (SINTEF)	Initial complete version of Section 1.
0.10	02/04/2019	Dario Varano (UNIPI)	Updated Section 2 by including comments
0.11	08/04/2019	Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Liliana Ribeiro (EDP), Gencer Erdogan (SINTEF)	Updated Section 2 by including profile descriptions. Updated Section 3 with the process carried out for identifying cybersecurity risks to be covered in the awareness courses. Updated Section 4 with new descriptions of some of the courses.
0.12	12/04/2019	Gencer Erdogan (SINTEF)	Removed the usage of ECTS credits from the course templates and the course descriptions (based on a discussion by all WP4 partners).
0.13	29/05/2019	Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT)	Input on section 6
0.14	31/05/2019	Aida Omerovic (SINTEF), Ketil Stølen (SINTEF)	Executive summary, conclusions, references to the applicable documents.
0.15	10/06/2019	Aida Omerovic (SINTEF), Ketil Stølen (SINTEF)	Final edits before internal review.
0.16	14/06/2019	Maria Teresa Garcia Gonzalez (Atos), Åsmund Hugo (SINTEF)	Updates based on the internal review and first Quality Check.

Revision	Date	Editor	Comments
0.17	14/06/2019	Åsmund Hugo (SINTEF)	Final edits. Ready for Final Quality Check.
1.0	17/06/2019	Maria Teresa Garcia Gonzalez (ATOS)	Quality Check performed. Deliverable ready for submission.
1.1	16/01/2020	Gencer Erdogan (SINTEF)	Included comments and new sections to guide the updating of D4.1 with respect to comments received from the first Technical Review.
1.2	27/01/2020	Gencer Erdogan (SINTEF)	Updated method for the development of curriculum, courses, and training material in Section 2, based on feedback from the consortium members.
1.3	29/01/2020	Gencer Erdogan (SINTEF)	Included a new Section 3 "Target-user cybersecurity roles and skills selected for CYBERWISER.eu".
1.4	30/01/2020	Gencer Erdogan (SINTEF)	Mapped the selected cybersecurity roles to the learning path in Section 4. Included roles and expected skills to be trained in each course described in Section 5.
1.5	04/02/2020	Gencer Erdogan (SINTEF)	Wrote the Executive Summary and the Introduction. Included Section 5.4.
1.6	05/02/2020	Gencer Erdogan (SINTEF)	Updated the glossary of acronyms and wrote the conclusion. Minor corrections in various sections.
1.7	06/02/2020	Dario Varano (UNIPI), Gianluca Dini (UNIPI)	Updated section 5.4.3 about how a course can be applied to classroom lectures.
1.8	06/02/2020	Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT)	Input to Sections 2 and 5.4.1. Included a new Section 6.4.
1.9	10/02/2020	Gencer Erdogan (SINTEF)	Update of Section 4 with additional input to the learning path. Input to Section 5.4. Minor corrections.
1.10	10/02/2020	Ioannis Kechaoglou (RHEA)	CIISec framework integration review and comment in Sections 3 and 5.
1.11	11/02/2020	Niccolò Zazzeri (TRUST-IT)	Included a new Section 6.5. Updated Section 6.4.
1.12	12/02/2020	Valerio Vitangeli (FFSS), Gencer Erdogan (SINTEF)	Updated the report based on feedback from the internal review carried out by FFSS.
1.13	14/02/2020	Rodrigo Diaz (ATOS), Gencer Erdogan (SINTEF)	Updated the report based on feedback from the internal review carried out by ATOS.
2.0	14/02/2020	Maria Teresa Garcia Gonzalez (ATOS)	Quality Check performed. Deliverable ready for submission.

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
1 Introduction	Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Åsmund Hugo (SINTEF), Ketil Stølen (SINTEF)
2 Method for the development of curriculum, courses, and training material	Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Åsmund Hugo (SINTEF), Dario Varano (UNIPI)
3 Target-user cybersecurity roles and skills selected for CYBERWISER.eu	Gencer Erdogan (SINTEF), Åsmund Hugo (SINTEF), Dario Varano (UNIPI), Gianluca Dini (UNIPI), Niccolò Zazzeri (TRUST-IT), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), José Ferreira Lourenço (EDP)
4 The overall learning path of CYBERWISER.eu	Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Åsmund Hugo (SINTEF), Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Liliana Ribeiro (EDP)
5 Courses for the primary and basic offering levels	Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Åsmund Hugo (SINTEF), Ketil Stølen (SINTEF), Dario Varano (UNIPI), Gianluca Dini (UNIPI), Gigliola Vaglini (UNIPI), Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT), Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Liliana Ribeiro (EDP)
6 Accessing and editing training material in the platform	Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT), Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Åsmund Hugo (SINTEF)
7 Conclusions	Gencer Erdogan (SINTEF), Aida Omerovic (SINTEF), Ketil Stølen (SINTEF), Åsmund Hugo (SINTEF), Niccolò Zazzeri (TRUST-IT), Cristina Mancarella (TRUST-IT)

Keywords

Training material, curriculum, courses, risk management, cybersecurity, awareness, security roles, security skills, risk-centric learning path, cyber range.

Disclaimer

Table of Contents

1. INTRODUCTION 10
1.1 Purpose 10
1.2 Structure of the document 11
1.3 Relation to other work in the project 11
1.4 Glossary of Acronyms 12
2. METHOD FOR THE DEVELOPMENT OF CURRICULUM, COURSES, AND TRAINING MATERIAL 13
2.1 Course and module templates 14
2.1.1 Course template 15
2.1.2 Module template 16
3. TARGET-USER CYBERSECURITY ROLES AND SKILLS SELECTED FOR CYBERWISER.EU 17
3.1 CIISec Skills Framework 17
3.2 CIISec Roles Framework 21
3.3 Roles and skills selected for CYBERWISER.eu 22
3.3.1 Overview of selected skills 22
3.3.2 Description of skill Threat Intelligence, Assessment and Threat Modelling 22
3.3.3 Description of skill Risk Assessment 23
3.3.4 Description of skill Information Risk Management 24
3.3.5 Overview of selected roles 24
3.3.6 Description of role Head of Information/Cyber Security 25
3.3.7 Description of role Information Security Risk Manager 25
3.3.8 Description of role Information Security Risk Officer 26
3.3.9 Description of role Threat Analyst 26
3.3.10 Description of role Vulnerability Assessment Analyst 27
4. THE OVERALL LEARNING PATH OF CYBERWISER.EU 29
4.1 Cyber-risk centric learning path 29
4.2 Cybersecurity and risk awareness 31
4.3 Cyber-risk analysis 35
4.3.1 Context establishment 36
4.3.2 Cyber-risk assessment 38
4.3.3 Cyber-risk treatment and cost/benefit analysis 39
4.4 Relating the learning path to the offering levels in CYBERWISER.eu 40
5. COURSES FOR THE PRIMER AND BASIC OFFERING LEVELS 42
5.1 Overview of the courses 42
5.2 Courses for the primer offering level 43
5.2.1 Introduction to cyber-risk analysis and cybersecurity 43
5.2.2 Awareness of five common cybersecurity risks 45
5.2.3 Introduction to cyber-risk assessment 50
5.3 Courses for the basic offering level 51
5.3.1 Describe target of analysis, level 1 51
5.3.2 Identify and describe security assets, level 1 52
5.3.3 Identify and describe threat profiles and high-level risks, level 1 53
5.3.4 Identify risks, level 1 54
5.3.5 Awareness of Password Weakness with hands-on training 56
5.4 The usage environment of the courses 57
5.4.1 Applying the courses for self-study 57
5.4.2 Applying the courses for classroom lectures 57

6. ACCESSING AND EDITING TRAINING MATERIAL IN THE PLATFORM 58
6.1 Logging into the CYBERWISER.eu Platform 58
6.2 Accessing the courses – From a student perspective 58
6.2.1 My Training Path section 60
6.3 Editing the courses – From a teacher perspective 62
6.4 Interactive and engagement features 64
6.5 Developing soft skills using the CYBERWISER.eu Platform 67
7. CONCLUSIONS 69

List of figures

Figure 1. Method for systematically developing the curriculum, courses and training material 13
Figure 2. SANS Framework 14
Figure 3. CYBERWISER.eu Framework 15
Figure 4. CIISec Skills Framework skill levels (adoped from CIISec [24]) 19
Figure 5. The overall cyber-risk centric learning path and security roles mapped to the learning path 30
Figure 6. Selection process of the five common cybersecurity risks for awareness training 32
Figure 7. Relationship between the learning path and the risk analysis process 35
Figure 8. The steps related to context establishment 37
Figure 9. The steps related to cyber-risk assessment 39
Figure 10. The steps related to cyber-risk treatment 40
Figure 11. Relating the learning path to the offering levels 41
Figure 12. Login/Register in the Home Page to be able to access the Workspace 58
Figure 13. Click on “Cross Learning facilities” to enter the Workspace after the Login/Registration 58
Figure 14. Click on the highlighted buttons to enter the “Group Area” within the Workspace 59
Figure 15. Sections of the “Group Area” within the Workspace 60
Figure 16. Inside the “My Training Path”, click on an Offering Level to access it. 60
Figure 17. Sections of the course level “PRIMER” 61
Figure 18. Modules of the first section of the PRIMER course 61
Figure 19. Training Path of the first module 62
Figure 20. Administrative menu example 63
Figure 21. Activities to be selected by a teacher 63
Figure 22. Example of students monitoring 64
Figure 23. Video example 64
Figure 24. Multiple choice answers 65
Figure 25. True/false answers 65
Figure 26. Embedded answers 65
Figure 27. Matching 66
Figure 28. Automatic certification 66

List of tables

Table 1. Table of course names 9
Table 2. Table of slide set numbers to document names 11
Table 3. Table of acronyms 12
Table 4. Course template 16

Table 5. Module template 16
Table 6. CIISec skills 19
Table 7. CIISec skill levels described 21
Table 8. Description of skill Threat Intelligence, Assessment and Threat Modelling 23
Table 9. Description of skill Risk Assessment 23
Table 10. Description of skill Information Risk Management 24
Table 11. Primary skill and skill level for the role Head of Information/Cyber Security 25
Table 12. Primary skill and skill level for the role Information Security Risk Manager 26
Table 13. Primary skill and skill level for the role Information Security Risk Officer 26
Table 14. Primary skill and skill level for the role Threat Analyst 27
Table 15. Primary skill and skill level for the role Vulnerability Assessment Analyst 28
Table 16. Overview of five common cybersecurity risks selected for the awareness training 34
Table 17. Overview of the courses for the Primer and Basic offering levels 42
Table 18. Course: Introduction to cyber-risk analysis and cybersecurity (P-01) 44
Table 19. Module: Conceptual clarification of cybersecurity and risk analysis (P-01-M-01) 44
Table 20. Module: Overview of the overall risk analysis process (P-01-M-02) 45
Table 21. Course: Awareness of Phishing (P-02) 46
Table 22. Course: Awareness of Password Weaknesses (P-03) 47
Table 23. Course: Awareness of Ransomware (P-04) 48
Table 24. Course: Awareness of Data Leakage (P-05) 49
Table 25. Course: Awareness of Insider Threat (P-06) 50
Table 26. Course: Introduction to cyber-risk assessment (P-07) 50
Table 27. Course: Describe target of analysis, level 1 (B-01) 51
Table 28. Module: Describe scope and focus of analysis, what is included and what is excluded? (B-01-M-01) 52
Table 29. Module: Model the target of analysis (B-01-M-02) 52
Table 30. Course: Identify and describe security assets, level 1 (B-02) 53
Table 31. Course: Identify and describe threat profiles and high-level risks, level 1 (B-03) 54
Table 32. Module: Document high-level risks, including threats, incidents, and assets using high-level risk table (B-03-M-01) 54
Table 33. Course: Identify risks, level 1 (B-04) 55
Table 34. Module: Introduction to CORAS (B-04-M-01) 55
Table 35. Module: Identify risks using the CORAS risk modelling language (B-04-M-02) 55
Table 36. Course: Awareness of Password Weaknesses with hands-on training (B-05) 56
Table 37. Description of soft skill Communication and Knowledge Sharing 67

Executive Summary

This deliverable presents the initial version of the training material provided in CYBERWISER.eu. This deliverable describes our systematic approach to develop the curriculum, courses including course templates, as well as the training material. The method consists of four main steps:

- Step 1: Identify target-user roles and skills to be trained via CYBERWISER.eu
- Step 2: Map the roles and their expected skills to the learning path of CYBERWISER.eu
- Step 3: Describe courses using predefined templates
- Step 4: Develop training material for the courses

In Step 1, we identify the target-user cybersecurity roles relevant to CYBERWISER.eu and describe the skills required by the roles as well as the expected skill level for each skill. In Step 2, we describe the learning path of CYBERWISER.eu and map the cybersecurity roles identified in Step 1 to the learning path. In Step 3, we describe courses offered by CYBERWISER.eu in line with the learning path and considering the roles and skills addressed in the learning path. The courses are described using predefined course templates. Finally, having identified and described a set of courses in Step 3, next we develop training material for the courses in Step 4.

The learning path consists of four main parts:

- Cybersecurity and risk awareness
- Context establishment
- Cyber-risk assessment
- Cyber-risk treatment and cost/benefit analysis

The learning path is carefully constructed to be in line with ISO 27001 [9] and ISO 27005 [10], which are security standards known globally and used both in industry and academia.

Using the above method this deliverable provides initial versions of 12 courses for the Primer and Basic offering levels. Table 1 gives an overview of these courses. Each course has training material in terms of PowerPoint presentations, supporting literature including references to external sources (for further reading), audio support, and questionnaires. The courses are primarily developed for self-study and collaborative training via training exercises provided in the cyber range. However, the training material of the courses act also as a basis for lecturers to prepare traditional classroom courses.

Course ID	Course name	Offering level	Overall learning path
P-01	Introduction to cyber-risk analysis and cybersecurity	Primer	Cybersecurity and cyber-risk awareness
P-02	Awareness of Phishing	Primer	Cybersecurity and cyber-risk awareness
P-03	Awareness of Password Weaknesses	Primer	Cybersecurity and cyber-risk awareness
P-04	Awareness of Ransomware	Primer	Cybersecurity and cyber-risk awareness
P-05	Awareness of Data Leakage	Primer	Cybersecurity and cyber-risk awareness
P-06	Awareness of Insider Threat	Primer	Cybersecurity and cyber-risk awareness
P-07	Introduction to cyber-risk assessment	Primer	Cybersecurity and cyber-risk awareness
B-01	Describe target of analysis, level 1	Basic	Context establishment
B-02	Identify and describe security assets, level 1	Basic	Context establishment

Course ID	Course name	Offering level	Overall learning path
B-03	Identify and describe threat profiles and high-level risks, level 1	Basic	Context establishment
B-04	Identify risks, level 1	Basic	Cyber-risk identification
B-05	Awareness of Password Weakness with hands-on training	Basic	Cybersecurity and cyber-risk awareness

Table 1. Table of course names

Finally, the deliverable outlines how the training material should be accessed and edited within the CYBERWISER.eu Platform.

The contents of this deliverable, in particular the course descriptions, will act as input to the rest of work package 4, particularly Task 4.2 (cyber-training scenarios and scenario development method), which will develop scenarios to support the training of the security roles and skills considered. The deliverable is also related to WP5 in the sense that we have mainly considered the requests of the pilots when we shaped the awareness courses. Thus, the awareness courses are shaped to accommodate the needs of the pilots. The deliverable is also related to the work carried out in WP6 in terms of the various offering levels. That is, the courses have been shaped with respect to the learning path, but also considering the technical aspects available in each offering level of CYBERWISER.eu. Finally, the deliverable is related to WP2 in the sense that the training material developed in Task 4.1 will help the shaping of relevant risk-model templates (patterns) in Task 2.3 (model adaptation and development).

1. Introduction

This section describes the purpose of this deliverable, provides the structure of the document, and relates the work reported in this deliverable to other work in the project.

1.1 Purpose

The purpose of this deliverable is to document the initial version of the training material to be provided in CYBERWISER.eu. This includes identifying target-user roles and skills to be trained via CYBERWISER.eu, describing the learning path of CYBERWISER.eu and mapping the roles and skills to the learning path, describing relevant courses using predefined course templates, and developing training material in terms of PowerPoint slides, supporting literature including references to external sources, audio support for the PowerPoint slides, and questionnaires testing the participants. We carry out these activities systematically following a four-step method described in Section 2. The learning material is made available to participants via the cross-learning facilities of CYBERWISER.eu.

With respect to the learning path, CYBERWISER.eu facilitates a risk-centric approach. By risk-centric, we mean that cyber-risk related activities are used as a mean to train the participants within cybersecurity. Moreover, the learning path includes also an awareness part with the aim of raising awareness on cybersecurity as well as introduce more complex concepts that will be further considered in the advanced offering levels of CYBERWISER.eu.

In relation to the offering levels, this deliverable provides courses and supporting training material for the first two (out of in total four) offering levels of CYBERWISER.eu, namely the Primer and Basic offering levels. Note that offering levels represent different delivery modes of the CYBERWISER.eu platform containing different level of capabilities as documented in Deliverable D6.1 [22]. Primer is the first offering level and will be accessible free of charge from the CYBERWISER.eu website. Primer will offer basic functionalities with the aim of raising awareness and introduce cybersecurity and cyber-risk assessment and related concepts. The Basic offering level is targeting users that are familiar with cybersecurity and are willing to test and improve their skills on a more sophisticated level. The reader is referred to D6.1 [22] for further information about the various offering levels of CYBERWISER.eu. The courses and supporting training material for the last two offering levels (Intermediate and Advanced) will be provided in D4.2 (training material, final version).

This deliverable describes seven courses for the Primer level and four courses for the Basic level. Basically, five of the seven courses for the Primer level focus on awareness on five common cybersecurity risks, while the remaining two focus on an introduction to cyber-risk analysis, cyber-risk assessment and cybersecurity. The courses for the Basic level focus on various aspects on context establishment and cybersecurity-risk identification. The training material are shaped according to the learning goals and objectives of the courses.

The courses are developed in the form of fourteen separate slide sets with supporting literature including references to external sources, audio support for the slides and questionnaires testing the participants. The training materials are made available via, and integrated in, the cross-learning facilities. The following documents, all of which are accompanied with this deliverable, represent one slide set each:

Accompanying slide set number	Document name
1	P-05 Awareness of Data Leakage
2	P-02 Awareness of Phishing
3	P-04 Ransomware Awareness
4	B-04-M-01 ExampleDrivenIntroductionToCORAS
5	B-04-M-02 Identify risks using the CORAS risk modelling language with respect to simulated scenarios

Accompanying slide set number	Document name
6	P-01-M-01 ConceptualClarificationOfCyberriskAssessmentAndCybersecurity
7	P-01-M-02 OverviewOfTheOverallCyberriskAssessmentProcess
8	P-06 – Awareness of Insider Threats
9	P-03 – Awareness of Password Weaknesses
10	B-01-M-01 Describe scope and focus of analysis, what is included and what is excluded?
11	B-01-M-02 Model the target of analysis
12	P-07 – Introduction to cyber-risk assessment
13	B-02 Identify and describe security assets, level 1
14	B-03 Identify and describe threat profiles and high-level risks, level 1

Table 2. Table of slide set numbers to document names

1.2 Structure of the document

Section 2 describes the steps we carried out to systematically develop the curriculum, courses, and training material. Section 3 describes the target-user cybersecurity roles and skills selected for CYBERWISER.eu. Section 4 explains in detail the overall cyber-risk centric learning path of CYBERWISER.eu, including cybersecurity and risk awareness, context establishment, cyber-risk assessment, and cyber-risk treatment and cost/benefit analysis. In addition, Section 4 relates the security roles and skills to the learning path, as well as the learning path to the offering levels in CYBERWISER.eu. Section 5 provides a description of all the courses that will be provided in the Primer and Basic offering levels. Section 6 provides a high-level explanation of how the courses and training material may be accessed and edited in the CYBERWISER.eu platform, the interactive and engagement features, as well as how the CYBERWISER.eu platform may contribute in developing soft skills. Finally, in Section 7, we conclude the deliverable by highlighting the main contributions of the deliverable and the next steps to be taken.

1.3 Relation to other work in the project

The contents of this deliverable, in particular the course descriptions, will act as input to rest of work package 4, particularly Task 4.2 (cyber-training scenarios and scenario development method), which will develop scenarios to support the training.

The deliverable is also related to WP5 in the sense that we have mainly considered the requests of the pilots when we shaped the awareness courses. Thus, the awareness courses are shaped to accommodate the needs of the pilots.

As indicated in the above sub-sections, the deliverable is also related to the work carried out in WP6 in terms of the various offering levels. That is, the courses have been shaped with respect to the learning path considering the relevant roles and skills selected, but also considering the technical aspects available in each offering level of CYBERWISER.eu.

Finally, the deliverable is related to WP2 in the sense that the training material developed in Task 4.1 will help the shaping of relevant risk-model templates (patterns) in Task 2.3 (model adaptation and development).

1.4 Glossary of Acronyms

Acronym	Description
CIISec	Chartered Institute of Information Security
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Professionals
CORAS	A Model-Driven Method for Conducting Security Risk Analysis
CREST	CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market.
ECSO	European Cybersecurity Organization
ENISA	European Union Agency for Cybersecurity
GDPR	The General Data Protection Regulation 2016/679
GIAC	Global Information Assurance Certification
ISO	International Organization for Standardization
MITRE	The MITRE Corporation
OWASP	The Open Web Application Security Project
R	R is a free software environment for statistical computing and graphics.
SANS	The SANS Institute is a private U.S. for-profit company founded in 1989 that specializes in information security, cybersecurity training and selling certificates.
SCORM	Sharable Content Object Reference Model. (SCORM defines a specific way of constructing Learning Management Systems (LMSs) and training content so that they work well with other SCORM conformant systems).
UML	Unified Modelling Language
WISER	Wide-Impact cyber SEcurity Risk framework
WP	Work Package

Table 3. Table of acronyms

2. Method for the development of curriculum, courses, and training material

This section describes the steps we carried out to systematically develop the curriculum, courses, and training material. As illustrated in Figure 1, our method consists of four main steps. In Step 1, we identify the target-user cybersecurity roles relevant to CYBERWISER.eu and describe the skills required by the roles as well as the expected level of advancement for each skill. The identified roles and skills are described in detail in Section 3.

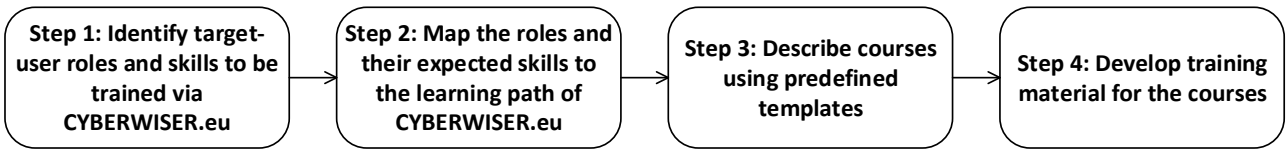


Figure 1. Method for systematically developing the curriculum, courses and training material

In Step 2, we describe the learning path of CYBERWISER.eu and map the cybersecurity roles identified in Step 1 to the learning path. The learning path of CYBERWISER.eu is mainly defined to support the expected outcomes of the project. Some of the main outcomes of CYBERWISER.eu are the following:

- Training materials for creation of cyber-risk models for cyber-risk assessment, as well as training materials for the identification and suggestion of countermeasures for the identified cyber-risks.
- Simulation of a variety of attacks and countermeasures concerning the digital assets characterized in the scenario object of the training.
- A set of innovative and highly descriptive economic risk models for cyber-risk assessment and countermeasure suggestion, to boost user training and performance evaluation.
- Pedagogic presentation of the cyber-risk assessment method inspired by the WISER project supported by extensive examples and guidelines.

Thus, the CYBERWISER.eu approach consists of cyber-risk assessment activities including the establishment and understanding of the target of analysis, as well as the consideration of cyber-risk treatments (countermeasures). This means that CYBERWISER.eu facilitates a cyber-risk centric approach and we will therefore structure a cyber-risk centric learning path. By cyber-risk centric learning path, we mean that cyber-risk related activities are used as means to train the participants within cybersecurity. The learning path is described in detail in Section 4.

In Step 3, we describe courses offered by CYBERWISER.eu in line with the learning path and considering the roles and skills addressed in the learning path. The courses are described using course templates that are presented in Section 2.1. The courses are defined first and foremost to be in line with the learning path of CYBERWISER.eu including relevant roles and skills. However, we also relate the learning path to the four offering levels (Primer, Basic, Intermediate and Advanced) of CYBERWISER.eu as well as the technical capabilities available in each offering level. In addition, we also considered for each course the difficulty level and the estimated time needed as shown in the templates in Section 2.1. In this deliverable we have defined courses for the Primer and Basic offering level of CYBERWISER.eu. Deliverable 4.4 (training material, final version) will contain courses for the remaining two offering levels, namely Intermediate and Advanced. The courses for the Primer and Basic offering levels are documented in Section 5.

Finally, having identified and described a set of courses in Step 3, next we develop training material for the courses in Step 4. The training material was developed with respect to the learning goals and learning objectives defined for each course considering also the cybersecurity roles and skills. This procedure is recommended by standard course design guidelines, such as the Bloom's Taxonomy [15], [16], which is also the framework we used to define learning goals and objectives. In this deliverable, we provide the learning material for the courses at Primer and Basic offering levels in terms of PowerPoint presentations with

supporting explanatory text. A series of additional training material will be added taking into account the capabilities of Moodle. These can include, video tutorials on how to deploy a scenario, video tutorials on how to perform a simple exercise in the cyber range, webinars on security topics, use of game-based quizzes. Some examples of these features are reported in Section 6.4. The output of Step 4 is thus a set of training material for the courses offered in CYBERWISER.eu to educate and train the target-user cybersecurity roles.

2.1 Course and module templates

The development of the course template started with an intensive research of the existing institutes providing Cybersecurity courses. The identified institutes were: SANS, InfoSec, Offensive-Security and Kaspersky. The selection of one of the approaches provided by these institutes was done considering the following features: 1) popularity, i.e. how much the institute is spread and well-known; 2) whether they give a certification; and 3) range of topics covered. Based on this activity, the most appropriate framework to organize courses in CYBERWISER.eu is the approach provided by the SANS institute [17]. SANS is well-known for serving many military forces, along with more than 165.000 security professionals in more than 90 cities around the world. It provides certification in many fields like Cyber Defence, Penetration Testing, Management, Legal, Incident Response, Forensic and many others. The SANS institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted and by far largest source for information security training and security certification in the world. The starting point for the development of the course template was the analysis of the framework employed by SANS for organizing courses. The SANS framework to organize a curriculum is shown in Figure 2.

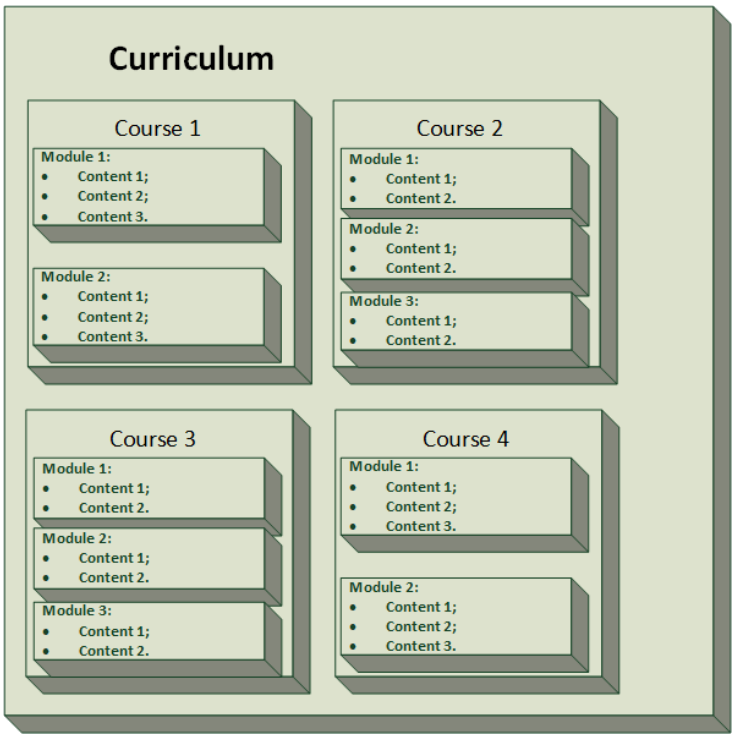


Figure 2. SANS Framework

By using the structure shown in Figure 2 as basis, we chose in CYBERWISER.eu to structure the courses in two main layers, namely *course* and *module*. A course contains a hierarchy of modules. A module may be a part of one or more courses. The idea behind this separation is to shape more complex courses using simpler modules, each of them bringing smaller contributions. The latter will facilitate trainees to increase their skills by progressing step by step in the learning path. The following sections present the templates for courses and modules. The course organization for the CYBERWISER.eu project is shown in Figure 3.

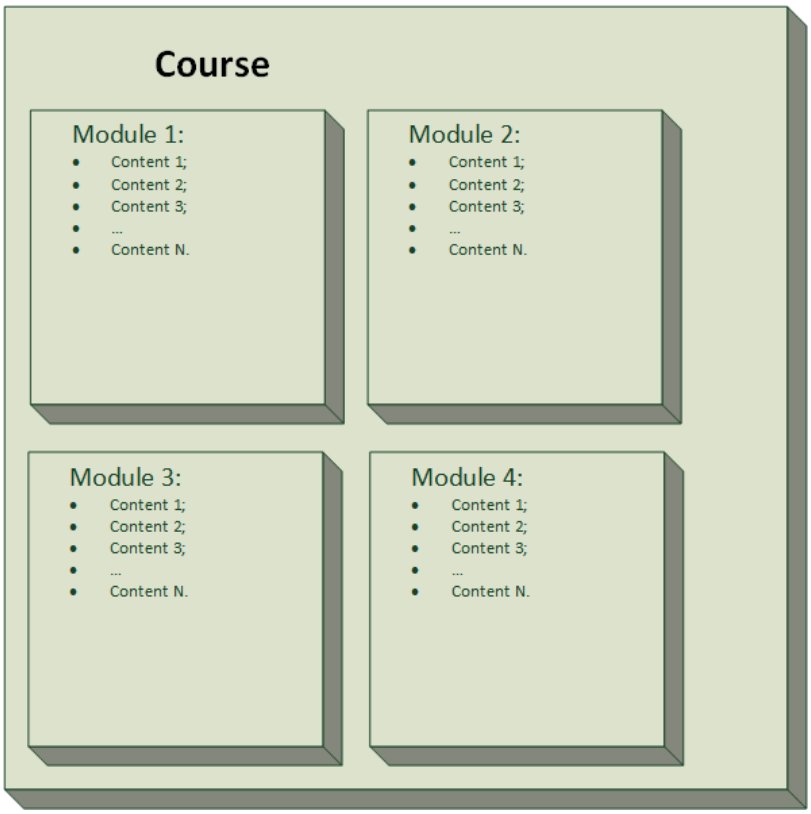


Figure 3. CYBERWISER.eu Framework

2.1.1 Course template

The course templates used to describe a course in CYBERWISER.eu is presented in Table 4. The description for each of the course feature presented in the template is embedded in the table. To complete a course, trainees need to complete all the modules related to it.

Course ID	Unique ID of the course
Name	Name of the course.
Cybersecurity role	The cybersecurity role relevant to the course. These roles are based on the roles described by the CIISec Roles Framework [23]. The roles are described in detail in Section 3.
Skill and expected skill level to be trained	The skill and the expected level of advancement of the skill for the abovementioned role. These skills are based on the skills described by the CIISec Skills Framework [24]. The skills are described in detail in Section 3.
Offering Level	The name of the CYBERWISER.eu offering level in which the course is provided. Possible options are {Primer, Basic, Intermediate, Advanced}.
Difficulty	Difficulty level of the course. Possible options are {Easy, Medium, Hard, Challenging}
Course Duration	Time needed to carry out the course in minutes.
Learning Goals	Learning goals of the course, written using the Bloom's Taxonomy [15], [16] indicating the broad learning outcome trainees will acquire at the end of the course.
Learning Objectives	Measurable objectives written in the Bloom Taxonomy [15], [16].

Course ID	Unique ID of the course
Prerequisites	List of prerequisites for the trainee attending the course, they may be degree level or skills. (e.g. bachelor's degree or fulfil the following: Good knowledge of …)
Module list	List here all the modules related to this course. The modules should reveal the list of argument composing the course learning path: • Module 1 • Module 2 • … • Module N

Table 4. Course template

2.1.2 Module template

The structure for each single module is presented in Table 5. Modules are split in several contents. The latter can help trainees to have a more complete view of the purpose of a single module.

Module ID	Unique ID of the module
Name	Name of the module
Learning Objectives	Specify what the trainee will learn after completing the module dividing it into multiple, specific and measurable objectives. These learning objectives can be considered as sub tasks of the course learning objectives.
Prerequisites	List of the module(s) that needs to be attended before this module. If no other modules are needed before this one, fill this field with "None"
Content list	List here all the contents related to this module. Contents will show a more granular division in the module's topic: • Content 1 • Content 2 • … • Content N

Table 5. Module template

3. Target-user cybersecurity roles and skills selected for CYBERWISER.eu

As explained in Section 2, the first step of our method to systematically develop the curriculum, courses and training material for CYBERWISER.eu is to identify the target-user cybersecurity roles and skills to be trained via CYBERWISER.eu. There exist several cybersecurity communities that may provide guidelines to help identify and select cybersecurity roles and skills, such as MITRE [25], OWASP [26], CREST [27], CIISec [23], [24], SANS [17] and CISSP [28] to mention a few. For the purpose of CYBERWISER.eu, we chose to use the CIISec Roles Framework and the CIISec Skills Framework. The rationales for this selection are:

- The CIISec Roles Framework and the CIISec Skills Framework are considering roles and skills that are well aligned with the risk-centric approach of CYBERWISER.eu. For example, the role Information Security Risk Officer and the associated skills Risk Assessment and Information Risk Management.
- Each role defined in the CIISec Roles Framework are associated to certain skills and expected skill level, which aligns well with the courses provided by CYBERWISER.eu in terms of course difficulty (level of advancement).
- The CIISec Skills Framework describes six skill levels {Knowledge (level 1), Knowledge and Understanding (level 2), Apply (level 3), Enable (level 4), Advice (level 5), Initiate, Enable and Ensure (level 6)}. These six levels align well with the six levels of advancement in learning skills provided by the Bloom's taxonomy [15], [16] {Remembering (level 1), Understanding (level 2), Applying (level 3), Analysing (level 4), Evaluating (level 5), Creating (level 6)}. As best practice, we use the action verbs provided by Bloom's taxonomy to help describe the learning goals and objectives of the courses in CYBERWISER.eu.
- The cyber-risk related roles and skills described in the CIISec framework support the risk-centric learning path of CYBERWISER.eu, which is in line with ISO 27005 [10] as described in Section 4.

In addition, the CIISec Roles and Skills frameworks are "developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders" [24] and are therefore representative of the current landscape of cybersecurity roles and skills.

In the following sections, we first describe the CIISec Skills Framework, CIISec Roles Framework, and finally, the roles and skills selected from these frameworks for CYBERWISER.eu.

3.1 CIISec Skills Framework

According to the Chartered Institute of Information Security (CIISec), the CIISec Skills Framework describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. The framework may be used as a basis to assess the knowledge of certain security roles as well as to define skills expected of the security roles in practice.

The largest part of the framework is dedicated to describing a wide range of technical and domain specific skills and what is required for each skill-advancement level. The technical and domain specific skills may be grouped into the following topics:

- Information Security Governance and Management
- Threat Assessment and Information Risk Management
- Implementing Secure Systems
- Assurance: Audit, Compliance and Testing
- Operational Security Management
- Incident Management, Investigation and Digital Forensics
- Data Protection, Privacy and Identity Management
- Business Resilience
- Information Security Research

However, the framework also points out the multi-disciplinary nature of security professionals and therefore includes a set of interpersonal and collegial skills needed to work effectively (Management, Leadership, Business and Communications) as well as skills required to support personal career development (Contributions to the Information Security Profession and Professional Development). Table 6 provides an overview of all skills addressed by the CIISec Skills Framework according to the abovementioned categories as provide by the framework [24].

Skill group	Skill
Information Security Governance and Management	A1 – Governance
	A2 – Policy and Standards
	A3 – Information Security Strategy
	A4 – Innovation and Business Improvement
	A5 – Behavioural Change
	A6 – Legal & Regulatory Environment and Compliance
	A7 – Third Party Management
Threat Assessment and Information Risk Management	B1 – Threat Intelligence, Assessment and Threat Modelling
	B2 – Risk Assessment
	B3 – Information Risk Management
Implementing Secure Systems	C1 – Enterprise Security Architecture
	C2 – Technical Security Architecture
	C3 – Secure Development
Assurance: Audit, Compliance and Testing	D1 – Internal and Statutory Audit
	D2 – Compliance Monitoring and Controls Testing
	D3 – Security Evaluation and Functionality Testing
	D4 – Penetration Testing and conducting Simulated Attack Exercises
Operational Security Management	E1 – Secure Operations Management
	E2 – Secure Operations and Service Delivery
Incident Management, Investigation and Digital Forensics	F1 – Intrusion Detection and Analysis
	F2 – Incident Management, Incident Investigation and Response
	F3 – Forensics
Data Protection, Privacy and Identity Management	G1 – Data Protection
	G2 – Privacy
	G3 – Identity and Access Management (IAM/IdM)
Business Resilience	H1 – Business Continuity and Disaster Recovery Planning
	H2 – Business Continuity and Disaster Recovery Management
	H3 – Cyber Resilience
Information Security Research	I1 – Research
	I2 – Applied Research
	J1 – Management, Leadership and Influence
	J2 – Business Skills

Skill group	Skill
Management, Leadership, Business and Communications	J3 – Communication and Knowledge Sharing
Contributions to the Information Security Profession and Professional Development	K1 – Contributions to the Community
	K2 – Contributions to the IS Profession
	K3 – Professional Development

Table 6. CIISec skills

As mentioned above, the CIISec Skills Framework also provides a scale to indicate skill levels for each skill listed in Table 6. Figure 4 illustrates the six skill levels provided by the framework.

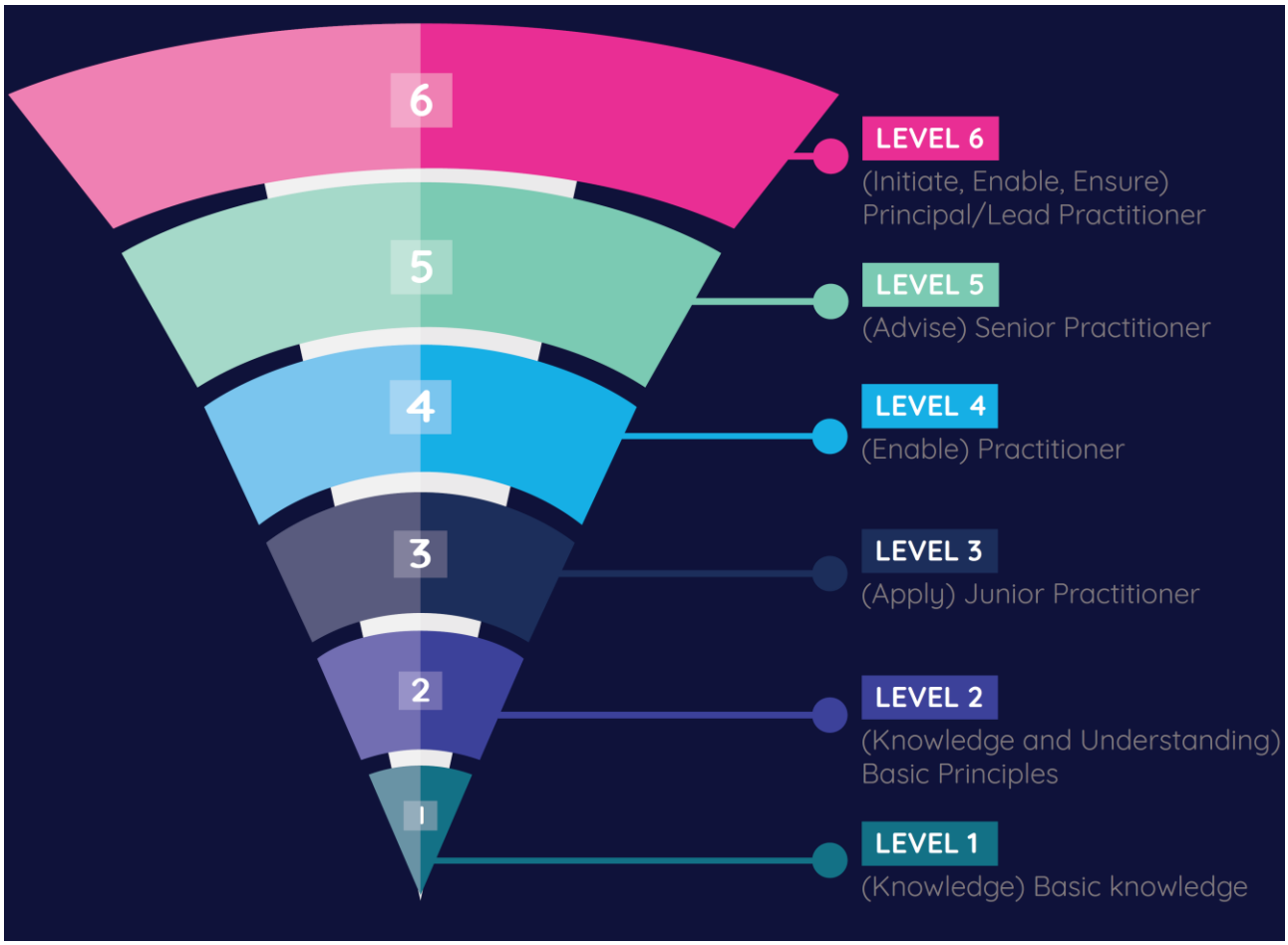


Figure 4. CIISec Skills Framework skill levels (adoped from CIISec [24])

Table 7 described each skill level as given by the framework in terms of required knowledge and practical experience. These skill levels are used in the course descriptions of CYBERWISER.eu to reflect the skill level to be trained in the course. As CYBERWISER.eu mainly aims to educate and train people that are either new to the field or have certain experience, most of the courses offered by CYBERWISER.eu will target skill levels 1 to 4. However, courses that target skill levels 5-6 may also be later added. For example, courses aimed at Trainers to create new courses and exercises. Thus, in this respect, CYBERWISER.eu is flexible and may include courses both for beginners but also for advanced and experienced people.

Skill level	Knowledge	Practice
Level 1: (Knowledge) Basic knowledge of principles/follow good user practice.	Has acquired and can demonstrate basic knowledge associated with the skill, e.g. through training or self-tuition.	
Level 2: (Knowledge and Understanding) Knowledge and Understanding of basic principles. Understands the skill and its application.	Has acquired and can demonstrate the basic knowledge associated with the skill, for example has attended a training course or completed an academic module in the skill. Understands how the skill should be applied.	Can explain the principles of the skill and how it should be applied. This might include experience of applying the skill to basic tasks in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises in using the skill, and/or passing a test or examination. Should be aware of recent developments in the skill.
Level 3: (Apply) Junior Practitioner. Understands the skill and applies it to basic tasks with some supervision.	Has acquired a good understanding of the knowledge associated with the skill and understands how the skill should be applied.	Has experience of applying the skill to a variety of basic tasks. Can work as an effective member of a team. Contributes ideas in the application of the skill. Demonstrates awareness of recent developments in the skill. Has experience of training potential and actual IS practitioners in the basics of the skill. Demonstrates awareness of recent developments in the skill.
Level 4: (Enable) Practitioner. Understands the skill and applies it to basic tasks with minimal supervision and to complex tasks with some supervision. Normally operates as a member of a team in a project/programme or system environment.	Has acquired a deep understanding of the knowledge associated with the skill. Understands how the skill should be applied.	Has experience of applying the skill to a variety of tasks, including some complex tasks under supervision. Contributes ideas in the application of the skill. Demonstrates awareness of recent developments in the skill. Contributes ideas for technical development and new areas for application of the skill. Has experience of training IS professionals in the skill above an introductory level. Demonstrates awareness of recent developments in the skill. Contributes ideas for technical development and new areas for application of the skill.
Level 5: (Advise) Senior Practitioner. Understands the skill and applies it to complex tasks with no supervision. Leads teams in a project/programme or system environment. Operates at a corporate level.	Has acquired a deep understanding of the knowledge associated with the skill. Understands how the skill should be applied across a number of projects in different client environments and/or within a large corporate organisation.	Has experience of applying the skill to a variety of complex tasks. Demonstrates significant personal responsibility or autonomy, with little need for escalation. Contributes ideas in the application of the skill. Demonstrates awareness of recent developments in the skill. Contributes ideas for technical development and new areas for application of the skill and contributes to public discussion debate on the skill. Has effective leadership and management skills. Has experience of training Information Security professionals in the skill at an advanced level or as a university lecturer. Demonstrates awareness of recent developments in the skill. Contributes ideas for technical development and new areas for application of the skill.

Skill level	Knowledge	Practice
Level 6: (Initiate, Enable, Ensure) Principal/Lead Practitioner. An authority who leads implementation of the skill. Is an acknowledged expert by peers in the skill.	As for level 5.	Has oversight responsibility for overall application of the skill across a range of customers or within a large corporate organisation, often reporting at Board level. Recognised as a Subject Matter Expert within a large organisation. Has experience of applying the skill in circumstances without precedence. Proposes, conducts, and/or leads innovative work to enhance the skill. Is approached to provide keynote presentations or papers on the skill. Develops and leads programmes of advanced training in the skill. A Professor or Senior Lecturer contributing sessions on the skill at MSc level.

Table 7. CIISec skill levels described

3.2 CIISec Roles Framework

The CIISec Roles Framework by the Chartered Institute of Information Security [23] provides a list of security roles and associates these roles to certain skills and expected skill levels (described in Section 3.1). The framework is mainly intended for organizations when they are looking to recruit into a role. However, in CYBERWISER.eu we use these roles in combination with the skills described in Section 3.1 to systematically identify the target users as well as to shape the curriculum of CYBERWISER.eu.

It is acknowledged by the framework that while the roles described in the framework may correspond to representative security roles currently considered in the industry, there may be variations in terms of what is expected from the roles. Each role will differ according to the organisation, sector and size of the organisation. These variations will therefore impact on the types of skills required. For example, an Information Security Risk Manager may have more specific responsibilities in a large organization, while the same role in a smaller organization may have a wider range of responsibilities. Moreover, the framework points out that there is no exact description of a role because of all the possible variations of an organization and that the suggested list of roles and their descriptions are based on a more general view. In addition to role descriptions, association to skills and skill levels, the framework relates also roles to certain "responsibilities" (Identify, Protect, Detect, Respond, Recover) based on the NIST Framework for Improving Critical Infrastructure Cybersecurity [29]. The following are the roles described by the CIISec Roles Framework:

- Chief Information Security Officer (CISO)
- Head of Cyber/Information Security
- Information Security Risk Manager
- Information Security Risk Officer
- System Security Manager
- ComSec Manager
- Senior Security Architect
- Technical Security Architect
- Pen tester
- Threat Analyst
- Vulnerability analyst

Before describing these roles in detail (as provided by the framework), we first select the skills relevant for CYBERWISER.eu and then describe the roles relevant for CYBERWISER.eu. This process is carried out and documented in Section 3.3.

3.3 Roles and skills selected for CYBERWISER.eu

In the following Sections 3.3.1 – 3.3.4, we describe the skills selected for CYBERWISER.eu, while in Sections 3.3.5 – 3.3.10, we describe the roles selected for CYBERWISER.eu.

3.3.1 Overview of selected skills

As explained in Section 3.1, there is a large variety of security-specific skills identified by the CIISec Skills Framework. It is not the goal of CYBERWISER.eu to cover all skills listed in Section 3.1. The skills that are most relevant for the successful fulfilment of the objectives of CYBERWISER.eu are those that align with the risk-centric approach of CYBERWISER.eu. Taking this into consideration, we select to focus on the skills related to Threat Assessment and Information Risk Management:

- B1 – Threat Intelligence, Assessment and Threat Modelling
- B2 – Risk Assessment
- B3 – Information Risk Management

According to Task T4.3 of the CYBERWISER.eu Grant Agreement [33], "*the strong focus on training in the CYBERWISER.eu project implies that we need a proper baseline for performance evaluation. We therefore need clear criteria for evaluating the real-time response of students during cyber-range exercises, as well as the degree to which risk models and algorithms selected and/or developed by the students reflect the cyber-risk posture of the (simulated) target system and provide support for real-time response. This task will establish such criteria, emphasising aspects such as relevance, coverage, correctness, and response preparedness support.*" The resulting evaluation criteria documented in Deliverable D4.2 (Real-time performance and evaluation criteria) are therefore oriented towards technical skills. The courses developed in Task T4.1 reported in this document (as well as in Deliverable D4.4) have a technical orientation to accommodate these evaluation criteria. Thus, CYBERWISER.eu in general focus mainly on technical skills. The explicit training of soft skills (courses teaching about e.g. communication) is outside the scope of CYBERWISER.eu. However, in order to support a holistic approach to cybersecurity training, we do address the development of soft skills as a result of participating CYBERWISER.eu courses. The relevant soft skills are addressed in context of the cross-learning facilities of CYBERWISER.eu described in Section 6.

In the following, we describe the abovementioned technical skills according to their description in the CIISec Skills Framework [24] for completeness. The reader is referred to the CIISec Skills Framework [24] for further details on the remaining skills listed in Section 3.1.

3.3.2 Description of skill Threat Intelligence, Assessment and Threat Modelling

Table 8 describes the skill Threat Intelligence, Assessment and Threat Modelling as provided by the CIISec Skills Framework [24]. As pointed out by the CIISec Skills Framework, the principles and example skills described in the following table are meant to be used as high level guidelines and not as "blueprint". Not all security roles require detailed experience in all competency areas as this may vary depending on the organisation, sector and size of the organisation.

Skill	Principles	Example Skills
B1 – Threat Intelligence, Assessment and Threat Modelling	Assesses and validates information from several sources on current and potential Cyber and Information Security threats to the business, analysing trends and highlighting Information Security issues relevant to the organisation, including Security Analytics for Big Data. Processes,	**Level 1**: Can describe the principles of threat intelligence, modelling and assessment.
		Level 2: Can explain the principles of threat intelligence, modelling and assessment. This might include experience of applying threat intelligence, modelling and assessment principles in a training or academic environment, for example through participation in syndicate exercises, undertaking practical

Skill	Principles	Example Skills
	collates and exploits data, taking into account its relevance and reliability to develop and maintain "situational awareness". Predicts and prioritises threats to an organisation and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Uses threat intelligence to develop attack trees. Prepares and disseminates intelligence reports providing threat indicators and warnings.	exercises, and/or passing a test or examination.
		Level 3: Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments under supervision. Appropriate and relevant certifications include CREST Practitioner Threat Intelligence Analyst, SANS GIAC Cyber Threat Intelligence.
		Level 4: Undertakes routine threat intelligence/modelling tasks or threat assessments without close supervision. Undertakes complex threat intelligence tasks or threat assessments under supervision. Appropriate and relevant certifications include CREST Registered Threat Intelligence Analyst.
		Level 5: Undertakes complex threat intelligence/modelling tasks or threat assessments without supervision. Manages threat intelligence/assessment teams. Appropriate and relevant certifications include CREST Certified Threat Intelligence Manager.
		Level 6: Leads corporate threat intelligence processes, reporting to the Board.

Table 8. Description of skill Threat Intelligence, Assessment and Threat Modelling

3.3.3 Description of skill Risk Assessment

Table 9 describes the skill Risk Assessment as provided by the CIISec Skills Framework [24]. As pointed out by the CIISec Skills Framework, the principles and example skills described in the following table are meant to be used as high level guidelines and not as "blueprint". Not all security roles require detailed experience in all competency areas as this may vary depending on the organisation, sector and size of the organisation.

Skill	Principles	Example Skills
B2 – Risk Assessment	Identifies and assesses information assets; uses this information and relevant threat assessments, business impacts, business benefits and costs to conduct risk assessments and identify and assess potential vulnerabilities.	**Level 1**: Can describe the concepts and principles of risk assessment.
		Level 2: Can explain the principles of risk assessment. This might include experience of applying risk assessment principles in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination.
		Level 3: Undertakes basic risk assessments with some supervision.
		Level 4: Undertakes complex risk assessments with supervision, either as an individual or a member of a team.
		Level 5: Leads complex risk assessments, interfacing routinely with senior management.
		Level 6: A recognised authority on risk assessment within a major organisation or across a range of clients or within an industry sector.

Table 9. Description of skill Risk Assessment

3.3.4 Description of skill Information Risk Management

Table 10 describes the skill Information Risk Management as provided by the CIISec Skills Framework [24]. As pointed out by the CIISec Skills Framework, the principles and example skills described in the following table are meant to be used as high level guidelines and not as "blueprint". Not all security roles require detailed experience in all competency areas as this may vary depending on the organisation, sector and size of the organisation.

Skill	Principles	Example Skills
B3 – Information Risk Management	Develops Cyber and Information Security risk management strategies and controls, taking into account business needs and risk assessments, and balancing technical, physical, procedural and personnel controls.	**Level 1**: Can describe the concepts and principles of Information Security risk management.
		Level 2: Can explain the principles of information risk management. This might include experience of applying risk management principles in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination.
		Level 3: Develops basic information risk management plans with some supervision.
		Level 4: Develops complex and innovative information risk management plans under supervision.
		Level 5: Develops complex and innovative information risk management plans either as an individual or leading a team.
		Level 6: A recognised authority on Cyber and Information risk management within a major organisation or across a range of clients.

Table 10. Description of skill Information Risk Management

3.3.5 Overview of selected roles

Based on the list of roles in Section 3.2, we select roles appropriate for CYBERWISER.eu. Each of these roles are assigned a set of *primary skills* and *secondary skills* (based on the CIISec Skills Framework described in Section 3.1). To make the selection of roles more focused and appropriate for CYBERWISER.eu, we considered two selection criteria:

- We select roles considering only their primary skills relevant for CYBERWISER.eu.
- We select roles that require skills necessary for the cyber-risk centric learning path of CYBERWISER.eu. That is, roles that require one or more of the skills B1, B2, or B3 described in Section 3.3.2, 3.3.3, and 3.3.4, respectively.

Based on these criteria, we selected the following roles:

- Head of Information/Cyber Security
- Information Security Risk Manager
- Information Security Risk Officer
- Threat Analyst
- Vulnerability Assessment Analyst

In the following sections, we describe each of the above roles as provided by the CIISec Roles Framework [23] followed by a table summarizing the primary skill suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as a suggested level for the skill.

3.3.6 Description of role Head of Information/Cyber Security

The post holder would typically be of senior management level with a high level of responsibility and accountability according to the agreed acceptable levels of risk assigned to that role (including legal and regulatory compliance obligations). This can include the management of several security function/elements. However, in smaller organisations the level and spread of knowledge, skills and experience may widen as fewer separate roles focussing on individual discipline areas may exist. This wider skill set would also be likely to be at a lesser skill level. May be a required regulatory role in some sectors [23].

The primary aim of a Head of Information/Cyber Security would be to enable the business to achieve its objectives in a safe and secure manner within an appropriate and proportionate set of controls, policies and procedures. The level of proportionality would depend on the value to which certain assets are viewed within the organization and their appetite to exploit opportunities with a degree of acceptance of risk whilst being prepared to respond to any adverse consequences [23].

Table 11 summarizes the primary skills for the role Head of Information/Cyber Security suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as suggested levels for the skills. Note that not all primary skills suggested by CIISec are included. The skills not included in the table are outside the scope of CYBERWISER.eu. The reader is referred to the CIISec Roles Framework for details on other skills for this role.

Role name	Primary skill suggested by CIISec (and addressed by CYBERWISER.eu)	Suggested skill level
Head of Information/Cyber Security	B2 - Risk Assessment	Level 4: Undertakes complex risk assessments with supervision, either as an individual or a member of a team.
	B3 - Information Risk Management	Level 5: Develops complex and innovative information risk management plans either as an individual or leading a team.

Table 11. Primary skill and skill level for the role Head of Information/Cyber Security

3.3.7 Description of role Information Security Risk Manager

The post holder would typically be of middle management level with a level of responsibility and accountability according to the agreed acceptable levels of risk assigned to that role (including legal and regulatory compliance obligations). Primarily focused on information security risk assessment and management within the organisation. However, in smaller organisations the level and spread of knowledge, skills and experience may widen as fewer separate roles focussing on individual discipline areas may exist. This wider skill set would also be likely to be at a lesser skill level. May be part a required regulatory role/function in some sectors [23].

Information Security Risk Managers are tasked to ensure that information security risks are identified and assessed, making appropriate recommendations. They would typically provide advice and guidance to stakeholders relating to the process and outcome of risk assessments. They may well support the organization’s information 'risk appetite' through their assessments and advice. They would identify mitigations to information security risk and likely to be involved in monitoring and assessing the effectiveness of such measures [23].

Table 12 summarizes the primary skills for the role Security Risk Manager suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as suggested levels for the skills. Note that not all primary skills suggested by CIISec are included. The skills not included in the table are outside the scope of CYBERWISER.eu. The reader is referred to the CIISec Roles Framework for details on other skills for this role.

Role name	Primary skill suggested by CIISec (and addressed by CYBERWISER.eu)	Suggested skill level
Information Security Risk Manager	B2 - Risk Assessment	Level 5: Leads complex risk assessments, interfacing routinely with senior management.
	B3 - Information Risk Management	Level 5: Develops complex and innovative information risk management plans either as an individual or leading a team.

Table 12. Primary skill and skill level for the role Information Security Risk Manager

3.3.8 Description of role Information Security Risk Officer

The post holder would typically be of junior management level with a level of responsibility and accountability according to the agreed acceptable levels of risk assigned to that role (including legal and regulatory compliance obligations). However, in smaller organisations the level and spread of knowledge, skills and experience may widen as fewer separate roles focussing on individual discipline areas may exist. This wider skill set would also be likely to be at a lesser skill level. They may support a required regulatory role in some sectors [23].

Information Security Risk Officers are tasked to ensure that information security risks are identified and assessed, making appropriate recommendations. They would typically provide advice and guidance to other areas of the business relating to the process and outcome of risk assessments. They may well support the organization's information 'risk appetite' through their assessments and advice. They would identify mitigations to information security risks and likely to be involved in monitoring and assessing the effectiveness of such measures [23].

Table 13 summarizes the primary skills for the role Information Security Risk Officer suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as suggested levels for the skills. Note that not all primary skills suggested by CIISec are included. The skills not included in the table are outside the scope of CYBERWISER.eu. The reader is referred to the CIISec Roles Framework for details on other skills for this role.

Role name	Primary skill suggested by CIISec (and addressed by CYBERWISER.eu)	Suggested skill level
Information Security Risk Officer	B2 – Risk Assessment	Level 3: Undertakes basic risk assessments with some supervision.
	B3 - Information Risk Management	Level 3: Develops basic information risk management plans with some supervision.

Table 13. Primary skill and skill level for the role Information Security Risk Officer

3.3.9 Description of role Threat Analyst

The primary role of Threat Analysts is to analyse intelligence and open source information in order to identify, monitor, assess and counter generic and more specific threats posed by threat actors against an organisation or sector [23].

The primary aim of Threat Analysts would be to develop indicators to identify and maintain awareness of the operating environment which can often be a changing and evolving one. They would collect, process, analyse and disseminate threat assessments and indicators. They would be mapping threats against the threat assessment relative to their organisation or business sector [23].

Table 14 summarizes the primary skills for the role Threat Analyst suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as suggested levels for the skills. Note that not all primary skills

suggested by CIISec are included. The skills not included in the table are outside the scope of CYBERWISER.eu. The reader is referred to the CIISec Roles Framework for details on other skills for this role.

Role name	Primary skill suggested by CIISec (and addressed by CYBERWISER.eu)	Suggested skill level
Threat Analyst	B1 - Threat Intelligence, Assessment and Threat Modelling	Level 2: Can explain the principles of threat intelligence, modelling and assessment. This might include experience of applying threat intelligence, modelling and assessment principles in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination.
		Level 3: Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments under supervision. Appropriate and relevant certifications include CREST Practitioner Threat Intelligence Analyst, SANS GIAC Cyber Threat Intelligence.
		Level 4: Undertakes routine threat intelligence/modelling tasks or threat assessments without close supervision. Undertakes complex threat intelligence tasks or threat assessments under supervision. Appropriate and relevant certifications include CREST Registered Threat Intelligence Analyst.
		Level 5: Undertakes complex threat intelligence/modelling tasks or threat assessments without supervision. Manages threat intelligence/assessment teams. Appropriate and relevant certifications include CREST Certified Threat Intelligence Manager.

Table 14. Primary skill and skill level for the role Threat Analyst

3.3.10 Description of role Vulnerability Assessment Analyst

The post holder would typically be a skilled individual. They analyse and test infrastructures, systems, websites and apps are correctly implemented and offering the levels of protection intended. To provide additional assurance independent penetration testing may still be required, even by organisations that employ their own testing teams, as this may be a regulatory requirement. Identifying assessing and prioritizing threats vulnerabilities that have been identified in an organisations infrastructures systems, apps and websites [23].

The primary aim of Vulnerability Assessment Analysts would be to test perform assessments of systems, infrastructures, networks website and apps to identify where they deviate from acceptable configurations or where their version or patch levels are not meeting accepted configuration tolerances. They would also measure the effectiveness of systems against known vulnerabilities. Through identifying any weaknesses using known vulnerabilities and common configuration faults they would provide a report to the business on their findings. This report should be written to enable a clear understanding of any vulnerabilities found together with an assessment of the level of any attacker's skills required to exploit them. They should offer recommendations based on severity to enable the business to set a remediation plan and prioritization of any actions based on their business need and levels of accepted risk [23].

Table 15 summarizes the primary skill for the role Vulnerability Assessment Analyst suggested by CIISec and that is also addressed by CYBERWISER.eu, as well as suggested level for the skill. Note that not all primary

skills suggested by CIISec are included. The skills not included in the table are outside the scope of CYBERWISER.eu. The reader is referred to the CIISec Roles Framework for details on other skills for this role.

Role name	Primary skill suggested by CIISec (and addressed by CYBERWISER.eu)	Suggested skill level
Vulnerability Assessment Analyst	B1 - Threat Intelligence, Assessment and Threat Modelling	Level 3: Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments under supervision. Appropriate and relevant certifications include CREST Practitioner Threat Intelligence Analyst, SANS GIAC Cyber Threat Intelligence.

Table 15. Primary skill and skill level for the role Vulnerability Assessment Analyst

4. The overall learning path of CYBERWISER.eu

From a competence and cybersecurity culture point of view, one of the main outcomes of CYBERWISER.eu is training materials to support the training of the selected skills and profiles described in Section 3. This includes training material for creating cyber-risk models for assessment and countermeasure suggestion to support the fulfilment of Objective 2 of CYBERWISER.eu. Objective 2 states: "Development of innovative tools with complete training material for the provision of cybersecurity training scenarios and exercises, simulation of cyberattacks and defence mechanisms, exercise progress monitoring and measurement of user performance."

Moreover, from the capacity building environment point of view, one of the main outcomes is a set of innovative and highly descriptive economic risk models for cyber-risk assessment and countermeasure suggestion, to boost user training and performance evaluation. This outcome supports the fulfilment of Objective 3 of CYBERWISER.eu, which states: "Create robust and insightful economic models for monetary exposure assessment to risk in virulent cyber climates, thereby boosting user training and performance evaluation."

In addition, from an innovation stream point of view, some of the contributions brought by CYBERWISER.eu are:

- Simulation of a wide variety of attacks and countermeasures concerning the digital assets characterized in the scenario object of the training.
- Advanced economic risk models and algorithms for an estimation of the money being at risk due to the cyber landscape to which the company is exposed.

Thus, the CYBERWISER.eu approach is a cyber-risk centric approach in which risk is used to guide and support training in cybersecurity. In addition, to boost cybersecurity awareness, the CYBERWISER.eu approach is supported by cybersecurity-awareness training provided in the Primer offering level.

This document is the first of two deliverables related to training material and the focus of this document is mainly on training material for courses that will be available in the first two offering levels (Primer and Basic). However, to provide a holistic picture, we first explain in this section the overall learning path of CYBERWISER.eu and how the learning path is related to the roles (and skills) described in Section 3, as well as the four offering levels (Primer, Basic, Intermediate, Advanced), before we describe the courses and training material offered at Primer and Basic level in Sections 5 and 6.

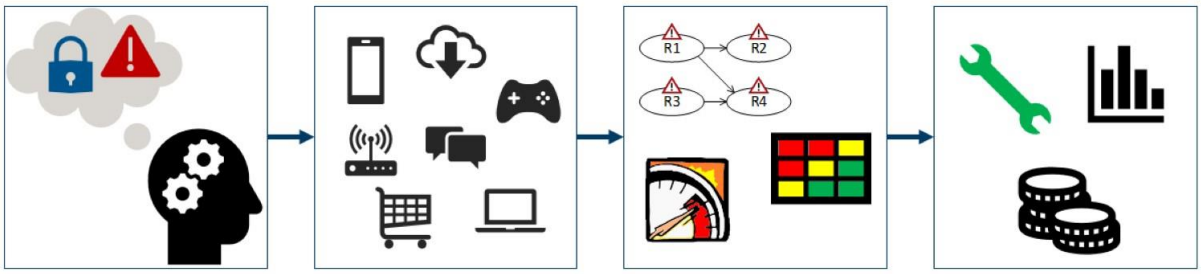
Although the focus in this deliverable is on courses and training material offered at Primer and Basic level, we will touch upon the overall contents of the courses that will be provided in all offering levels. Section 4.1 provides a high-level explanation of the cyber-risk centric learning path, while Sections 4.2 and 0 go more into the details of the awareness and cyber-risk analysis parts, respectively, which together make up the learning path. Finally, Section 4.4 relates the learning path to the offering levels in CYBERWISER.eu.

4.1 Cyber-risk centric learning path

As illustrated in Figure 5 the learning path consists of four main parts:

- Cybersecurity and risk awareness
- Context establishment
- Cyber-risk assessment
- Cyber-risk treatment and cost/benefit analysis

Although these parts are illustrated as consecutive steps, they do not have to be carried out consecutively. Depending on their previous knowledge and skills participants may choose to obtain training in one or more parts of the learning path by selecting appropriate courses. Some courses may also cover more than one part of the learning path.



Cybersecurity and risk awareness	Context establishment	Cyber-risk assessment	Cyber-risk treatment and cost/benefit analysis
R1			R1
R2	R2	R2	R2
R3	R3	R3	R3
R4	R4	R4	
R5	R5	R5	

Figure 5. The overall cyber-risk centric learning path and security roles mapped to the learning path

The learning path is constructed to be in line with ISO 27001 [9] and ISO 27005 [10], which are security standards known globally and used both in industry and academia. The goal of cybersecurity and risk awareness is to make participants aware of common cybersecurity risks as well as to teach cybersecurity concepts important for the rest of the learning path. Context establishment, cyber-risk assessment, and cyber-risk treatment and cost/benefit analysis are in line with corresponding steps of ISO 27005 [10] and are typically collectively referred to as cyber-risk analysis. In CYBERWISER.eu, the goal of context establishment is to teach about defining and describing the target of analysis including its scope and focus. In the case of CYBERWISER.eu, the target of analysis is referring to the infrastructure simulated on the cyber range. The goal of cyber-risk assessment is to teach about risk identification including vulnerabilities and unwanted incidents, risk estimation, and risk evaluation, as well as risk modelling, while the goal of cyber-risk treatment and cost/benefit analysis is to teach about treatments/countermeasures and their economic effects as well as their impact on the cyber-risk picture.

Figure 5 illustrates also a mapping of security roles that require skills addressed in one or more parts of the learning path. The roles are those selected in Section 3.3:

- R1: Head of Information/Cyber Security (described in Section 3.3.6)
- R2: Information Security Risk Manager (described in Section 3.3.7)
- R3: Information Security Risk Officer (described in Section 3.3.8)
- R4: Threat Analyst (described in Section 3.3.9)
- R5: Vulnerability Assessment Analyst (described in Section 3.3.10)

The positioning of the roles in relation to the learning path is based on their description provided in Section 3.3, which is based on the CIISec Roles Framework [23]. As pointed out by the CIISec Roles Framework, the role descriptions, as well as the skills required by the roles, may vary because of factors such as the size of the organisation, complexity, sector and business model. This means that the mapping above may also vary among different organizations. However, given that the above-mentioned CIISec frameworks have been "*developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders [24]*" the mapping will apply in most cases. The mapping in Figure 5 will also guide the appropriate shaping of the curriculum and the courses in Section 5 as well as in Deliverable D4.4 Training material, final version.

All the above-mentioned roles need to be aware of the basics of cyber-risk such as domain specific concepts and processes, and well-known risks. All roles therefore fit under the first part of the learning path (cybersecurity and risk awareness).

Role R1 fit mainly under cyber-risk treatment and cost-benefit analysis because the role is typically at senior management level who makes decisions on, among other things, the value of certain security assets and whether certain risks that may harm the assets should be treated or not based on treatment cost.

The roles R2 and R3 fit in all parts of the learning path because they must ensure that cybersecurity risks are identified and assessed and based on risk assessment results make appropriate recommendations. These roles are also typically in charge of leading such tasks.

The roles R4 and R5 are more technical in nature and collect, process, analyse and disseminate threat assessments and indicators. These roles also identify weaknesses using known vulnerabilities and common configuration faults to obtain a risk picture. Thus, roles R4 and R5 fit under the context establishment and the cyber-risk assessment parts of the learning path.

4.2 Cybersecurity and risk awareness

To make participants aware of common cybersecurity risks and to teach cybersecurity concepts important for the rest of the learning path, the cybersecurity and risk awareness part is supported by three main topics:

- Introduction to cyber-risk analysis and cybersecurity
- Awareness of five common cybersecurity risks
- Introduction to cyber-risk assessment

The first topic gives a basic introduction to cyber-risk analysis and cybersecurity as well as related concepts. The second topic presents five common cybersecurity risks for awareness purposes and teaches also how to protect oneself from these cybersecurity risks. While the first topic covers a high-level explanation about the cyber-risk analysis process, the third topic focuses on cyber-risk assessment and explains its purpose and the activities typically covered within cyber-risk assessment. These topics are further detailed in terms of courses in Section 5.

With respect to the second topic (awareness), it is necessary to explain the selection process of the five cybersecurity risks for the awareness training and the rationale behind the selection. As illustrated in Figure 6 we used, as a starting point, reports from recognized organizations/unions in the cybersecurity field including the European Cybersecurity Organization (ECSO) [30] and the European Union agency for Network and Information Security (ENISA) [2] exploiting their experience and research on the topic. Later we applied some criteria to make the selection more case specific for the needs of CYBERWISER.eu. The applied criteria were:

- Risks with high impact on the sectors represented by the three Full Scale Pilots in CYBERWISER.eu
- Risks that are most significant for non-technical people
- Risks that are relevant for basic awareness
- Feedback from experts in the consortium (made the list of five common cybersecurity risks available to the consortium and received feedback)

Initially, one of the five common risks selected was "web-based attacks and web application attacks", but this was later replaced with “password weakness” as this is one of the most commonly exploited vulnerabilities as discussed in Table 16, and because cyber-risks related to web-based attacks and web application attacks will be covered in detail in courses provided at Intermediate and Advanced offering levels. This decision is based on work carried out in Task 2.3 (model adaptation and development) in which a set of web-based attacks is selected as the most important cyber-risks to address in CYBERWISER.eu.

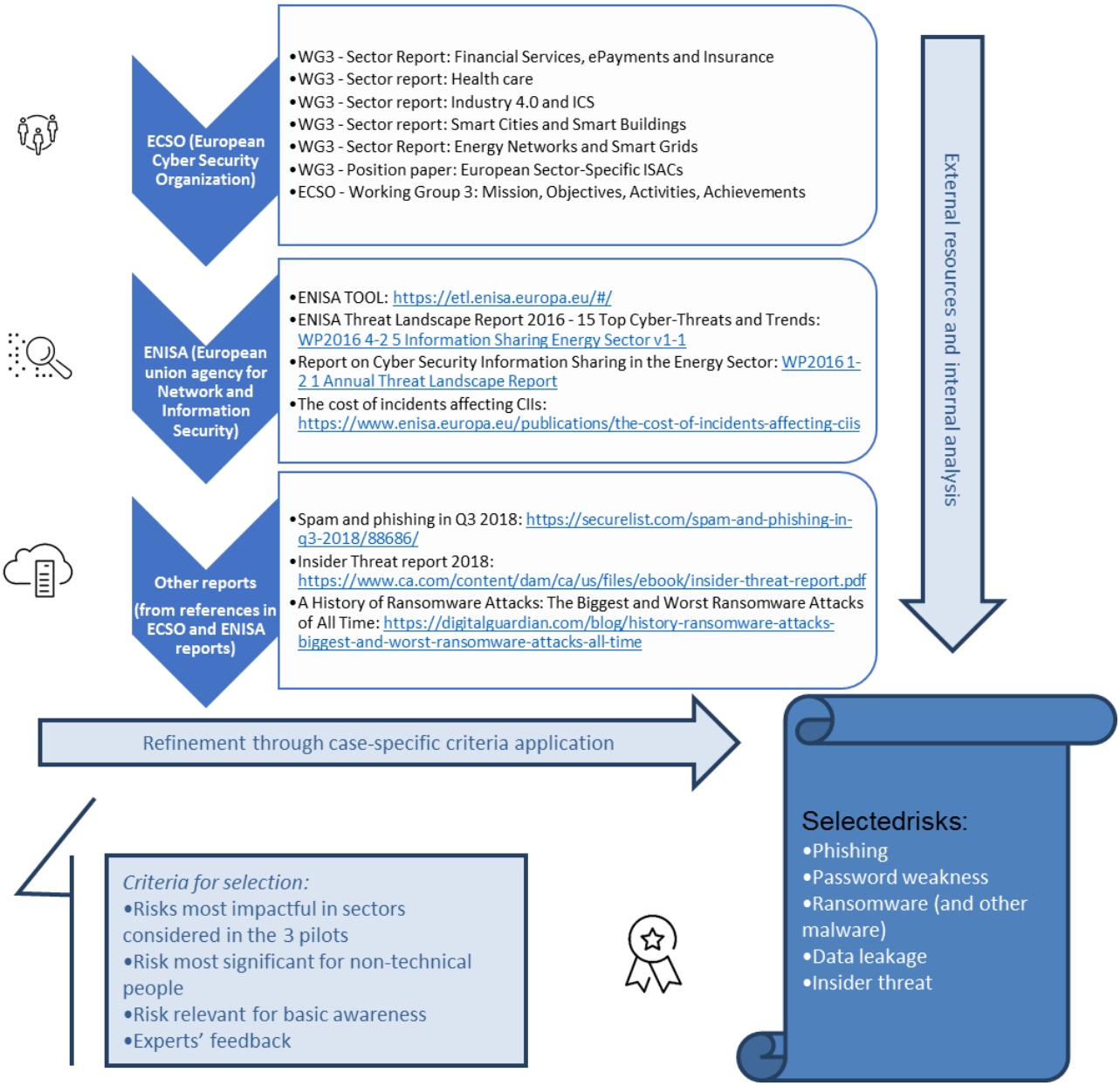


Figure 6. Selection process of the five common cybersecurity risks for awareness training

Table 16 provides an overview of the five common cybersecurity risks selected for the awareness training. The table provides a brief explanation for each cybersecurity risk and the rationale for inclusion in the awareness training.

Cybersecurity risk	Brief description	Rationale for inclusion
Phishing	Phishing is a cybercrime that aims to lure users to malicious sites to provide sensitive data such as personally identifiable information (PII), banking and credit card details, and passwords. The information is used to access important accounts and can result in identity theft and financial loss. It is a pervasive attack because it primarily uses social engineering to attack end users and it is becoming more sophisticated and targeted, which makes its detection difficult. Moreover, also low capability criminals can perform a phishing attack using frameworks of Phishing as a Service [2].	1) 85% of organizations have been and are targeted for phishing attacks. Moreover, phishing damages exceeds $1 billion [1]. 2) The European Cyber Security Organization (ECSO) reports that Phishing is one of the most common and impactful threats within Energy, Transportation and other specific sectors [18]. 3) The threat landscape tool by ENISA [2] reports that Phishing was one of top 15 cybersecurity risks in 2017 and 2018. 4) The target of a Phishing attack can be employees of every job level and job profile [2]. 5) Social engineering techniques are mostly unknown by employees [2]. 6) Phishing is the most successful attack vector for data breaches and security incidents and for most of the cyber threats [2].
Password weakness	Weak passwords are one of the most common vulnerabilities exploitable to access company infrastructure and facilitating more complex attacks. According to internet security threat reports by Symantec and WatchGuard, weak passwords are a major security threat [3][4].	1) Symantec reports that IoT devices experienced an average of 5200 attacks per month in 2018 and that 24.6% of passwords used in IoT attacks were "123456", while 17% were blank in the sense that there were no passwords [3]. 2) WatchGuard carried out an investigation of passwords used for 335,000+ government and military accounts and found that nearly half of all passwords associated with .gov and .mil email addresses are weak. As an example, they found 1700 cases where the password "123456" were used [4].
Ransomware (and other malware)	Ransomware is a type of malware that imprisons user data making them unavailable by encrypting in order to request a ransom to release them. While traditional malware requires cybercriminals to go through multiple steps before making profit, ransomware makes it an automated process. Moreover, also low capability criminals can spread a ransomware by using prepared frameworks (Ransomware as a Service).	1) The European Cyber Security Organization (ECSO) reports that Ransomware is one of the most common and impactful threats within Energy, Transportation and other specific sectors [18]. 2) The threat landscape tool by ENISA [2] reports that 60% of malware payloads were ransomware and this threat keeps growing. Ransomware was also one of top 15 cybersecurity risks in 2017 and 2018. 3) Real cases of financial loss because of ransomware [19]. 4) A series of "police" ransomware packages appeared, so called because they purported to be warnings from law enforcement about the victims' illicit activities and demanded payment of "fines"; they began to exploit the new generation of anonymous payment services to better harvest payments without getting caught [20].
Data leakage	Information leakage is a category of cyber threats exploiting weaknesses of run	1) The European Cyber Security Organization (ECSO) reports that data leakage is one of the most common and impactful threats within

Cybersecurity risk	Brief description	Rationale for inclusion
	time systems, of components configuration, programming mistakes and user behaviour in order to leak important information.	Energy, Transportation and other specific sectors [18]. 2) The threat landscape tool by ENISA [2] reports that data leakage is among top 15 cybersecurity risks in 2017 and 2018. Similar report is also given by OWASP [5]. 3) There exist many incidents causing data leakage, including employees. This means that employees in an organization must be aware of this cybersecurity risk. Data leakage is an issue both for organization and for users themselves because of identity theft. 4) The General Data Protection Regulation (GDPR) [6] poses possible administrative sanctions for data breaches, which are essentially data leakage of personal data. Sanctions are requested when the necessary security countermeasures (both technical and organizational) have not been put in place.
Insider threat	Insider threat is related to the use of authorized access, wittingly or unwittingly, that can result in a harm to the security of an organization. An insider threat can be a current or former employee, contractor or business partner, all those that can compromise the confidentiality, integrity and availability of the organization's network systems, data or premises. This type of threat can include fraud, theft of intellectual property, unauthorized trading, espionage and information technology infrastructure sabotage.	1) The European Cyber Security Organization (ECSO) reports that insider threat is one of the most common and impactful threats within Energy, Transportation and other specific sectors [18]. 2) The threat landscape tool by ENISA [2] reports that insider threat is among top 15 cybersecurity risks in 2017 and 2018. 3) ENISA reports that the most expensive attacks are insider threats, followed by DDoS and web-based attacks [7]. 4) According to a survey carried out by CA Technologies, 90% percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%) [8].

Table 16. Overview of five common cybersecurity risks selected for the awareness training

4.3 Cyber-risk analysis

Figure 7 illustrates the relationship between the risk analysis process in ISO 27005 [10] (illustrated on the left-hand side) and the corresponding steps of the learning path described in Section 4.1 (illustrated on the right-hand side). This section describes the learning path in more detail with respect to the steps of the risk analysis process.

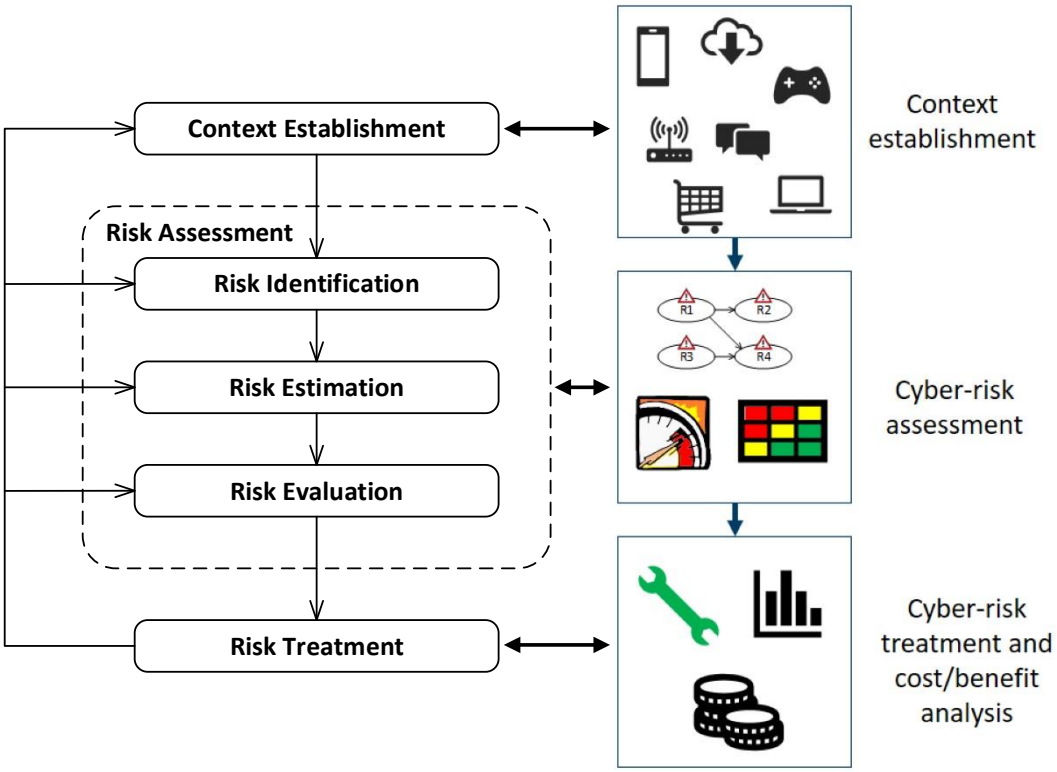


Figure 7. Relationship between the learning path and the risk analysis process

The purpose of the steps in the risk analysis process are as follows:

- The context establishment is the preparatory step for the subsequent activities and involves the documentation of both the external and the internal context of relevance for the assessment in question [12]. We do this by carrying out the following four sub-steps:
  - Describe target of analysis
  - Identify and describe security assets
  - Identify and describe threat profiles and high-level risks
  - Identify risk criteria
- The purpose of risk assessment is to identify, estimate, and evaluate risks. Each of these activities are carried out in their respective sub-steps:
  - Risk identification is an activity that aims to identify, describe, and document risks and possible causes of risks.
  - Risk estimation is an activity that aims to estimate and determine the level of the identified risks. The risk level is derived from the combination of the likelihood and consequence. In CYBERWISER.eu, we regard likelihood in terms of frequency and consequence in terms of economic impact. Thus, the risk level is given in terms of monetary loss.
  - Risk evaluation is an activity involving the comparison of the risk estimation results with the risk evaluation criteria to determine which risks should be considered for treatment.
- The purpose of risk treatment is to identify and select means for risk mitigation and reduction. The selection of which treatment to implement is based on an analysis of the costs and benefits of the identified treatments. The implementation of a treatment has in turn an effect on the risk picture as

illustrated by the arrows in Figure 7 going from risk treatment to context establishment, risk identification, estimation, and evaluation.

4.3.1 Context establishment

As mentioned above, and illustrated in Figure 8, context establishment consists of the following four main steps:

1. Describe target of analysis
2. Identify and describe security assets
3. Identify and describe threat profiles and high-level risks
4. Identify risk criteria

Each of these steps consists of their respective sub-steps as illustrates in Figure 8. Looking closer at the first step, we describe the target of analysis by first describing the scope and focus of the analysis (Step 1.1). The scope of the analysis is the extent or range of a risk assessment; it defines what is held inside and what is held outside of the assessment. The focus of the analysis is the main issue or central area of attention in a risk assessment; the focus is within the scope of the assessment. Typically, a risk analysis is carried out by an analysis team which consists of at least two persons where each person takes the role as risk analysis leader and risk analysis secretary, respectively. These roles are important to define early to carry out the assessment as smoothly as possible (Step 1.2). Finally, it is necessary to model the target of analysis (Step 1.3). In CYBERWISER.eu, we will do this by modelling the target using a (semi-) formal language, such as the Unified Modelling Language (UML), which is a specification defining a graphical language for visualizing, specifying, constructing, and documenting the artefacts of distributed object systems [13].

A crucial step in the context establishment, which also supports the further definition of the focus of the assessment, is the identification and documentation of the security assets, which brings us to the second step. First, we identify and describe information security assets based on target description to pinpoint the most important valuables to consider in the analysis. This is done using CORAS asset diagrams [11] (Step 2.1). The assets are the things or entities we want to protect and are the real motivation for conducting the risk assessment in the first place. Often there are multiple assets and limited resources to conduct the risk analysis, in such cases we need to rate all assets according to their importance in order to prioritize the risk assessment (Step 2.2). Finally, we need to identify and describe existing security controls and the information security assets they protect (Step 2.3).

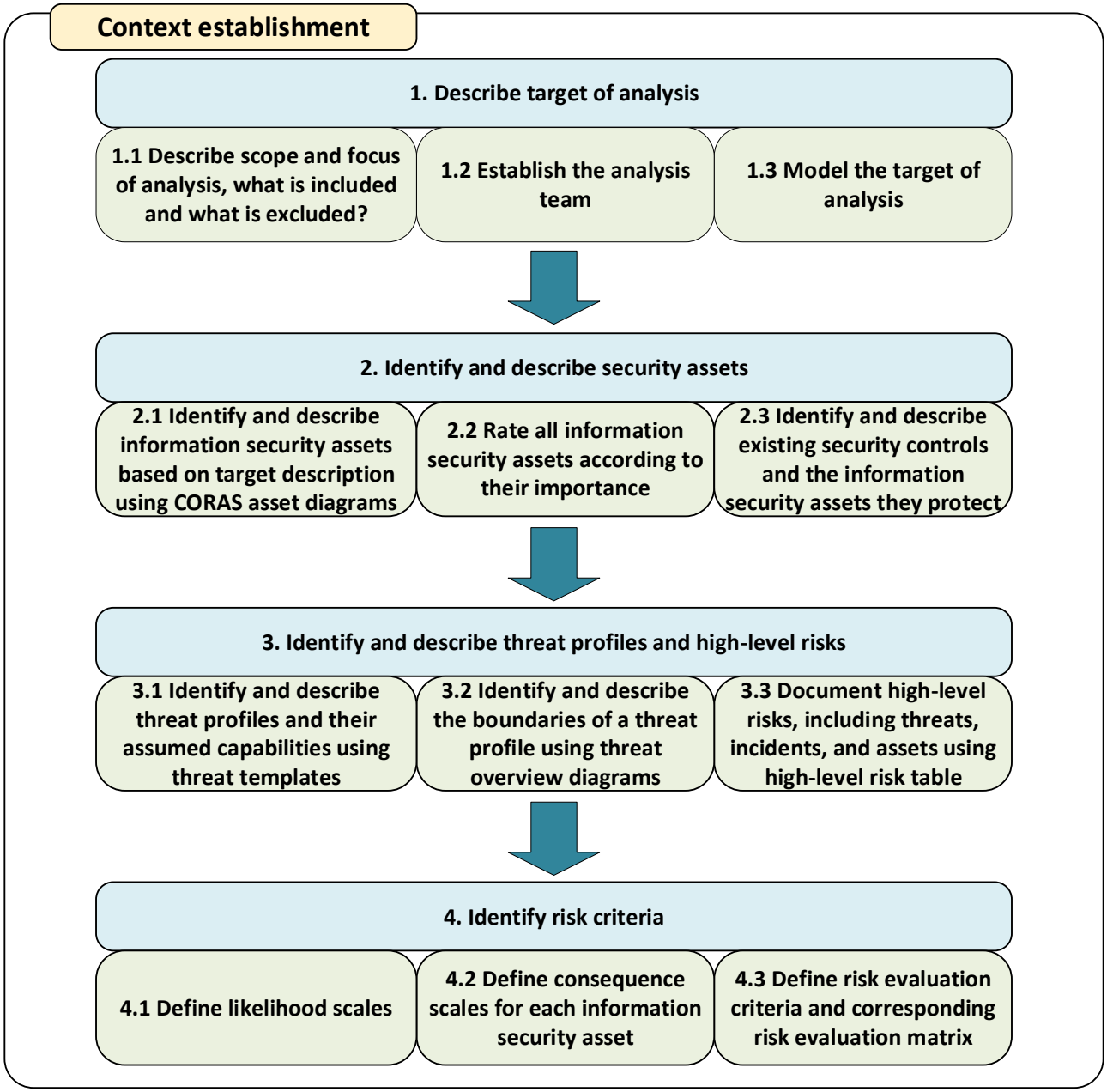


Figure 8. The steps related to context establishment

The identification and description of threat profiles is necessary to reason about attacker types and attacker motivation in relation to assets and the target description (Step 3.1). The documentation of threat profiles may be carried out using a template [14]. In order to easily obtain an overview of the boundaries of a threat profile we can identify and describe the boundaries of a threat profile using threat overview diagrams (Step 3.2) [14]. Finally, having documented the threat profiles and their boundaries, it is necessary to document a high-level risk picture using a high-level risk tables in which we capture threat sources, threats, vulnerabilities, unwanted incidents, and assets (Step 3.3) [11], which will function as a guiding basis when identifying risks in Step 5.

The identification of risk criteria is basically about defining likelihood scales (Step 4.1), consequence scales (Step 4.2), and risk evaluation criteria (Step 4.3). These scales will later be used to estimate and evaluate risks.

4.3.2 Cyber-risk assessment

The process for cyber-risk assessment in CYBERWISER.eu is mainly inspired by the corresponding process from the WISER project. However, there is one substantial difference: while WISER provided a straightforward method-description aimed at experienced cyber-risk professionals, CYBERWISER.eu will offer pedagogic presentations supported by examples and guidelines. As illustrated in Figure 9, cyber-risk assessment consists of three main steps (the following numbering of the steps continues from the last step of context establishment):

5. Identify risks
6. Estimate risks
7. Evaluate risks

Risk identification is carried out using the CORAS risk modelling language to identify and document threat sources, threats, vulnerabilities, incidents, and security assets that may be harmed by incidents. In addition, indicators are also identified and included in the risk model to capture the dynamic behaviour of the target and to facilitate dynamic risk assessment (Step 5.1). Having identified risks and created risk models, next, we need to validate the model to make sure that the final risk model corresponds to the reality (Step 5.2). Finally, in order to be able to execute the risk model in the platform, we translate the risk model schematically into a script written in R (Step 5.3). This script is then fed to the Economic Risk Evaluator component (described in D2.3 Platform Design, initial version [21]).

Risk estimation is carried out using empirical methods such as interviews and brainstorming sessions to gather expert opinions, inspection of logs or other statistical and historical data, and the use of available repositories. The purpose is to identify base line estimates for likelihood and consequence values of the risk assessment algorithm defined previously (Step 6.1). Next, we need to validate the base line estimates integrated in the risk assessment algorithms to make sure that our base line estimates correspond to reality (Step 6.2). The Steps 5.2, 6.1 and 6.2 require programming skills. Considering the scope of CYBERWISER.eu, the courses provided in CYBERWISER.eu are not directed on how to program but is mainly about teaching cybersecurity in a risk-centric approach. Thus, in CYBERWISER.eu, the courses will cover the principles and activities in risk assessment properly equipping and preparing the relevant roles in Section 3 to carry out risk assessment. For a detailed technical explanation on how to program risk assessment algorithms, the reader is referred to the deliverables from the WISER project: D3.2 - Cyber risk modelling language and guidelines, preliminary version [31], and D3.4 - Cyber risk modelling language and guidelines, final version [32].

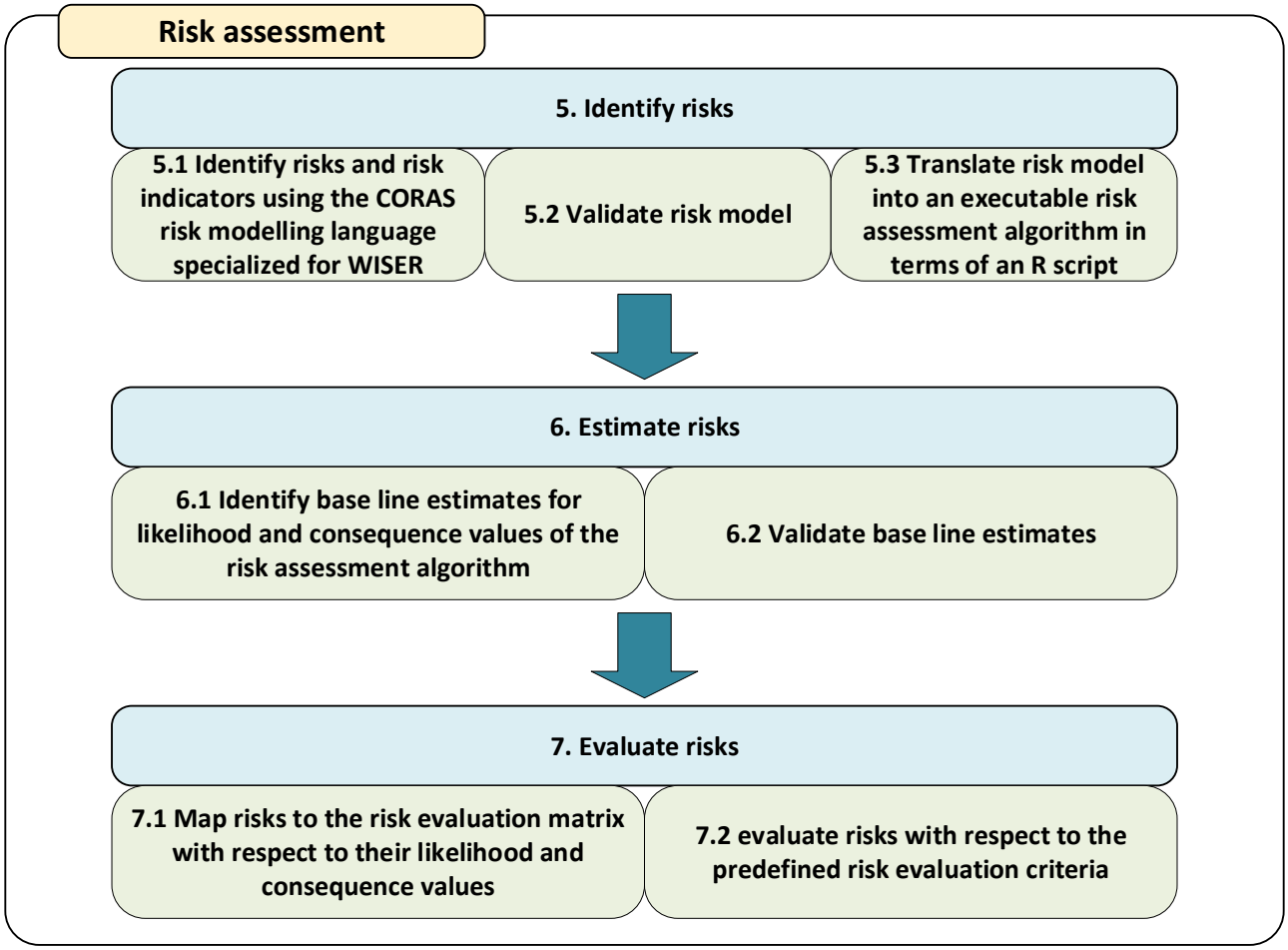


Figure 9. The steps related to cyber-risk assessment

Risk evaluation is typically carried out by mapping each risk into a predefined risk evaluation matrix (defined in Step 4 of the context establishment) with respect to its likelihood and consequence value to determine the risk level (Step 7.1). However, as risk evaluation is a decision point in the overall risk analysis process, we need to confirm the risk evaluation criteria and consolidate the risk estimates before commencing the evaluation of risks. Moreover, we need to investigate the identified risks to see whether certain sets of risks should be aggregated and evaluated as a single risk. This is done to avoid accepting risks that individually are non-critical, but unacceptable in combination. Finally, we also group risks that have elements in common because risks that share common elements such as threats and vulnerabilities may be treated by the same means (Step 7.2).

4.3.3 Cyber-risk treatment and cost/benefit analysis

In CYBERWISER.eu, we focus on the identification of treatments for the purpose of reducing or removing risks. As illustrated in Figure 10, risk treatment consists of one main step (Step 8) with two sub-steps.

The risk treatment activity involves both the identification and the analysis of treatment. Treatment identification is done similarly to the risk identification, for example via brainstorming or by using available lists and repositories. Treatments are identified and documented using CORAS treatment diagrams (Step 8.1). The identified treatments are then included in the Countermeasure Simulator in CYBERWISER.eu, which in turn makes the treatments (risk countermeasures) available to the participants. The countermeasures are made available to the course participants at a stage where they need to select treatments, based on a cost/benefit analysis (Step 8.2).

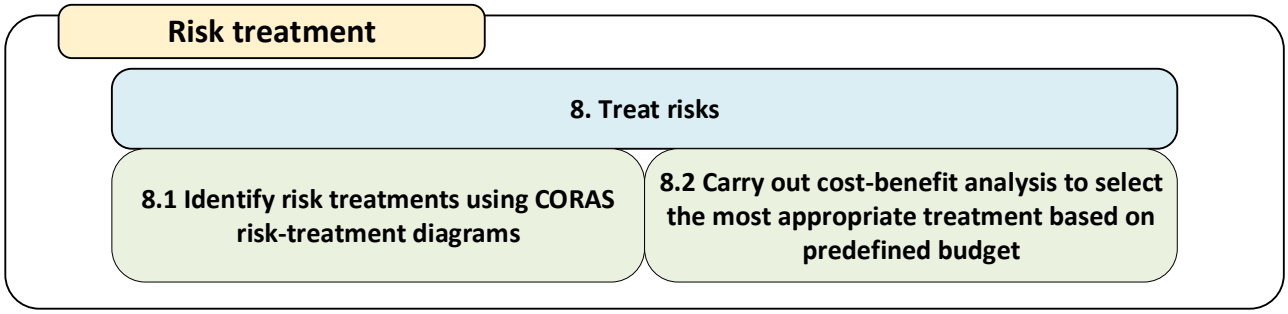


Figure 10. The steps related to cyber-risk treatment

4.4 Relating the learning path to the offering levels in CYBERWISER.eu

As illustrated in Figure 11, the various offering levels of CYBERWISER.eu will support one or more parts of the learning path presented in the above sections. Cybersecurity and risk awareness will be covered in the Primer and Basic offering levels. As mentioned in Section 4.1, the courses in the cybersecurity and risk awareness part of the learning path not only has the goal to teach and make participants aware about common cybersecurity risks, but also to teach the cybersecurity concepts important for the rest of the learning path. The courses provided in the Primer and Basic offering levels are further described in Section 5.

In addition to cybersecurity and risk awareness, the Basic offering level covers both context establishment and cyber-risk assessment of the learning path. With respect to context establishment, the courses in the Basic offering level will mainly address the steps related to describing target of analysis, identifying and describing security assets, and identifying and describing threat profiles and high-level risks. With respect to cyber-risk assessment, the courses in the Basic offering level will mainly address the step related to risk identification. Thus, the courses in the Basic offering level do not address *all* aspects of context establishment and cyber-risk assessment. As illustrates in Figure 11, context establishment and cyber-risk assessment are also covered in the Intermediate and the Advanced offering levels.

The courses in the Intermediate offering level will address additional aspects of context establishment and cyber-risk assessment not covered by the courses in the Basic level. The courses in the Advances offering level will address all aspects of context establishment and cyber-risk assessment. In addition to context establishment and cyber-risk assessment, the courses in the Intermediate and Advanced offering levels will also address cyber-risk treatment and cost/benefit analysis. Each offering level includes the courses and training material of the previous offering level. As mentioned in Section 1, the focus of this deliverable is on the courses and training material for the Primer and Basic offering levels (documented in Section 5). The courses and training material for the Intermediate and the Advanced offering levels will be identified and described as part of D4.4 (training material, final version).

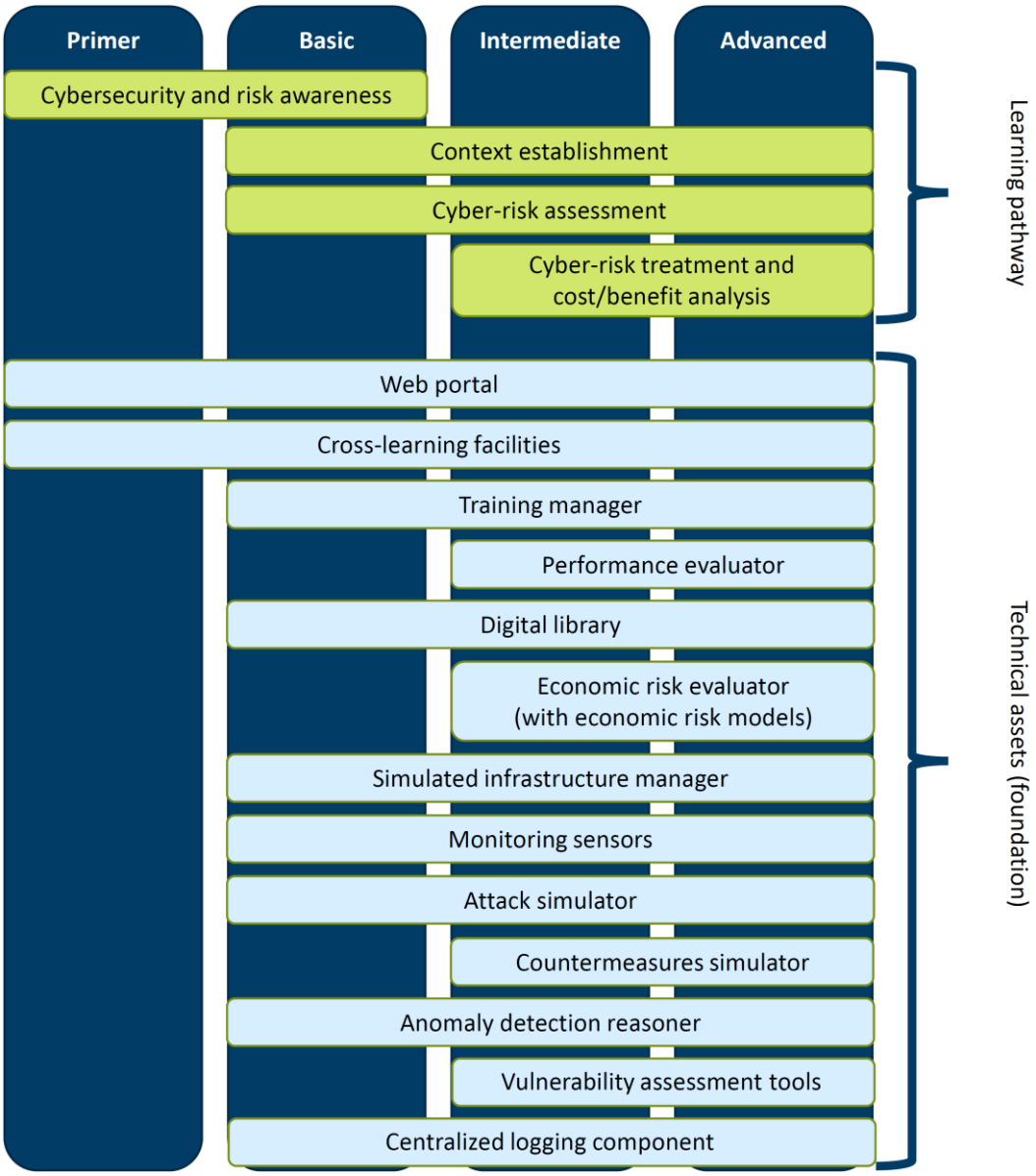


Figure 11. Relating the learning path to the offering levels

The final and third dimension we need to address to get a holistic picture of the relationship between the learning path and the offering levels is the technical aspects of CYBERWISER.eu. The technical assets are the technical foundation enabling the various courses in the different offering levels. Thus, the courses will be shaped also considering the technical capabilities that are available in the various offering levels. The technical assets are described in detail in Deliverables D2.3 and D2.5 [21].

5. Courses for the Primer and Basic offering levels

This section provides a detailed description of all courses provided in the Primer and Basic offering levels. Section 5.1 provides an overview of the courses, while Sections 5.2 and 5.3 provide descriptions of the courses provided at the Primer and Basic offering levels, respectively.

5.1 Overview of the courses

Table 17 shows an overview of the courses for the Primer and Basic offering levels and their relationship to the overall learning path. The following sections describe these courses in detail by using the course template outlined in Section 2.1.1. For the courses that have modules, we include module description immediately after the course description using the module template described in Section 2.1.2. There are in total seven courses for the Primer offering level (P-01 – P-07) and five courses for the Basic offering level (B-01 – B-05). The letter "P" in the course ID means "Primer", while the letter "B" means "Basic".

Course ID	Course name	Offering level	Overall learning path
P-01	Introduction to cyber-risk analysis and cybersecurity	Primer	Cybersecurity and cyber-risk awareness
P-02	Awareness of Phishing	Primer	Cybersecurity and cyber-risk awareness
P-03	Awareness of Password Weaknesses	Primer	Cybersecurity and cyber-risk awareness
P-04	Awareness of Ransomware	Primer	Cybersecurity and cyber-risk awareness
P-05	Awareness of Data Leakage	Primer	Cybersecurity and cyber-risk awareness
P-06	Awareness of Insider Threat	Primer	Cybersecurity and cyber-risk awareness
P-07	Introduction to cyber-risk assessment	Primer	Cybersecurity and cyber-risk awareness
B-01	Describe target of analysis, level 1	Basic	Context establishment
B-02	Identify and describe security assets, level 1	Basic	Context establishment
B-03	Identify and describe threat profiles and high-level risks, level 1	Basic	Context establishment
B-04	Identify risks, level 1	Basic	Cyber-risk identification
B-05	Awareness of Password Weakness with hands-on training	Basic	Cybersecurity and cyber-risk awareness

Table 17. Overview of the courses for the Primer and Basic offering levels

As shown in Table 17, the courses P-03 – P-06 are awareness courses addressing the selected five common cybersecurity risks described in Section 4.2. The course P-01 introduces basic concepts central to cybersecurity and cyber-risk analysis, which provides the conceptual framework important for the rest of CYBERWISER.eu, while the course P-07 goes more into the details of cyber-risk assessment and its main processes.

The courses B-01 – B-03 address mainly the context establishment part of the learning path, including describing the target of analysis, identifying security assets to protect, and identifying threat profiles. The course B-04 on the other hand focuses on the risk identification part of the learning path. These courses have been named as "level 1" courses to indicate that they intend to cover a "beginner level" of the topics related to

context establishment and risk identification. Since the context establishment and the risk identification parts of the learning path spans Basic, Intermediate and Advanced offering levels, we foresee that there may be "level 2"/"level 3" courses of B-01 – B-04. However, this will become clearer when we identify the courses for Intermediate and Advanced offering levels in Deliverable D4.4 Training material, final version.

In the following sections, we assign security roles to the courses indicating the target audience of the course and the overall skill addressed. The roles are those selected in Section 3.3:

- R1: Head of Information/Cyber Security (described in Section 3.3.6)
- R2: Information Security Risk Manager (described in Section 3.3.7)
- R3: Information Security Risk Officer (described in Section 3.3.8)
- R4: Threat Analyst (described in Section 3.3.9)
- R5: Vulnerability Assessment Analyst (described in Section 3.3.10)

We also refer to skills (B1, B2, B3) as described in Section 3.3.

- B1: Threat Intelligence, Assessment and Threat Modelling
- B2: Risk Assessment
- B3: Information Risk Management

5.2 Courses for the primer offering level

This section describes the Courses P-01 – P-07 outlined above.

5.2.1 Introduction to cyber-risk analysis and cybersecurity

The purpose of this course is to teach about basic concepts central within cybersecurity and cyber-risk analysis that are important to understand in context of CYBERWISER.eu. In other words, the course introduces and clarifies the concepts (related to cybersecurity and cyber-risk analysis) that will be used throughout the various courses in CYBERWISER.eu. This course gives also an overall introduction to the cyber-risk analysis process and how cybersecurity is considered within this process. By cyber-risk analysis, we mean the five-step process outlined in Section 4.3. Table 18 describes the course with respect to the course template described in Section 2.1.1.

ID	P-01
Name	Introduction to cyber-risk analysis and cybersecurity
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	• R1 – Skill B2, Level 1. • R2 – Skill B2, Level 1. • R3 – Skill B2, Level 1. • R4 – Skill B1, Level 1. • R5 – Skill B1, Level 1.
Offering Level	Primer
Difficulty	Easy
Course Duration	90 minutes (two modules, 45 minutes each module)
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the basic concepts related to cyber-risk analysis and cybersecurity. 2. Understand the overall process of cyber-risk analysis and the relationship between cybersecurity and cyber-risk analysis.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to:

ID	P-01
	1. Identify and describe basic concepts related to cyber-risk analysis and cybersecurity. 2. Name and describe the steps in the overall process of cyber-risk analysis.
Prerequisites	General knowledge within information technology is an advantage, but not a requirement.
Module list	• P-01-M-01: Conceptual clarification of cyber-risk analysis and cybersecurity. • P-01-M-02: Overview of the overall cyber-risk analysis process.

Table 18. Course: Introduction to cyber-risk analysis and cybersecurity (P-01)

As indicated above, the course consists of the two modules P-01-M-01 and P-01-M-02. These modules are described in Table 19 and Table 20, respectively.

ID	P-01-M-01; Accompanying slide set number: 1
Name	Conceptual clarification of cyber-risk analysis and cybersecurity
Learning Objectives	It is expected that by the end of this module, participants will be able to identify and describe basic concepts related to cyber-risk analysis and cybersecurity. This includes: 1. Describe and distinguish risk-related concepts: a. Risk b. Unwanted incident c. Asset d. Party e. Likelihood f. Conditional likelihood g. Consequence h. Risk level i. Target of analysis j. System k. Vulnerability l. Threat m. Threat source n. Treatment o. 2. Describe and distinguish cybersecurity-related concepts: a. Cyberspace b. Cyber-system c. Cyber-physical system d. Cybersecurity e. Cyber-threat f. Cyber-risk g. Information security h. Confidentiality i. Integrity j. Availability
Module Duration	45 minutes
Prerequisites	General knowledge within information technology is an advantage, but not a requirement.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining the risk-related concepts and the cybersecurity-related concepts listed above.

Table 19. Module: Conceptual clarification of cybersecurity and risk analysis (P-01-M-01)

ID	P-01-M-02; Accompanying slide set number: 1
Name	Overview of the overall cyber-risk analysis process
Learning Objectives	It is expected that by the end of this module, participants will be able to name and describe the steps in the overall process of cyber-risk analysis. This includes: 1. Briefly describe the purpose of: a. Context establishment b. Risk identification c. Risk estimation d. Risk evaluation e. Risk treatment 2. Identify the differences of the above steps.
Module Duration	45 minutes
Prerequisites	General knowledge within information technology is an advantage, but not a requirement.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining the overall process of cyber-risk analysis.

Table 20. Module: Overview of the overall risk analysis process (P-01-M-02)

5.2.2 Awareness of five common cybersecurity risks

This section describes the five awareness courses provided in the Primer offering level. The five awareness courses are:

- Awareness of Phishing (see Table 21)
- Awareness of Password Weaknesses (see Table 22)
- Awareness of Ransomware (see Table 23)
- Awareness of Data Leakage (see Table 24)
- Awareness of Insider Threat (see Table 25)

Table 21 describes the course “Awareness of Phishing”. Upon completion of the course, the trainee will be able to define what phishing means, distinguishing between phishing and spear phishing. The trainee acquires understanding of social engineering techniques in order to defend himself from disclosing important information. The course aims also to raise personal commitment in security enhancement, teaching to signal phishing attempt.

ID	P-02; Accompanying slide set number: 2
Name	Awareness of Phishing
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	For all roles, the skill obtained is general awareness and mitigation of well-known Phishing attack they may be exposed to. This also implicitly trains them in the skills B1, B2, B3 by thinking about how such an attack may occur, what are the indicators, and how to mitigate such attacks.
Offering Level	Primer
Difficulty	Easy
Course Duration	15 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand what phishing is 2. Understand the phishing attack kill chain 3. Describe why phishing is so popular

ID	P-02; Accompanying slide set number: 2
	4. Understand how to protect against phishing
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. For Learning Goal1: a. Remember what social engineering is and how it is used in phishing attacks b. Understand the categories of phishing 2. For Learning Goal 2: a. Remember the main stages of the phishing attack b. Understand the importance of social engineering in a phishing attack 3. For Learning Goal 3: a. Name who is using phishing b. Understand the need of attackers to use phishing c. Understand why phishing is still popular 4. For Learning Goal 4: a. Identify phishing indicators b. Distinguish phishing emails c. Estimate proper action upon suspicious email d. Remember good habits for keeping security
Prerequisites	The participant must have the following knowledge: • Basic knowledge of using e-mail • Basic knowledge of how a browser works
Module list	None

Table 21. Course: Awareness of Phishing (P-02)

Table 22 describes the course “Awareness of Password Weaknesses”. Upon completion of this course, the trainee will be able to understand the need to have a password and be aware of good practices associated when defining it.

ID	P-03; Accompanying slide set number: 3
Name	Awareness of Password Weaknesses
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	For all roles, the skill obtained is general awareness and mitigation of well-known Password Weakness vulnerabilities they may be exposed to. This also implicitly trains them in the skills B1, B2, B3 by thinking about how such weaknesses may occur, what are the indicators, and how to mitigate such weaknesses.
Offering Level	Primer
Difficulty	Easy
Course Duration	15 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the use of passwords for authentication 2. Understand the risks associated with weak passwords Remember password best practices

ID	P-03; Accompanying slide set number: 3
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. For Learning Goal 1: a. Understand why a strong password is important b. Explain the need of different passwords for the various systems 2. For Learning Goal 2: a. List factors that make a password weak b. List different attacks exploring password weakness c. Explain the need to change a default password d. Describe different actions of an attacker with a password 3. For Learning Goal 3: a. List different guidelines for creating a strong password b. Identify password bad practices c. List mechanisms for password management
Prerequisites	The participant must have the following knowledge: • Basic knowledge of using e-mail • Basic knowledge of how a browser works
Module list	None

Table 22. Course: Awareness of Password Weaknesses (P-03)

Table 23 describes the course "awareness of ransomware". Upon completion of the course, the trainee will learn about ransomware, a type of malware that imprisons user data making the data unavailable by encryption in order to request a ransom to release them (decrypt the data). The course participants will become aware of ransomware kill chain and of other types of malware, understanding impacts and correlation with other threats. Finally, the participant will be able to estimate suspicious payloads and evaluate proper action against attacks' attempts and good habits to mitigate malware probabilities of success.

ID	P-04; Accompanying slide set number: 4
Name	Awareness of Ransomware
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	For all roles, the skill obtained is general awareness and mitigation of well-known Ransomware attack they may be exposed to. This also implicitly trains them in the skills B1, B2, B3 by thinking about how such an attack may occur, what are the indicators, and how to mitigate such attacks.
Offering Level	Primer
Difficulty	Easy
Course Duration	15 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand what ransomware is among malware definition 2. Learn about the malware attack kill chain 3. Describe how Malware is increasingly targeting our society 4. Understand how to protect against Ransomware and other Malware
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to:

ID	P-04; Accompanying slide set number: 4
	1. For Learning Goal 1: a. Remember what malicious software (malware) is and how ransomware is used b. Understand different types of malware 2. For Learning Goal 2: a. Recall the main stages of ransomware infection b. Understand the correlation with other cyber threats 3. For Learning Goal 3: a. Remember examples about malware attacks b. Understand why malware can't be completely defeated 4. For Learning Goal 4: a. Remember good cybersecurity hygiene practices b. Identify malware and ransomware indicators of infection c. Estimate proper action and mitigation after malware infection
Prerequisites	The participant must have the following knowledge: • Basic knowledge of using e-mail • Basic knowledge of how a browser works
Module list	None

Table 23. Course: Awareness of Ransomware (P-04)

Table 24 describes the course "awareness of data leakage". Upon completion of this course, the participant will understand the drivers of data leakage attacks, by learning attack vectors, scope and impacts of this threat. The participant will be aware of crucial factors that enable data leakage and the correlation with other threats or consequences (data breach, data disclosure).

ID	P-05; Accompanying slide set number: 5
Name	Awareness of Data Leakage
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	For all roles, the skill obtained is general awareness and mitigation of well-known Data Leakage weaknesses they may be exposed to. This also implicitly trains them in the skills B1, B2, B3 by thinking about how such a weakness may occur, what are the indicators, and how to mitigate such weaknesses.
Offering Level	Primer
Difficulty	Easy
Course Duration	15 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the scope and impact of data leakage 2. Understand the attack vectors used for data leakage 3. Describe how data leakage is increasingly targeting our society 4. Understand how to protect against data leakage
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. For Learning Goal 1: a. Remember what data leakage is and what information is targeted b. Understand different scopes and impacts of data leakage c. Understand the difference between data leakage and personal data breach 2. For Learning Goal 2: a. Remember common data leakage attack vectors

ID	P-05; Accompanying slide set number: 5
	b. Understand the correlation with other cyber threats 3. For Learning Goal 3: a. Recall examples about data leakage and personal data breaches b. Recall new paths for attacks c. Name security threat agents and top sectors under attack 4. For Learning Goal 4: a. List data leakage mitigation actions and countermeasures b. Name security threat agents and top sectors under attack
Prerequisites	The participant must have the following knowledge: • Basic knowledge of using e-mail • Basic knowledge of how a browser works
Module list	None

Table 24. Course: Awareness of Data Leakage (P-05)

Table 25 describes the course “Awareness of Insider Threat”. After doing this course, the trainee will be aware of the different insider threat profiles and how an insider threat can compromise the confidentiality, integrity and availability of the organization’s network systems, data or premises.

ID	P-06; Accompanying slide set number: 6
Name	Awareness of Insider Threat
Cybersecurity role	R1, R2, R3, R4, R5
Skill and expected skill level to be trained	For all roles, the skill obtained is general awareness and mitigation of Insider Threats they may be exposed to. This also implicitly trains them in the skills B1, B2, B3 by thinking about how insider threats may occur, what are the indicators, and how to mitigate such threats.
Offering Level	Primer
Difficulty	Easy
Course Duration	15 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the concept of insider threat 2. Remember the indicators of insider threats 3. Remember measures to detect insider threats 4. Understand legal concerns related with insider threats
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. For Learning Goal 1: a. Describe what an insider threat is b. Understand the need to know all your assets c. Understand the need to keep the record of all approved accesses/communications 2. For Learning Goal 2: a. List different characteristics of an insider threat b. Identify different insider threat profiles 3. For Learning Goal 3: a. Understand how an insider threat can be detected b. List different mechanisms to detect an insider threat 4. For Learning Goal 4: a. Understand the need to protect employee privacy

ID	P-06; Accompanying slide set number: 6
	b. Identify the boundaries between protecting and surveillance
Prerequisites	The participant must have the following knowledge: • Basic knowledge of using e-mail • Basic knowledge of how a browser works
Module list	None

Table 25. Course: Awareness of Insider Threat (P-06)

5.2.3 Introduction to cyber-risk assessment

The purpose of this course is to teach in more detail (compared to Course P-01) the purpose of cyber-risk assessment including the activities risk identification, risk estimation, and risk evaluation. The course will go into more detail of various strategies for each of the aforementioned activities, but still stay at a general level.

ID	P-07; Accompanying slide set number: 7
Name	Introduction to cyber-risk assessment
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 1, Level 2. • R3 – Skill B2, Level 1, Level 2. • R4 – Skill B1, Level 1. • R5 – Skill B1, Level 1.
Offering Level	Primer
Difficulty	Medium
Course Duration	45 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: Understand at a deeper level (compared to course P-01) the purpose of cyber-risk assessment and the activities typically covered within cyber-risk assessment.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: Describe at high-level the activities typically carried out in cyber-risk assessment including: a. Risk identification b. Risk estimation c. Risk evaluation
Prerequisites	Complete the Course P-01 (Introduction to cyber-risk analysis and cybersecurity). General knowledge within information technology is an advantage, but not a requirement.
Module list	None

Table 26. Course: Introduction to cyber-risk assessment (P-07)

Training material content will for this course (in D4.1) be in the form of PowerPoint presentation and supporting text describing the overall cyber-risk assessment activities.

5.3 Courses for the basic offering level

This section describes the Courses B-01 – B-05 outlined in Table 17.

5.3.1 Describe target of analysis, level 1

The purpose of this course is to teach about describing the scope and focus of the target system under analysis. The course will also explain the importance of doing this and teach about general strategies to document the target of analysis at a sufficient level of abstraction. The course has two modules. The first module (see Table 28) focuses on describing the scope and focus of the target system, while the second module (see Table 29) focuses on documenting the target of analysis.

ID	B-01
Name	Describe target of analysis, level 1
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 2. • R3 – Skill B2, Level 2. • R4 – Skill B1, Level 2. • R5 – Skill B1, Level 2.
Offering Level	Basic
Difficulty	Medium
Course Duration	90 minutes (two modules, 45 minutes each module)
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand how to describe the scope and focus of the analysis based on a given context. 2. Understand how to document the target of analysis.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. Describe the scope and focus of analysis with respect to a predefined context. 2. Create a model representing the target of analysis.
Prerequisites	Complete the Courses P-01 and P-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Module list	• B-01-M-01: Describe scope and focus of analysis, what is included and what is excluded? • B-01-M-02: Model the target of analysis

Table 27. Course: Describe target of analysis, level 1 (B-01)

ID	B-01-M-01; Accompanying slide set number: 8
Name	Describe scope and focus of analysis, what is included and what is excluded?
Learning Objective	It is expected that by the end of this module, participants will be able to: 1. Understand the concepts scope and focus and how they are related. 2. Describe the scope and focus of analysis with respect to a predefined context. 3. Understand the importance of, and how to explicitly describe, what is excluded from the target of analysis.
Module Duration	45 minutes
Prerequisites	Complete the Courses P-01 and P-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining how to describe scope, focus, and what is included/excluded of the analysis.

Table 28. Module: Describe scope and focus of analysis, what is included and what is excluded? (B-01-M-01)

ID	B-01-M-02; Accompanying slide set number: 8
Name	Model the target of analysis
Learning Objective	It is expected that by the end of this module, participants will be able to: Model the target of analysis in an informal and semi-formal manner.
Module Duration	45 minutes
Prerequisites	Complete the Courses P-01 and P-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining how to model the target of analysis in an informal/semi-formal manner.

Table 29. Module: Model the target of analysis (B-01-M-02)

5.3.2 Identify and describe security assets, level 1

The purpose of this course is to teach a structured approach to identify and document security assets that are to be considered in the cyber-risk assessment. This includes teaching strategies for how to analyse the target description to extract the asset-relevant information.

ID	B-02; Accompanying slide set number: 9
Name	Identify and describe security assets, level 1
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 2. • R3 – Skill B2, Level 2. • R4 – Skill B1, Level 2. • R5 – Skill B1, Level 2.
Offering Level	Basic
Difficulty	Medium
Course Duration	45 minutes

ID	B-02; Accompanying slide set number: 9
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand how to analyse the target to identify and describe security assets. 2. Describe security assets using CORAS asset diagrams.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. Identify and select appropriate security assets for the predefined target of analysis. 2. Understand the constructs necessary to create CORAS asset diagrams. 3. Create CORAS asset diagrams capturing security assets.
Prerequisites	Complete the Courses P-01 and P-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Module list	None

Table 30. Course: Identify and describe security assets, level 1 (B-02)

Supporting literature will be in the form of PowerPoint presentation and supporting text explaining how to use the target description to identify security assets, and how to use CORAS asset diagrams to document the security assets.

5.3.3 Identify and describe threat profiles and high-level risks, level 1

The purpose of this course is to teach a structured approach to organize risk-related information based on the target description, and how to use this information later to identify risks. The course introduces also the basic constructs of the risk modelling language CORAS.

ID	B-03
Name	Identify and describe threat profiles and high-level risks, level 1
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 2. • R3 – Skill B2, Level 2. • R4 – Skill B1, Level 2. • R5 – Skill B1, Level 2.
Offering Level	Basic
Difficulty	Medium/Hard
Course Duration	45 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the constructs necessary to create CORAS risk models. 2. Understand how to organize risk-related information to describe high-level risks. 3. Understand how to organize this information and later use it as input to risk identification.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. Associate risk-related concept to the corresponding CORAS risk model constructs.

ID	B-03
	2. Create tables documenting high-level risks.
Prerequisites	Complete the Courses P-01, P-02 and B-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Module list	B-03-M-01: Document high-level risks, including threats, incidents, and assets using high-level risk table

Table 31. Course: Identify and describe threat profiles and high-level risks, level 1 (B-03)

The course has one module (see Table 32), which focuses on the organization of risk-related information to support risk identification.

ID	B-03-M-01; Accompanying slide set number: 10
Name	Document high-level risks, including threats, incidents, assets and vulnerabilities using high-level risk table
Learning Objective	It is expected that by the end of this module, participants will be able to: Use a high-level risk table to document: 1. Threat sources by answering: who/what causes the risk? 2. Threats, unwanted incidents, and assets by answering: how? What is the incident? What does the risk harm? Respectively. 3. Vulnerabilities by answering: what makes the risk possible?
Module Duration	45 min.
Prerequisites	Complete the Courses P-01 and P-02. Basic knowledge within but not limited to a bachelor's degree in computer science.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining how to document high-level risks.

Table 32. Module: Document high-level risks, including threats, incidents, and assets using high-level risk table (B-03-M-01)

5.3.4 Identify risks, level 1

The purpose of this course is to teach the basic usage of the CORAS modelling language to identify and document cyber-risks. The course provides hands-on training in identifying cybersecurity risks by simulating a target of analysis exposed to certain cyber-attacks. The participant will, amongst other activities, look for possible attacks by observing the simulation and document these attacks using the CORAS modelling language.

ID	B-04
Name	Identify risks, level 1
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 2, Level 3. • R3 – Skill B2, Level 2, Level 3. • R4 – Skill B1, Level 2, Level 3. • R5 – Skill B1, Level 2, Level 3.
Offering Level	Basic
Difficulty	Medium/Hard
Course Duration	90 minutes (two modules, 45 minutes each module)
Learning Goals	It is expected that by the end of this course, participants in this course will:

ID	B-04
	1. Understand how to apply the CORAS modelling language to identify risks. 2. Demonstrate the application of the CORAS risk modelling language by identifying appropriate risks with respect to a target of analysis simulated on the cyber range.
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. Understand the basics of the CORAS risk modelling language. 2. Identify risks, including threat source, threats, vulnerabilities, incidents, and security assets to protect, with respect to a target of analysis simulated on the cyber range.
Prerequisites	Complete the Courses P-01, P-02, B-02 and B-03. Basic knowledge within but not limited to a bachelor's degree in computer science.
Module list	• B-04-M-01: Introduction to CORAS • B-04-M-02: Identify risks using the CORAS risk modelling language with respect to simulated scenarios

Table 33. Course: Identify risks, level 1 (B-04)

The course has two modules to achieve the learning objectives. The first module introduces the CORAS risk modelling language and its basic usage (see Table 34), while the second module focuses on hands-on training of risk identification (see Table 35).

ID	B-04-M-01; Accompanying slide set number: 11
Name	Introduction to CORAS
Learning Objectives	It is expected that by the end of this module, participants will be able to: 1. Understand the basic constructs of the CORAS modelling language. 2. Associate cyber-risk concepts to the constructs of CORAS.
Module Duration	45 minutes
Prerequisites	Complete the Courses P-01, P-02, B-02 and B-03. Basic knowledge within but not limited to a bachelor's degree in computer science.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining the basics of the CORAS modelling language.

Table 34. Module: Introduction to CORAS (B-04-M-01)

ID	B-04-M-02; Accompanying slide set number: 11
Name	Identify risks using the CORAS risk modelling language with respect to simulated scenarios
Learning Objective	It is expected that by the end of this module, participants will be able to: Create basic risk models using the CORAS constructs: Threat source, Threat, Vulnerability, Unwanted incident, and Asset with respect to simulated scenarios.
Module Duration	45 min.
Prerequisites	Complete the Courses P-01, P-02, B-02 and B-03. Basic knowledge within but not limited to a bachelor's degree in computer science.
Content list	Literature (in the form of PowerPoint presentation and supporting text) explaining how to step-by-step create a CORAS risk model.

Table 35. Module: Identify risks using the CORAS risk modelling language (B-04-M-02)

5.3.5 Awareness of Password Weakness with hands-on training

This course is an extended version of the Course P-03 (Awareness of Password Weaknesses). In addition to what is covered in P-03, this course provides hands-on training in demonstrating how weak passwords are exploited.

ID	B-05; Accompanying slide set number: 12
Name	Awareness of Password Weaknesses with hands-on training
Cybersecurity role	R2, R3, R4, R5
Skill and expected skill level to be trained	• R2 – Skill B2, Level 2. • R3 – Skill B2, Level 2. • R4 – Skill B1, Level 2. • R5 – Skill B1, Level 2.
Offering Level	Basic
Difficulty	Easy
Course Duration	45 minutes
Learning Goals	It is expected that by the end of this course, participants in this course will: 1. Understand the use of passwords for authentication 2. Understand the risks associated with weak passwords 3. Remember password best practices
Learning Objectives	To determine whether the participants have achieved the learning outcomes, it is expected that participants, by the end of the course, will be able to: 1. For Learning Goal 1: a. Understand why a strong password is important b. Explain the need of different passwords for the various systems 2. For Learning Goal 2: a. List factors that make a password weak b. List different attacks exploring password weakness c. Explain the need to change a default password d. Describe different actions of an attacker with a password 3. For Learning Goal 3: a. List different guidelines for creating a strong password b. Identify password bad practices c. List mechanisms for password management
Prerequisites	Basic knowledge of windows and Linux systems operations.
Module list	None

Table 36. Course: Awareness of Password Weaknesses with hands-on training (B-05)

5.4 The usage environment of the courses

The following sections provide a high-level explanation of two main usage areas of the CYBERWISER.eu courses, namely using the courses for self-study and using the courses for classroom lectures.

5.4.1 Applying the courses for self-study

The Cross-Learning Facilities will allow CYBERWISER.eu to create standalone independent study courses to be used by trainees.

Given the online nature of the Cross-Learning Facilities, they can provide a high degree of flexibility for trainees who can study at any time and in any location, without the direct interaction with a teacher.

For this reason, the Cross-Learning Facilities also offer tools to help students in their learning path such as progress tracker to help them know where they stand in a course, and different evaluation mechanisms such as tests and quizzes to keep the students engaged and motivated.

All courses in CYBERWISER.eu will be accompanied by:

- A set of PowerPoint slides.
- Supporting audio for each slide (implemented in Moodle).
- Accompanying literature including references to external sources/literature.
- Questions/quiz during the course.
- Questions/quiz exam at the end of the course.

Some of the courses will also have associated training scenarios on the cyber range. Thus, the courses in CYBERWISER.eu are very well supported and organized for self-study.

5.4.2 Applying the courses for classroom lectures

Topics presented during classroom lectures should be atomic as much as possible. This means that each theoretical topic should be started and completed by the end of the lecture, if possible. When a topic is not fully explained during the same lecture, it would be hard to directly start by continuing from the stopping point of the previous lecture, a recap is always necessary. This will usually take time and should be avoided.

The trainer should be supported by a set of slides, previously distributed to trainees. Giving them before the lecture starts let them the time to be confident with this initial training material. Slides are also useful to keep trainees' attention at an acceptable level. Slides presented during the lecture should be furnished with additional materials (e.g. booklets or lecture notes) provided by the trainer by the end of the lecture. This additional material will contain all the details which cannot be added to the slides. This will also answer to most of trainees' doubts, which may raise after the lecture ends.

An import point, when conducting a classroom lecture, is the alternation between theoretical topics and practical implications. Trainees usually lose attention when lectures are only focused to theoretical part. In order to gain back their attention, it is important the Trainer shows how the theoretical concepts can be applied in practice. This can be done by the mean of the CYBERWISER.eu platform, if a corresponding scenario is available for the course.

Before starting each classroom lecture, it is important to have a Q/A session with trainees. This will let them ask questions regarding topics explained during the previous lecture. Having all clear will let them be more focused on new topics. The same applies for the last part of each classroom lecture, it should be used for a Q/A session about topics explained during the same day.

Courses, when provided in the form of classroom lecture, should be furnished with interactive questionnaire, to keep trainees attention higher. At some point during the lecture and at the end of it, trainer should ask trainees to answer a brief questionnaire about the topics explained. This questionnaire should be anonymous, as the focus is not to give trainees a grade, but to check the overall learning level. This can be helpful also to the trainer, who can react accordingly.

6. Accessing and editing training material in the platform

This section describes how the training material (including the courses) are accessed and edited in the CYBERWISER.eu platform. This includes logging into the CYBERWISER.eu platform, accessing the courses from a student/trainee perspective, overview of the training path section, editing the courses from a teacher/trainer perspective, overview of interactive and engagement features in the platform, and finally a section explaining the soft skill addressed by CYBERWISER.eu.

6.1 Logging into the CYBERWISER.eu Platform

The Workspace is the interface where trainers and trainees find the training courses. Each group of Pilot users has a dedicated Workspace that can be accessed via the CYBERWISER.eu website Login/Registration form with Single Sign On (Figure 12).

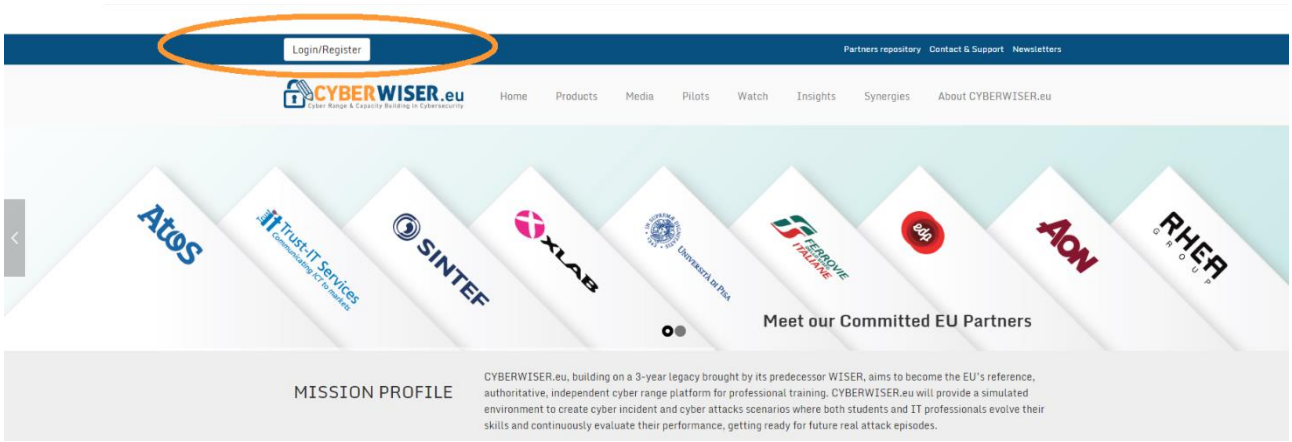


Figure 12. Login/Register in the Home Page to be able to access the Workspace

6.2 Accessing the courses – From a student perspective

After accessing the CYBERWISER.eu website, the student can enter the Workspace by clicking the “Cross Learning Facilities” button on the top left of the screen (Figure 13):

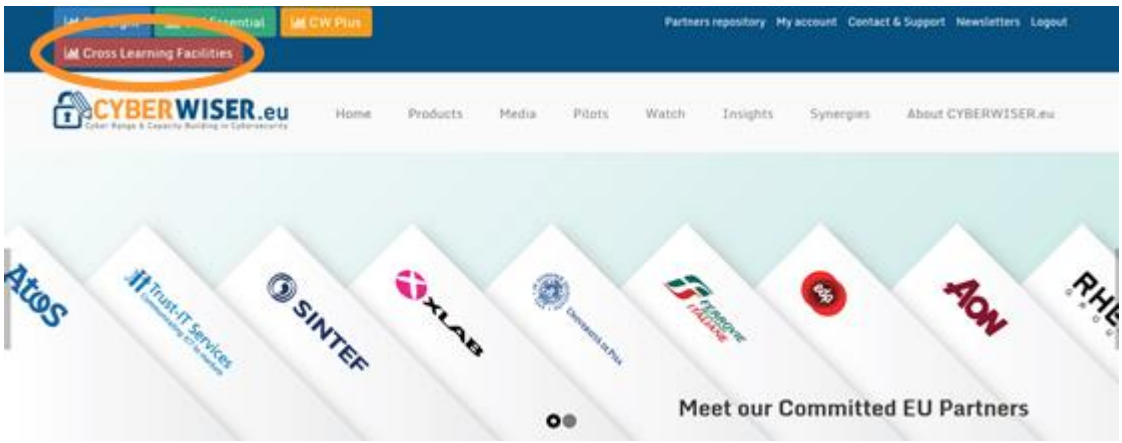


Figure 13. Click on “Cross Learning facilities” to enter the Workspace after the Login/Registration

In the example below, the user is part of the FFSS pilot. Within the workspace, the student can enter his/her “Group Area”, by either clicking on the Pilot’s name or on the “Continue Reading” button (Figure 14). This procedure is the same whether the user is part of a Pilot (Full-Scale or Open) or is a customer.

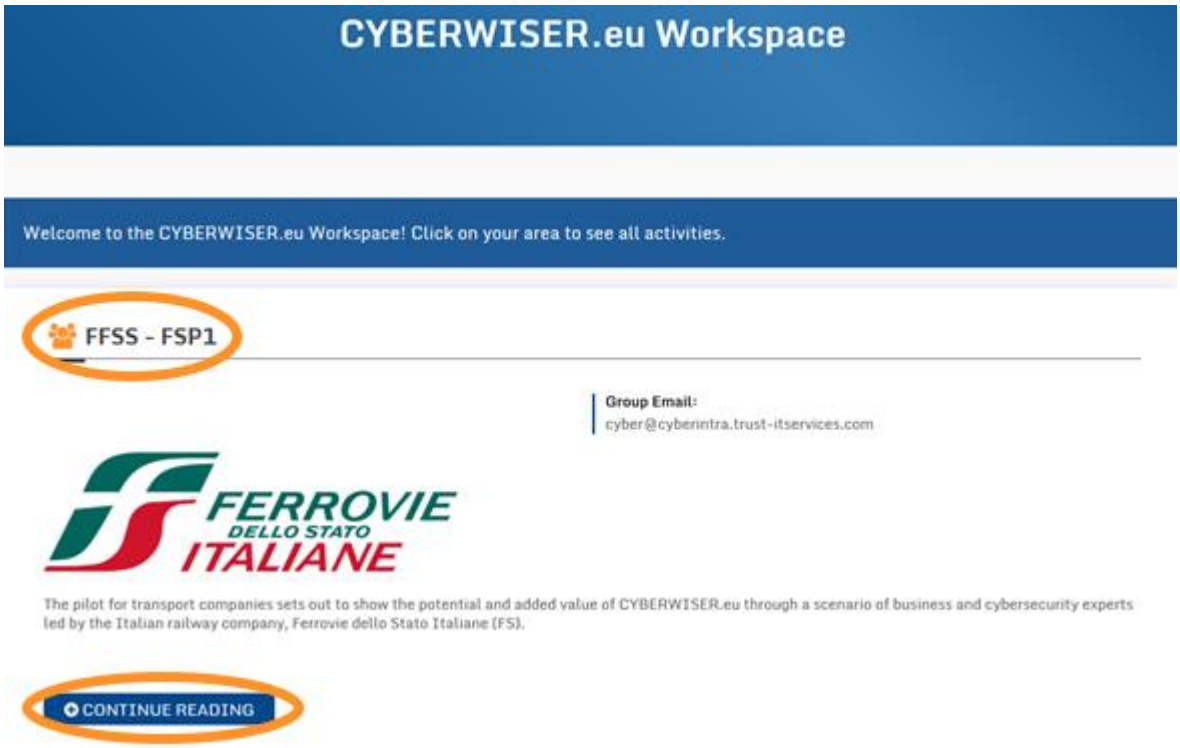


Figure 14. Click on the highlighted buttons to enter the “Group Area” within the Workspace

Inside her/his group’s area, the student can access the following sections, by simply clicking on them (Figure 15):

- Group’s details: a brief description of the Group the user is part of.
- My Training Path: Courses Overview where the student can choose between different course level; this section is described in detail in the paragraph 6.2.1.
- File Repository: repository containing any downloadable material.
- Group Contact Email (mails sent to this address will be delivered to all the members of a Group).
- Unsubscribe button.
- Add new content: users can post to the Group Mailing List and/or Add a Group Event. All members of a group will receive a mail notification each time a post is published.
- List of the Pilot’s members.
- Recent Activity: search bar allowing research by Type of activity, keywork or Surname.
- Posts Section where all existing posts are displayed.

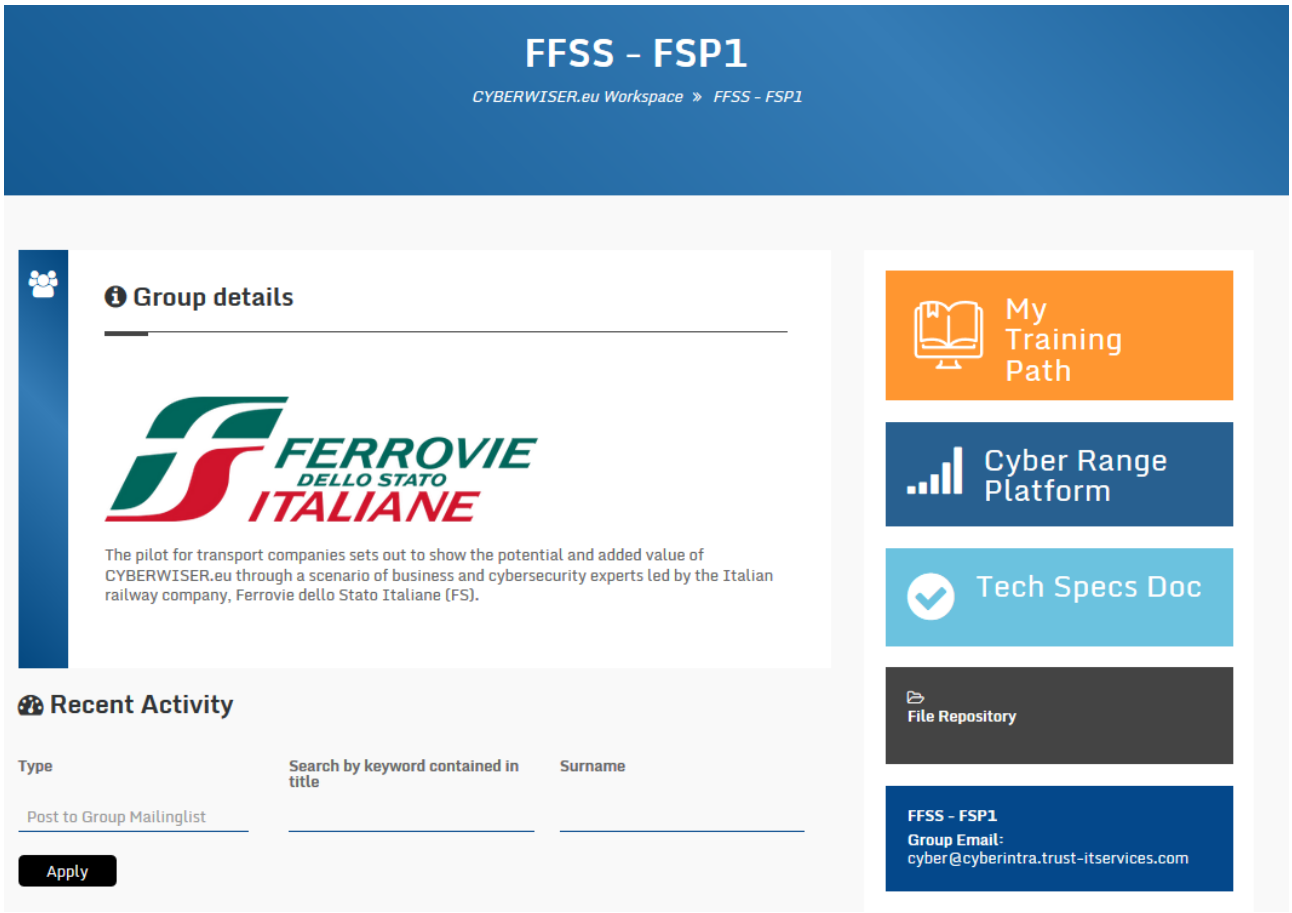


Figure 15. Sections of the “Group Area” within the Workspace

6.2.1 My Training Path section

The “My Training Path” section (Figure 16) contains the different Offering Level (Primer, Basic, Intermediate and Advanced) available for the specific Pilot or customer. The student can access the relative Offering Level, by clicking on it.

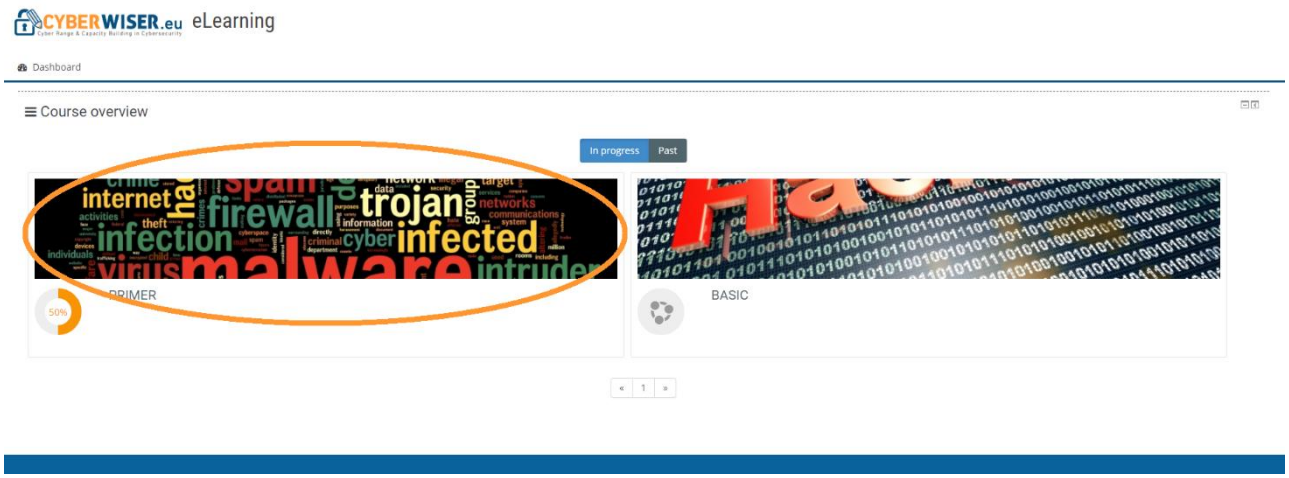


Figure 16. Inside the “My Training Path”, click on an Offering Level to access it.

Each Offering Level is made up of various courses, one or more quizzes (or exercises) and a certification page (figure 16).

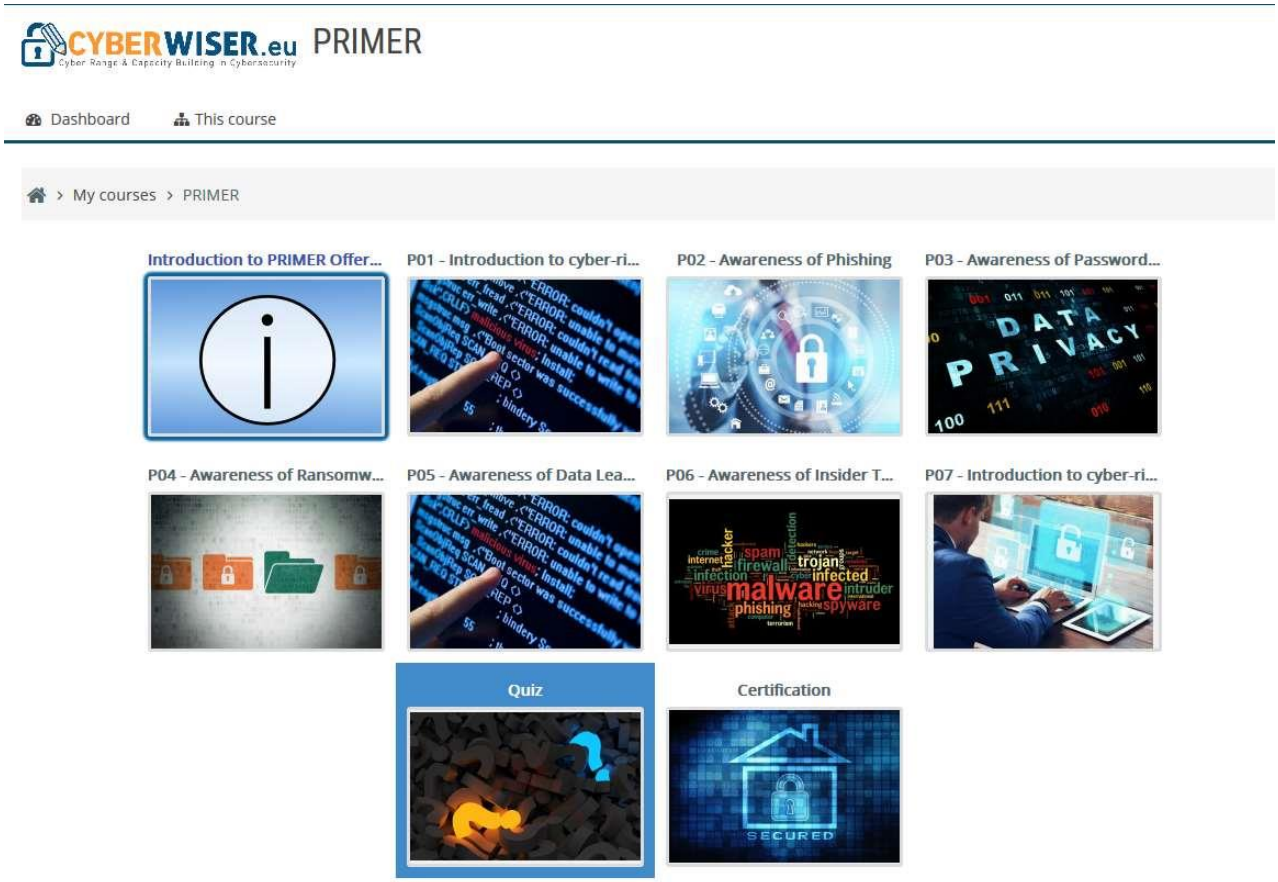


Figure 17. Sections of the course level “PRIMER”

When all the courses and quizzes (or exercises) are completed, a certificate will be issued to the student. The student can enter a course, by clicking on it. Each course can be made up of one or more modules (Figure 17).

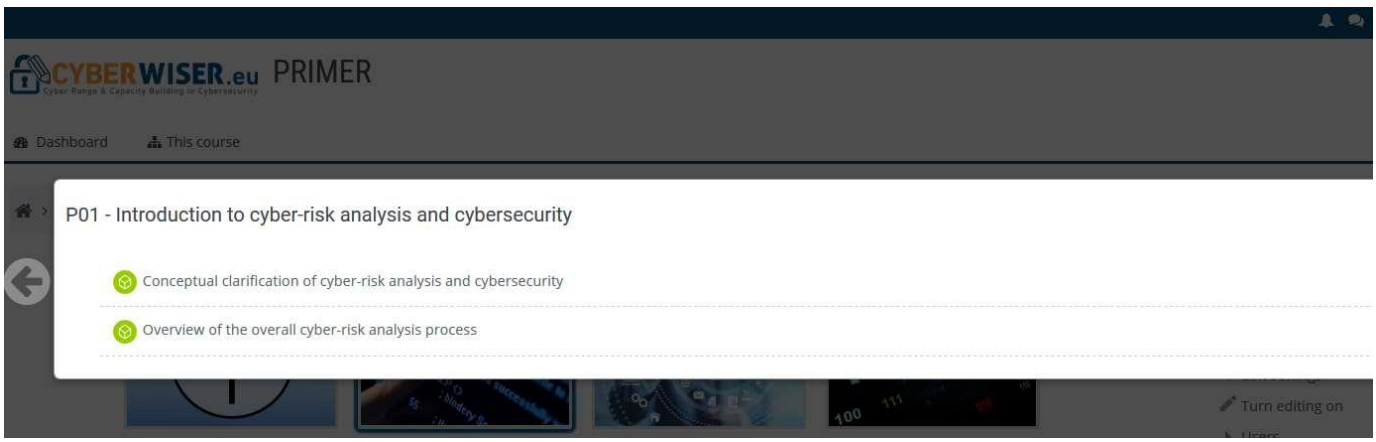


Figure 18. Modules of the first section of the PRIMER course

Each module can be made up of a “Training path” (Figure 18).

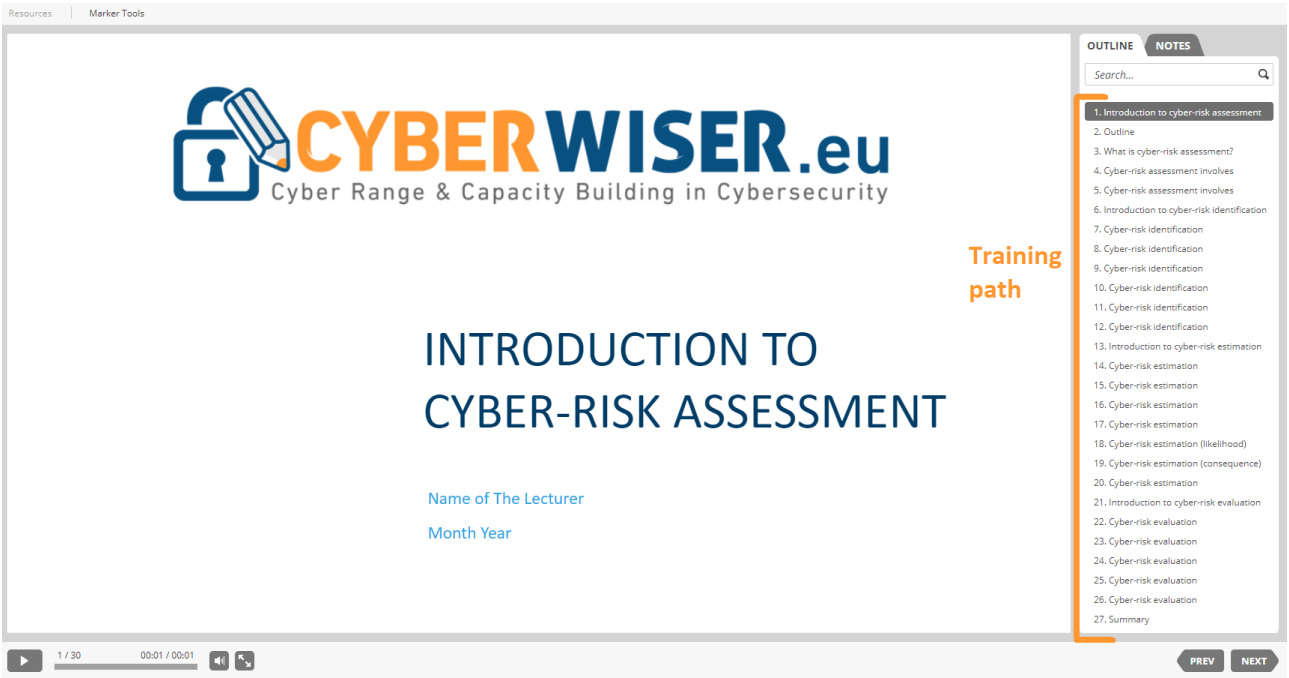


Figure 19. Training Path of the first module

Each Training Path can be composed by several SCORM files that contains a combination of one or more of the following elements (Figure 19):

- Power Point Presentation.
- Video.
- Training Class.
- Webinar.
- Cyber Range Tool Session, available starting from the Basic level, through a link to the Cyber Range Platform.
- Evaluation test.

Each element in the Training Path is available progressively only when the preceding one has been completed. A time indicator ensures that the student does not skip any element.

The workflow analysed so far refers to the initial version of the training platform as developed in its early stage. The platform is subject to continuous improvement and elaboration and any change will be discussed in the following versions of this deliverable.

6.3 Editing the courses – From a teacher perspective

The teacher can access the CYBERWISER.eu platform in the same exact way of a student as reported in section 6.1. The interface for the teacher is very similar to the one for the students but it allows the teacher to have more functionalities. After selecting an Offering Level, the teacher can access the editing functionalities by clicking on the “administrative” menu in the right corner of the page:

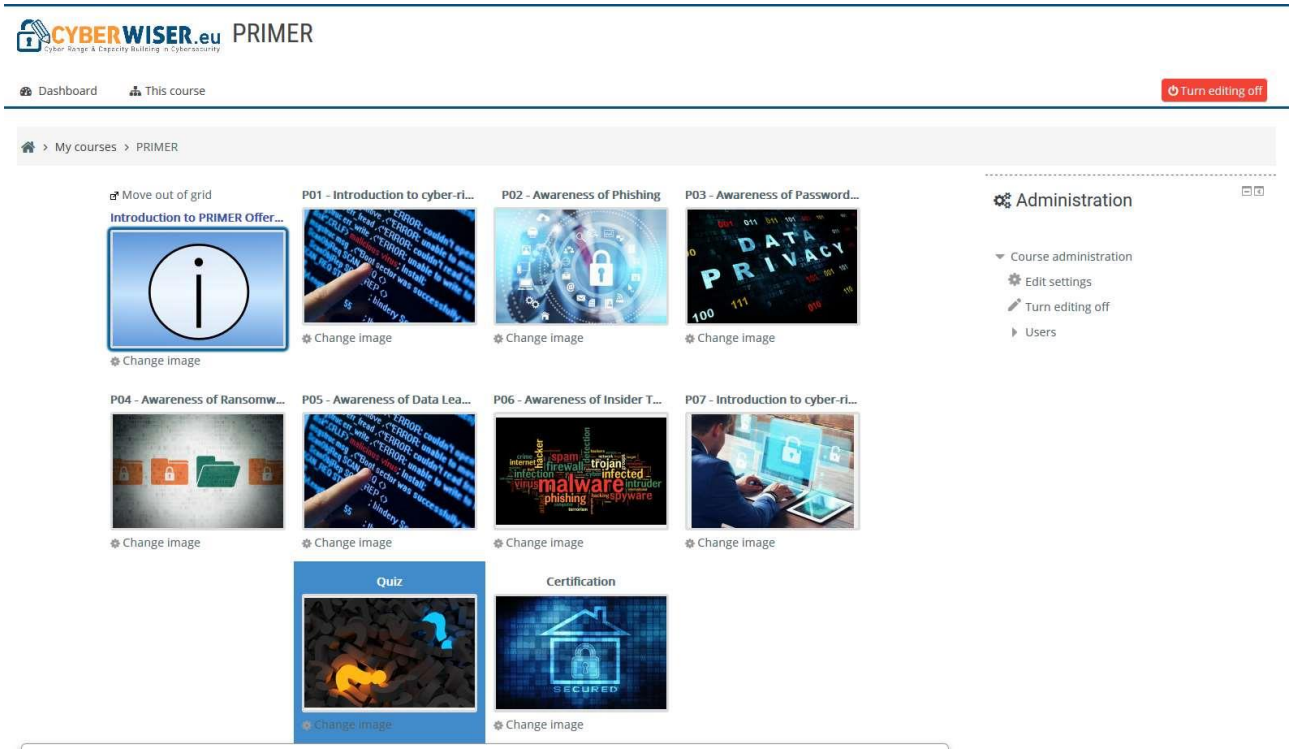


Figure 20. Administrative menu example

Every aspect of each course is customizable, spanning from titles of each course, images, course description etc. Inside each course, the teacher can add specific activities spanning from a different range of resources as shown in the figure below:

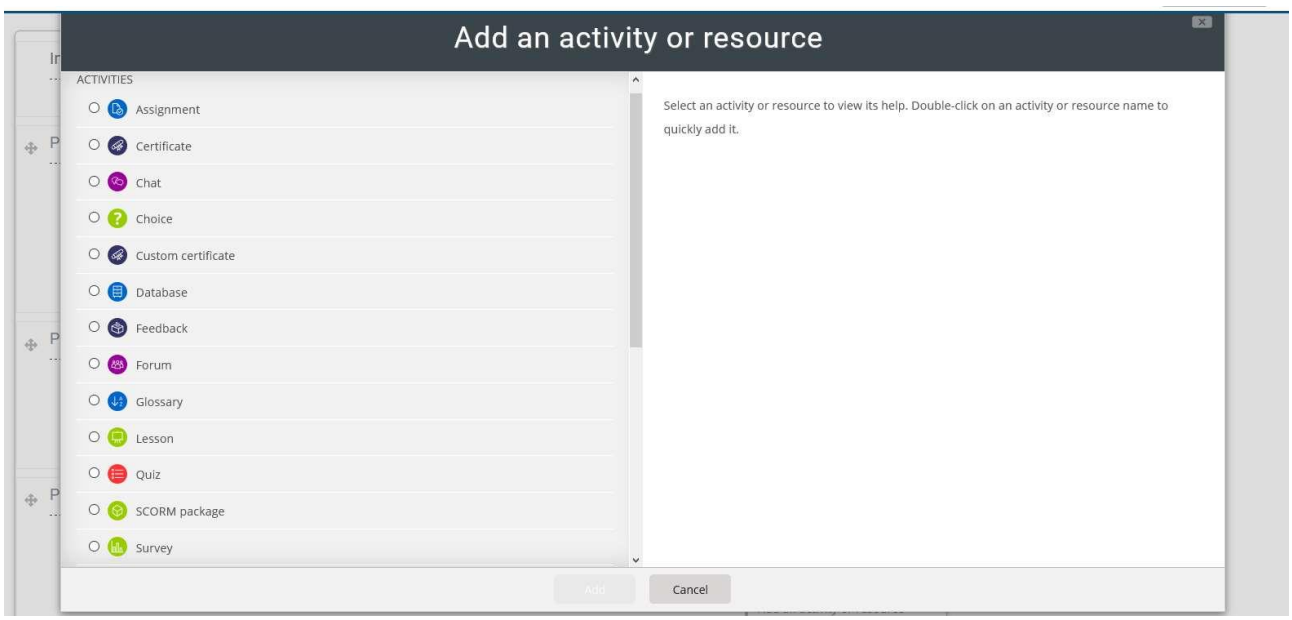


Figure 21. Activities to be selected by a teacher

Typically, a teacher will add SCORM files that can contain a combination of different elements (as already explained in section 6.2) but will be also able to customise courses thanks to an archive of resources.

Thanks to the “administrative” menu, the teacher can clearly see the students that are taking each course and also track their progress for each course as shown in the figure below:

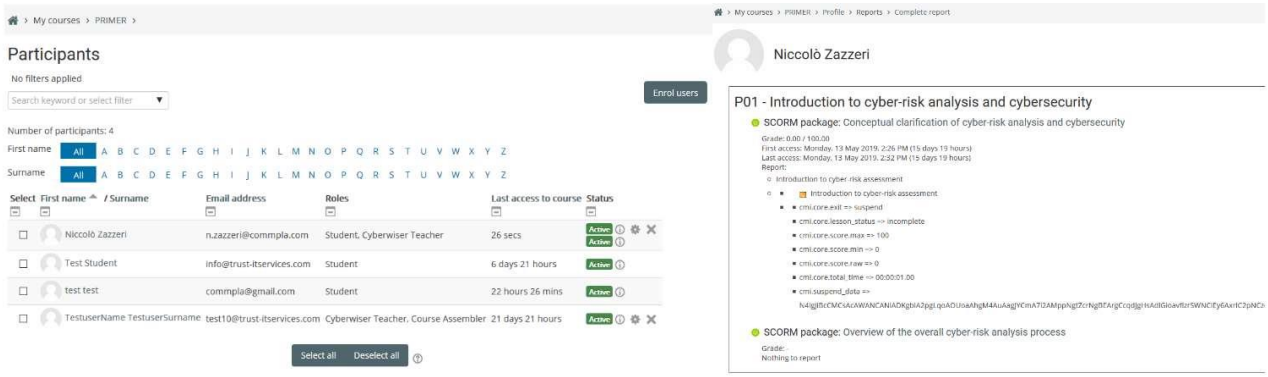


Figure 22. Example of students monitoring

6.4 Interactive and engagement features

A series of features have been added to the training path in order to increase interactivity and engagement with the trainees.

These include mainly videos helping trainees to increase their learning motivation and quizzes that are presented to the trainees at the end of each module to test the gained knowledge. Some examples are reported below.

Videos/Webinars - Video is one of the most effective ways to keep trainees engaged and interested. Within the platform this kind of multimedia can be used in different ways:

- as simple how-to videos on how to deploy scenarios, or how to run an exercise in the cyber range
- as live lectures in the form of webinars on a specific topic
- as catalogue of additional resources coming from external, reputable providers

Figure 23. Video example

Multiple choice - The trainee must choose from multiple answers based on a certain question. Two types of multiple choice are available - single answer (where there is only one correct answer) and multiple answer (where the trainee can pick all answers that apply). After submitting the answer, a message is shown to the trainee.

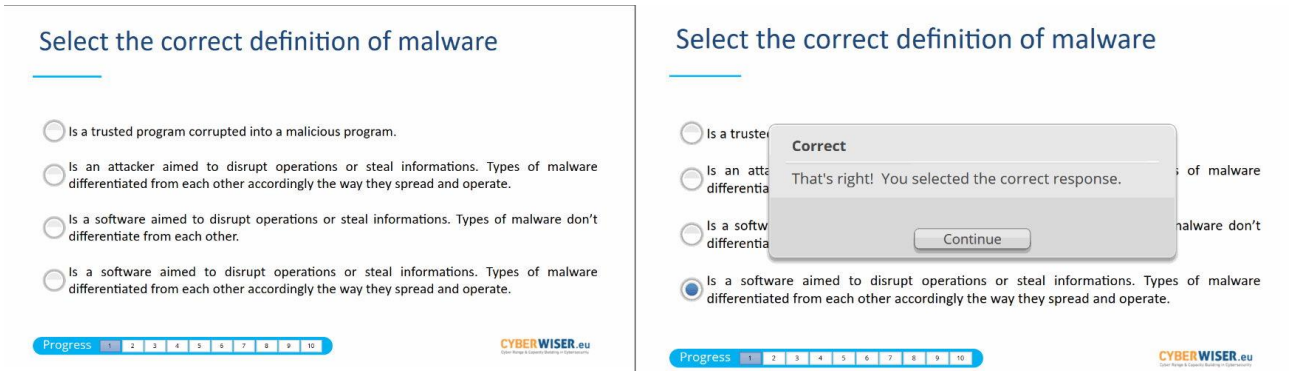


Figure 24. Multiple choice answers

True/False – The trainee must choose either True or False based on a certain question, which could be either a text-based or an image-based question. After submitting the answer, a message is shown to the trainee.

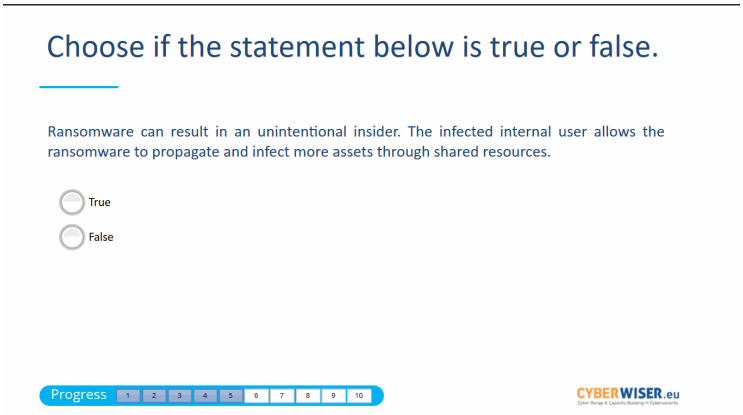


Figure 25. True/false answers

Embedded answers – This allows the use of multiple different question types within a single question. After submitting the answer, a message is shown to the trainee.

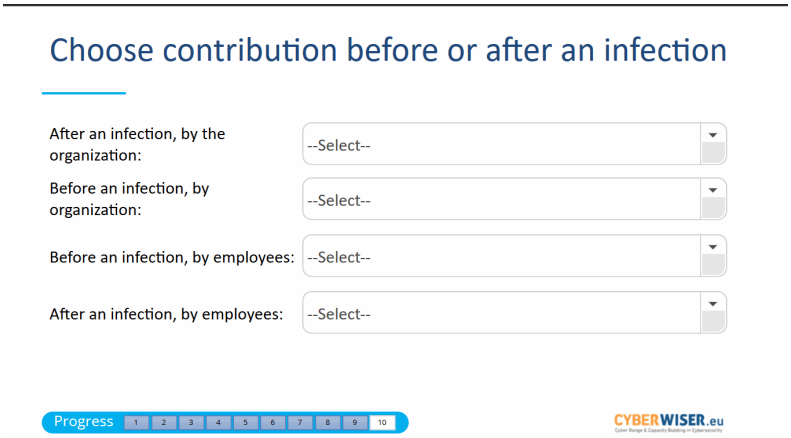


Figure 26. Embedded answers

Matching - The trainee must match a set of questions/statements against answers/other statements. This includes a drag and drop interface for the trainee. After submitting the answer, a message is shown to the trainee.

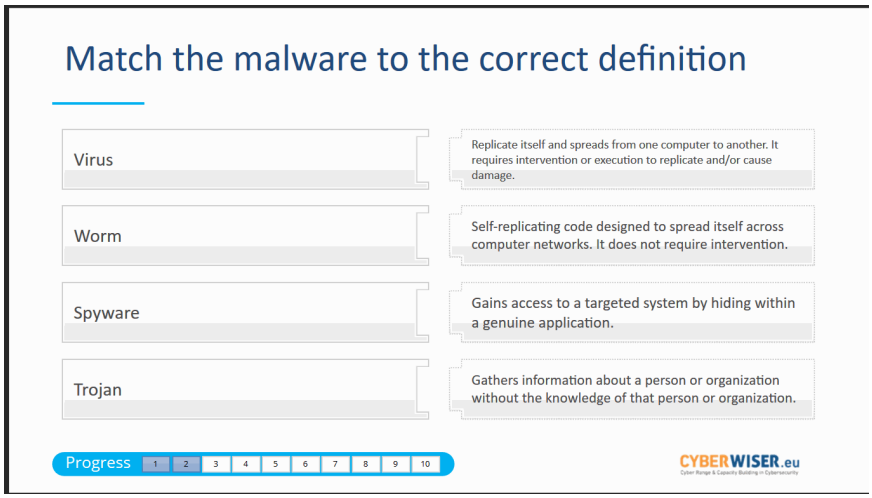


Figure 27. Matching

When a trainee successfully completes a test, the system automatically notifies this to him together with its scoring based on the answers given. A trainee that successfully complete an entire learning path is also automatically given a personalised certification.

Figure 28. Automatic certification

6.5 Developing soft skills using the CYBERWISER.eu Platform

As mentioned in Section 3.3.1, the explicit training of soft skills (courses teaching about e.g. communication) is outside the scope of CYBERWISER.eu. However, by taking courses offered on the CYBERWISER.eu Platform, students can also benefit from and develop a range of general soft skills mainly in terms of "J3 – Communication and Knowledge Sharing" outlined in Table 6. Table 37 describes in detail the soft skill Communication and Knowledge Sharing. This soft skill has 6 advancement levels according to CIISec Skills Framework [24]. In the context of CYBERWISER.eu, however, we select the first four skill levels as relevant to trainees that use the CYBERWISER.eu platform (see Table 37) because Skill Levels 5 and 6 are required by already experts with high level of autonomy and very little oversight from others [24].

Skill	Principles	Example Skills
J3 – Communication and Knowledge Sharing	Communicates information clearly and in a manner relevant to the target audience. Influences senior management. Shares knowledge on Information Security. Negotiates effectively on Information Security issues.	**Level 1**: Understands and interprets instructions effectively. Communicates effectively with colleagues.
		Level 2: Has clear written and verbal communication skills. Shares information and knowledge with others.
		Level 3: Is sensitive and constructive when challenging other's ideas or decisions.
		Level 4: Proactively shares good practice and expertise with colleagues. Contributes effectively to debates and complex discussion demonstrating well-reasoned arguments and conclusions. Adapts communication style to suit audience, developing effective mechanisms to disseminate information to colleagues.
		Level 5: Is a persuasive communicator using logic to win support and change views. Sets a lead in sharing knowledge across the organisation and uses a variety of effective strategies to capture and share information. Addresses and discusses key concerns and ensures key stakeholders are kept informed.
		Level 6: Is persuasive and diplomatic in external negotiation, influencing major programmes, projects or policy outside of the organisation. Uses and develops knowledge sharing strategies to share experience across organisations. Presents effectively and influentially to a range of audiences.

Table 37. Description of soft skill Communication and Knowledge Sharing

For example, trainees in the Cross-Learning Facilities can benefit of a simple and intuitive channel to communicate with each other and with the teachers where they can exchange experience, problems and solutions.

Furthermore, trainees can come from very different backgrounds, therefore reflecting an almost real-case scenario in which cybersecurity must be communicated to every level of the organisation, not only the technical or IT staff.

Collaboration and teamwork could also be improved by means of the actual cyber range environment in CYBERWISER.eu, in which trainees will be able to play the role of attackers (red team) and/or defenders (blue team) in different scalable and configurable scenarios.

A trainee's advancement in these soft skills are clearly subjective, situational and most importantly highly dependent on how an organisation is structured and working. It is therefore difficult to measure the performance of the considered soft skill in a dynamic manner as for the technical skills described in Section 3.3 based on the evaluation criteria documented in Deliverable D4.2. Thus, in the context of CYBERWISER.eu, the soft skills need to be measured by a trainer/teacher as part of the Performance Evaluator in which the trainer/teacher comments on how well a trainee has performed based on observations done by the trainer/teacher.

Based on the courses currently available in CYBERWISER.eu documented in Section 5 (including supporting training material), the levels of advancement anticipated to be developed in skill J3 are:

- Level 1: Understands and interprets instructions effectively. Communicates effectively with colleagues.
- Level 2: Has clear written and verbal communication skills. Shares information and knowledge with others.

The next courses to be developed and made available at the Intermediate and Advanced offering levels will require more interactivity, collaboration (e.g. red team/blue team), and communication, and therefore develop further skill J3 to levels 3 and 4. However, this will be clear when developing the next courses in Deliverable D4.4 Training material final version.

7. Conclusions

This deliverable presents the initial version of the training material provided in CYBERWISER.eu. This deliverable describes our systematic approach to develop the curriculum, courses including course templates, as well as the training material. The method consists of four main steps:

- Step 1: Identify target-user roles and skills to be trained via CYBERWISER.eu
- Step 2: Map the roles and their expected skills to the learning path of CYBERWISER.eu
- Step 3: Describe courses using predefined templates
- Step 4: Develop training material for the courses

The target-user roles considered are Head of Information/Cyber Security, Information Security Risk Manager, Information Security Risk Officer, Threat Analyst, and Vulnerability Assessment Analyst. The selected relevant skills associated with these roles are Threat Intelligence, Assessment and Threat Modelling, Risk Assessment, and Information Risk Management. The abovementioned roles are related to appropriate parts of the learning path in which one or more of the skills are requires. The learning path consists of four main parts:

- Cybersecurity and risk awareness
- Context establishment
- Cyber-risk assessment
- Cyber-risk treatment and cost/benefit analysis

The learning path is carefully constructed to be in line with ISO 27001 [9] and ISO 27005 [10], which are security standards known globally and used both in industry and academia.

Using the above method this deliverable provides initial versions of 12 courses for the Primer and Basic offering levels of CYBERWISER.eu.

Finally, the deliverable outlines how the training material should be accessed and edited within the CYBERWISER.eu Platform (the Cross-Learning Facilities).

As next step, we will develop courses that will be available for the Intermediate and Advanced offering levels of CYBERWISER.eu. The courses and supporting training material (literature, questionnaires, training scenarios in the cyber range, etc.) will be developed following the method described in this report.

References

[1] Phishing.org. http://www.phishing.org/what-is-phishing – Accessed: 21.03.2019.
[2] European Union Agency for Cybersecurity (ENISA). Threat landscape tool by ENISA. https://etl.enisa.europa.eu/#/ - Accessed: 21.03.2019.
[3] Symantec. Internet Security Threat Report, Volume 24, February 2019. https://www.symantec.com/security-center/threat-report – Accessed: 21.03.2019.
[4] WatchGuard. Internet Security Report, Q4 2018. https://www.watchguard.com/wgrd-resource-center/security-report-q4-2018 – Accessed: 21.03.2019.
[5] The Open Web Application Security Project (OWASP). OWASP Top Ten Project. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project – Accessed 21.03.2019.
[6] European Commission. General Data Protection Regulation. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en – Accessed: 21.03.2019
[7] European Union Agency for Cybersecurity (ENISA). The cost of incidents affecting CIIs. Published August 5, 2016. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis – Accessed: 21.03.2019.
[8] CA Technologies. Insider Threat 2018 Report. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf – Accessed: 21.03.2019.
[9] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements (2013).
[10] ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011).
[11] M.S. Lund, B. Solhaug, K. Stølen. Model-driven risk analysis – The CORAS approach. Springer (2011).
[12] A. Refsdal, B. Solhaug, K. Stølen. Cyber-risk management. Springer (2015).
[13] Object Management Group (OMG). Unified Modelling Language (UML) v2.5.1, Published December 2017.
[14] K. Beckers. Pattern and Security Requirements – Engineering-Based Establishment of Security Standards. Springer (2015).
[15] Anderson LW, Krathwohl DR, Airasian PW, Cruikshank KA, Mayer RE, Pintrich PR, Raths J, Wittrock MC. A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives, abridged edition. White Plains, NY: Longman. 2001.
[16] Wikipedia. Bloom's taxonomy. https://en.wikipedia.org/wiki/Bloom%27s_taxonomy – Accessed 29.03.2019.
[17] The SANS Institute. https://www.sans.org/about/ - Accessed 01.04.2019.
[18] European Cyber Security Organization. Energy Networks and Smart Grids – Cyber security for the energy sector. WG3 Sectoral Demand. November 2018. https://ecs-org.eu/documents/publications/5bfc08317f722.pdf – Accessed: 04.04.2019.
[19] Digital Guardian. A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. January 3, 2019. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time – Accessed: 04.04.2019.
[20] Malwarebytes. Cybercrime tactics and techniques Q1 2017. https:\www.malwarebytes.com\pdf\labs\Cybercrime-Tactics-and-Techniques-Q1-2017.pdf – Accessed: 04.04.2019.
[21] CYBERWISER.eu Project. D2.3 Platform Design. Initial Version. February 2019
[22] CYBERWISER.eu Project. D6.1 Communication & Stakeholder plan first version. December 2018
[23] Chartered Institute of Information Security. CIISec Roles Framework, Version 0.3, November 2019. https://www.ciisec.org/ - Accessed 28.01.2020.
[24] Chartered Institute of Information Security. CIISec Skills Framework, Version 2.4, November 2019. https://www.ciisec.org/ - Accessed 28.01.2020.
[25] The MITRE Corporation. https://www.mitre.org/ - Accessed 28.01.2020.
[26] The Open Web Application Security Project (OWASP). https://owasp.org/ - Accessed 28.01.2020.

[27] CREST - an international not-for-profit accreditation and certification body that represents and supports the technical information security market. https://www.crest-approved.org/index.html - Accessed 28.01.2020.
[28] The International Information System Security Certification Consortium. https://www.isc2.org/ - Accessed 28.01.2020.
[29] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf - Accessed 29.01.2020.
[30] European Cyber Security Organization (ECSO). https://ecs-org.eu/ - Accessed 10.02.2020.
[31] Wide-Impact cyber Security Risk framework (WISER). D3.2 - Cyber risk modelling language and guidelines, preliminary version. https://www.cyberwiser.eu/content/d32-cyber-risk-modelling-language-and-guidelines-preliminary-version – Accessed 10.02.2020.
[32] Wide-Impact cyber Security Risk framework (WISER). D3.4 - Cyber risk modelling language and guidelines, final version. https://www.cyberwiser.eu/content/d34-cyber-risk-modelling-language-and-guidelines-final-version – Accessed 10.02.2020.
[33] European Commission. Research Executive Agency. Grant Agreement Number 786668 – CYBERWISER.eu.