



Digital4Security

Shaping Europe's cyber future

Interim D3.2 Ready-to-Use Online Training Materials

Create of a suite of Ready-to-Use online Training Materials for the delivery of the online Masters.

Table of Contents

About the Digital4Security project	4
Document Control Information	7
Introduction	8
Objectives of Interim Deliverable 3.2.....	9
Importance of Ready-to-Use Online Training Materials.....	10
Overview of Learning Materials	11
Role of Online Learning Materials	11
Advantages of Online Training Materials.....	12
Ready-to-Use Online Training Materials for Flexible Learning	14
Structure and Design of Modules.....	15
Framework for Module Development	15
Key Guidelines Used for Designing Moodle Modules	17
II. Consistency Across Modules.....	17
III. Learner-Centered Design	22
IV. Interactive Tools.....	22
V. Accessibility.....	23
VI. Visual Cues and Navigation.....	23
VII. Completion Tracking.....	23
Moodle & Ready-to-Use Online Training Material	24
Moodle framework.....	26
Instructional Design of Ready-to-Use Online Training Materials	27
Key Considerations for Designing Online Content for Adult Learners in a European Masters Programme	29
Demonstration of Ready-to-Use Materials	31
Roles in development of Ready-to-Use Online Training Material and Process	32
Sustainability and Future Updates	34
Appendices.....	36
A. References and Bibliography	36

B.	List of Modules and Descriptions	38
C.	Technical Specifications of Moodle Setup	43
D.	Accessibility and Compliance Reports.....	44

About the Digital4Security project

Digital4Security is as a ground-breaking pan-European master's Programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. With funding of almost 20 million euros from the European Union, this four-year initiative has garnered support from a Consortium comprising 35 partners spanning 14 countries. This industry-driven Programme will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

WP3 is responsible for the Programme development and setup. This document represents an interim version of Deliverable 3.2: Ready-to-Use Online Training Materials. An interim report serves as a progress update, providing insight into the development process, and the framework established for the final deliverable. This interim deliverable outlines the methodology, structure, and key guidelines applied in the creation of the Ready-to-Use Online Training Materials, designed to support the delivery of the online Master's Programme.

As the Digital4Security project continues to evolve, the document demonstrates the foundational work completed thus far, including the integration of sample content, a Demo module, and initial materials for five modules covering Week 1. By leveraging the latest authoring tools and cutting-edge technologies, the interim deliverable ensures that a robust structure is in place to facilitate the development of a highly engaging and interactive learning experience for all participants.

Additionally, this report includes links and credentials to the Moodle Digital Learning Platform, offering reviewers the opportunity to explore the module designs, interactive elements, and overall framework. It is important to note that the platform's content is being updated almost daily. The five modules currently containing content for Week 1 reflect the state of progress as of November 27, 2024, showcasing the ongoing effort to populate the materials.

The Ready-to-Use Online Training Materials framework has been developed and integrated into Moodle, which serves as the central hub for organizing, delivering, and managing these materials. Moodle offers an intuitive and user-friendly interface for learners and instructors alike. The development process is guided by a detailed roadmap, with academic partners currently drafting module content. Profil Klett ensures the seamless integration of finalized content into Moodle, adhering to the standardized structure, creating interactive elements, and applying the design guidelines outlined in this document.

It is important to note that the actual module content is still under development by the academic partners. Once finalized, this content will be uploaded into the Moodle platform to ensure seamless access and an adaptive learning environment. The target completion date for all materials is June 2025, ensuring the Programme is fully prepared for implementation. Updates will also be made in Year 3 of the project as part of the T2.6 Curriculum Review & Update, ensuring ongoing relevance and alignment with the latest technological and pedagogical advancements.

The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management Programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

No.	Role	Short name	Partner	Country
1	COO	POLITEHNICA BUCHAREST	NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST	RO
2	BEN	SA	SCHUMAN ASSOCIATES SCRL	BE
3	BEN	Ataya	ATAYA & PARTNERS	BE
4	BEN	POLIMI	POLITECNICO DI MILANO	IT
5	BEN	CMIP	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	PL
6	BEN	Contrader	CONTRADER SRL	IT
7	BEN	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE
8	BEN	indiepics	INDEPENDENT PICTURES LIMITED	IE
9	BEN	MATRIX	MATRIX INTERNET APPLICATIONS LIMITED	IE
10	BEN	PROFIL KLETT	PROFIL KLETT D.O.O.	HR
11	BEN	ServiceNow	SERVICENOW IRELAND LIMITED	IE
12	BEN	UNIBS	UNIVERSITA DEGLI STUDI DI BRESCIA	IT
13	BEN	UDS	UNIVERSITY OF DIGITAL SCIENCE GGMBH	DE
14	BEN	SKILLNET	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	IE
15	BEN	IT@CORK	IT@CORK ASSOCIATION LIMITED LBG	IE
16	BEN	ADECCO TRAINING	ADECCO FORMAZIONE SRL	IT
17	BEN	UNI KO	UNIVERSITAT KOBLENZ	DE

18	BEN	BRNO UNIVERSITY	VYSOKE UCENI TECHNICKE V BRNE	CZ
19	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE
20	BEN	DIGITAL SME	EUROPEAN DIGITAL SME ALLIANCE	BE
21	BEN	DIGITALEUROPE	DIGITALEUROPE AISBL*	BE
22	BEN	MRU	MYKOLO ROMERIO UNIVERSITETAS	LT
23	BEN	UNIRI	SVEUCILISTE U RIJECI	HR
24	BEN	NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	PL
25	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES
26	BEN	NCI	NATIONAL COLLEGE OF IRELAND	IE
27	BEN	TERAWE	TERAWE TECHNOLOGIES LIMITED	IE
28	BEN	CY CERGY PARIS	CY CERGY PARIS UNIVERSITE	FR
29	BEN	BANCO SANTANDER	BANCO SANTANDER SA	ES
30	BEN	CYBER RANGES	CYBER RANGES LTD	CY
31	BEN	RED OPEN S.R.L	RED OPEN S.R.L.	IT
32	BEN	VMU	VYTAUTO DIDZIOJO UNIVERSITETAS	LT
33	AP	FHG	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	DE
34	AP	Pearson Benelux	Pearson Benelux BV	NL

Document Control Information

Project	Digital4Security
Document Title	Interim D3.2 Ready-to-Use Online Training Materials
Work Package Number	WP3
Deliverable Number	D3.2
Lead Beneficiary	Profil Klett
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (UPB)
Dissemination Level	PU
Authors	Kristina Ferara Blašković, Tvrtko Pleić, Profil Klett
Reviewers	Zvonimir Stanić, Profil Klett (1st level review)
Description	Create of a suite of Ready-to-Use online Training Materials for the delivery of the online Masters.
Status	Final v1
Delivery Date	30.11.2024
Due date	30.11.2024
Approval Date:	DD.MM.YYYY

Revision history

Version	Date	Modified by	Comments
1	27.11.2024	Kristina Ferara Blašković, Profil Klett	Draft for the QA review
2	28.11.2024	Lucia Grilli, Brian Cochrane, Schuman Associates	QA Review



Introduction

Interim Deliverable D3.2 represents a critical milestone in the Digital4Security Master's Programme, aiming to provide a comprehensive suite of Ready-to-Use Online Training Materials and Modules. These materials are specifically designed to facilitate the delivery of a highly engaging and effective online learning experience. By leveraging the latest instructional design methodologies and advanced digital tools, Interim D3.2 ensures that learners can acquire both theoretical knowledge and practical skills essential for addressing complex challenges in the cybersecurity field.

The purpose of this deliverable is to:

- Develop modular and adaptable learning materials tailored to the needs of cybersecurity professionals.
- Integrate the materials seamlessly into the Moodle Learning Management System (LMS), ensuring ease of access and usability.
- Demonstrate the alignment of learning resources with Programme objectives, real-world applications, and industry standards.
- Set a foundation for ongoing updates and improvements through a structured, flexible, and scalable approach.

Objectives of Interim Deliverable 3.2

The Digital4Security Master's Programme is a ground-breaking initiative designed to equip learners with advanced competencies in cybersecurity, addressing the increasing demand for skilled professionals in the field. Interim Deliverable D3.2 plays a major role in supporting this mission by providing Ready-to-Use Online Training Materials that align with the overarching learning goals of the Master's Programme. These materials are designed to ensure a seamless integration of theory and practice, empowering students to meet the complex demands of the cybersecurity landscape.

The alignment of the modules and training materials with the Programme's learning goals ensures that students achieve the following:

No.	Goal
PO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.
PO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
PO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

The materials are carefully developed to enhance learning outcomes by fostering critical thinking, problem-solving abilities, and hands-on skills, thereby preparing students to tackle the evolving challenges in cybersecurity. Additionally, the use of online materials provides learners with unparalleled flexibility and accessibility, enabling global participation regardless of location or personal commitments. By emphasizing real-world applications and integrating cutting-edge tools, the materials bridge the gap between theoretical learning and professional practice, ensuring students are industry-ready upon completion of the Programme.

Importance of Ready-to-Use Online Training Materials

The dynamic nature of cybersecurity **demands that learners have access to up-to-date, interactive, and accessible learning materials to stay ahead in this rapidly evolving field.** These materials form the backbone of advanced education, particularly in a Master's Programme, as they provide the foundation for critical thinking, advanced learning, and the practical application of theoretical concepts.



Overview of Learning Materials

Role of Online Learning Materials

Learning materials play an essential role in helping students develop skills such as analysis, research, and problem-solving. In a Master's context, these resources - ranging from textbooks and research articles to multimedia tools and interactive case studies - enhance students' ability to deeply engage with their subject matter, achieve academic goals, and prepare for professional challenges. Institutions must ensure access to diverse, up-to-date resources to maximize students' academic and professional potential.

In the case of the Digital4Security Master's Programme, the choice of online training materials reflects the evolving needs of cybersecurity education. The Programme capitalizes on the flexibility and interactivity of online materials to meet the demands of modern learners, ensuring both accessibility and practicality.

Advantages of Online Training Materials

Online training materials provide numerous benefits that transform the educational experience in cybersecurity:

1. **Dynamic and Up-to-Date Content**

Online materials can be updated instantly, ensuring that learners always have access to the latest research, tools, and trends in cybersecurity, an essential feature for a rapidly evolving discipline.

2. **Interactive and Engaging Learning**

Incorporating multimedia elements such as videos, animations, quizzes enhance engagement and improves retention. Features like discussion forums and live chats enable collaborative learning in virtual settings.

3. **Flexibility and Accessibility**

Students can access materials anytime, anywhere, accommodating their schedules and commitments. This flexibility is particularly beneficial for adult learners, working professionals, and international students balancing academic commitments with personal and professional responsibilities. Furthermore, online materials ensure that learners in remote or underserved regions can access the same high-quality education as their peers, bridging geographical and economic divides.

4. **Application-Oriented Learning**

Hands-on practice through virtual labs, simulations, and case studies allows students to apply concepts in real-world scenarios, bridging the gap between theory and practice.

5. **Global Reach and Inclusivity**

Online resources break geographical barriers, ensuring access to high-quality education worldwide. Materials are designed to support diverse learning styles.

6. **Sustainability and Cost-Effectiveness**

Digital resources reduce the need for printed materials, lowering costs and supporting environmental sustainability. The integration of Open Educational Resources (OER) provides free access to textbooks and other learning materials, making education more affordable for students. From a sustainability perspective, reducing reliance on printed materials significantly lowers the environmental footprint of the Programme, aligning with global efforts to promote eco-friendly educational practices.

7. **Enhanced Learning Analytics**

Platforms track user interactions, offering insights into performance and engagement. These analytics inform improvements to the learning experience.



Figure 1: Benefits of Online Training Materials

Ready-to-Use Online Training Materials for Flexible Learning

The Digital4Security Programme utilizes **ready-to-use online training materials** to create a flexible and learner-centred educational environment. Flexible learning enables students to engage with content in a way that suits their individual needs and circumstances.

- **Personalized Learning Paths:** Online resources support a learner-centred approach by enabling personalized learning paths. Students can revisit lectures, pause and reflect, and explore supplementary materials, fostering autonomy in their educational journey. Additionally, the incorporation of interactive elements - such as videos, quizzes, gamified content, and collaborative tools - creates an engaging and dynamic learning experience that enhances knowledge retention and application.
- **Diverse Delivery Modes:** The combination of **synchronous and asynchronous** methods, along with interactive features, ensures flexibility and accessibility for all learners.
- **Application-Focused Content:** A key strength of the Digital4Security learning materials is their focus on application-oriented learning. Through case studies, virtual labs, simulations, and problem-solving tasks, students gain hands-on experience in addressing real-world cybersecurity challenges. This practical approach ensures that learners develop not only theoretical knowledge but also the skills necessary to excel in professional environments.
- **Inclusivity:** Materials are designed to be accessible regardless of location, ability, or prior knowledge, meeting the diverse needs of adult learners.

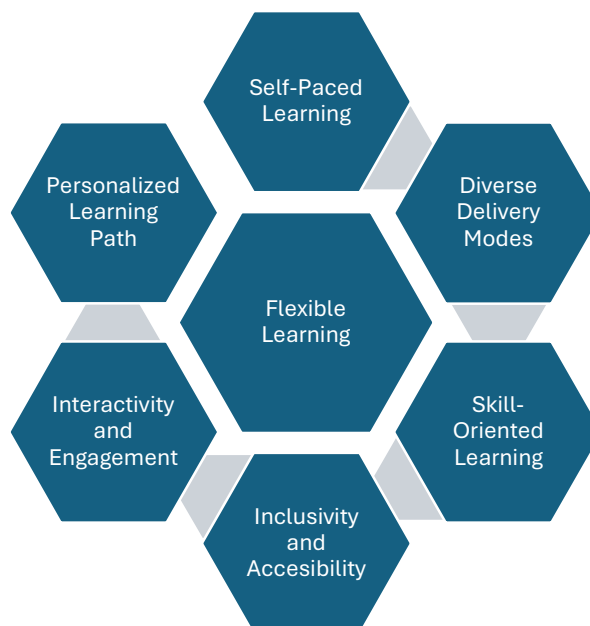


Figure 2. Flexible learning characteristics



Structure and Design of Modules

Framework for Module Development

The Framework for Module Development establishes the foundational principles and methodologies guiding the creation of modules for the Digital4Security Master's Programme. This framework ensures that all modules align with the Programme's objectives, delivering a high-quality, learner-centred, and practical educational experience. It emphasizes consistency, scalability, and flexibility while addressing the diverse needs of learners.

Each module is carefully aligned with the overarching goals of the Digital4Security Master's Programme. The framework ensures that modules contribute to the development of critical knowledge and practical skills in cybersecurity. They are designed to achieve specific learning outcomes, such as fostering critical thinking, enhancing problem-solving abilities, and cultivating leadership skills in cybersecurity contexts. Furthermore, the modules integrate theoretical concepts with practical applications, preparing learners to tackle real-world challenges effectively.

The modular design principles within the framework prioritize a unified approach, ensuring consistency across all modules. Each module adheres to a standardized structure, including consistent naming conventions, uniform navigation elements, and cohesive visual styles. This approach ensures a seamless learning experience and reduces cognitive load for learners. The modular structure is also highly scalable, allowing for the addition of new topics or updates to existing content as advancements occur in the rapidly evolving field of cybersecurity. Additionally, the framework is flexible, accommodating diverse learning preferences and promoting inclusivity for learners from various backgrounds and expertise levels.

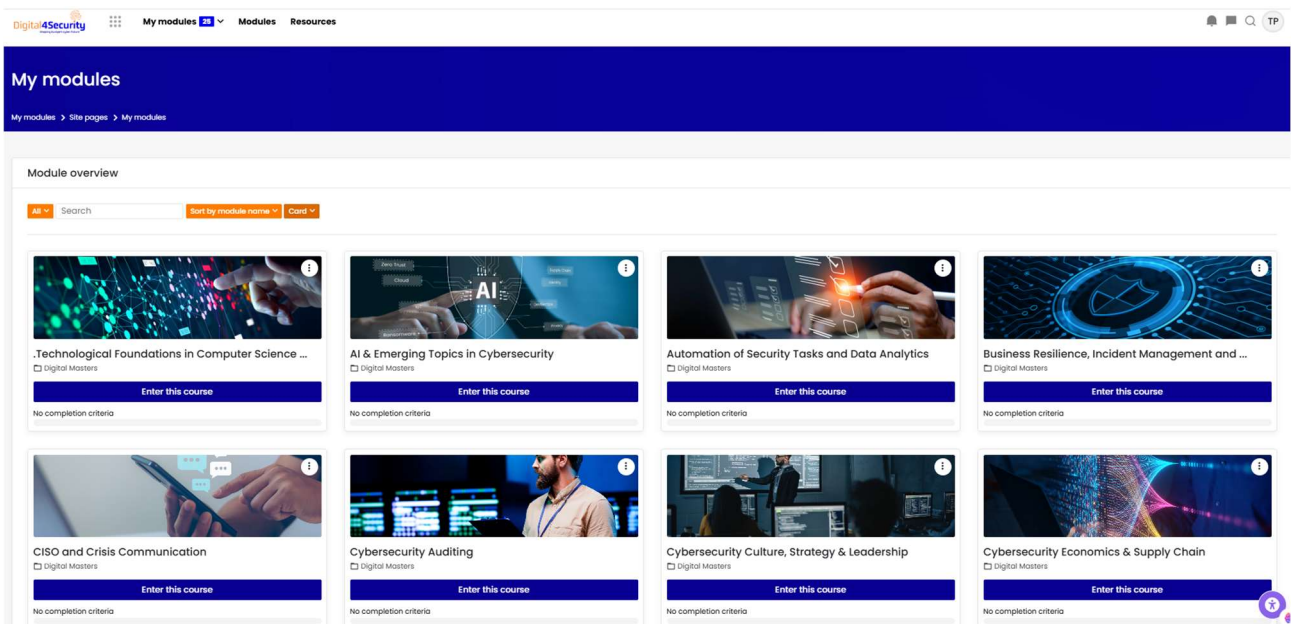


Figure 3: UI design of how modules will display when students are logged in.

The framework adopts a learner-centred methodology, emphasizing engaging, practical, and accessible content. Learning outcomes for each module are clearly defined to help learners understand the purpose and expectations. Real-world applications, such as case studies, simulations, and interactive exercises, are integrated to provide practical learning opportunities. Feedback loops are also incorporated into the design process to refine content and activities based on learner experiences and evolving needs.

Moodle serves as the central platform for delivering the modules, leveraging its technological capabilities to enhance the learning experience. Interactive tools, such as H5P, enable the creation of engaging activities, while collaborative features like forums and live sessions facilitate peer-to-peer and instructor-led interactions. Accessibility features ensure that all learners, including those with disabilities, can fully engage with the content and activities.

Each module is structured to provide a clear and progressive learning pathway. It begins with an introduction that includes an overview of the module's purpose, structure, and learning outcomes. The module is divided into a weekly breakdown, offering a logical and step-by-step roadmap for learners to follow. The framework also incorporates well-defined assessment and feedback methods, ensuring learners have opportunities to demonstrate their understanding and receive constructive guidance.

The framework includes quality assurance mechanisms to uphold high standards in module development. Peer reviews validate the accuracy and relevance of content, while interactive tools and activities undergo thorough testing to ensure functionality and usability. Regular updates are implemented based on learner feedback and advancements in the cybersecurity field, maintaining the modules' relevance and effectiveness.

Key Guidelines Used for Designing Moodle Modules

The Moodle modules for the Digital4Security Master's Programme have been meticulously designed to provide a learner-centred, interactive, and accessible educational experience. The following guidelines serve as the foundation for their design, ensuring consistency, usability, and engagement across all modules:

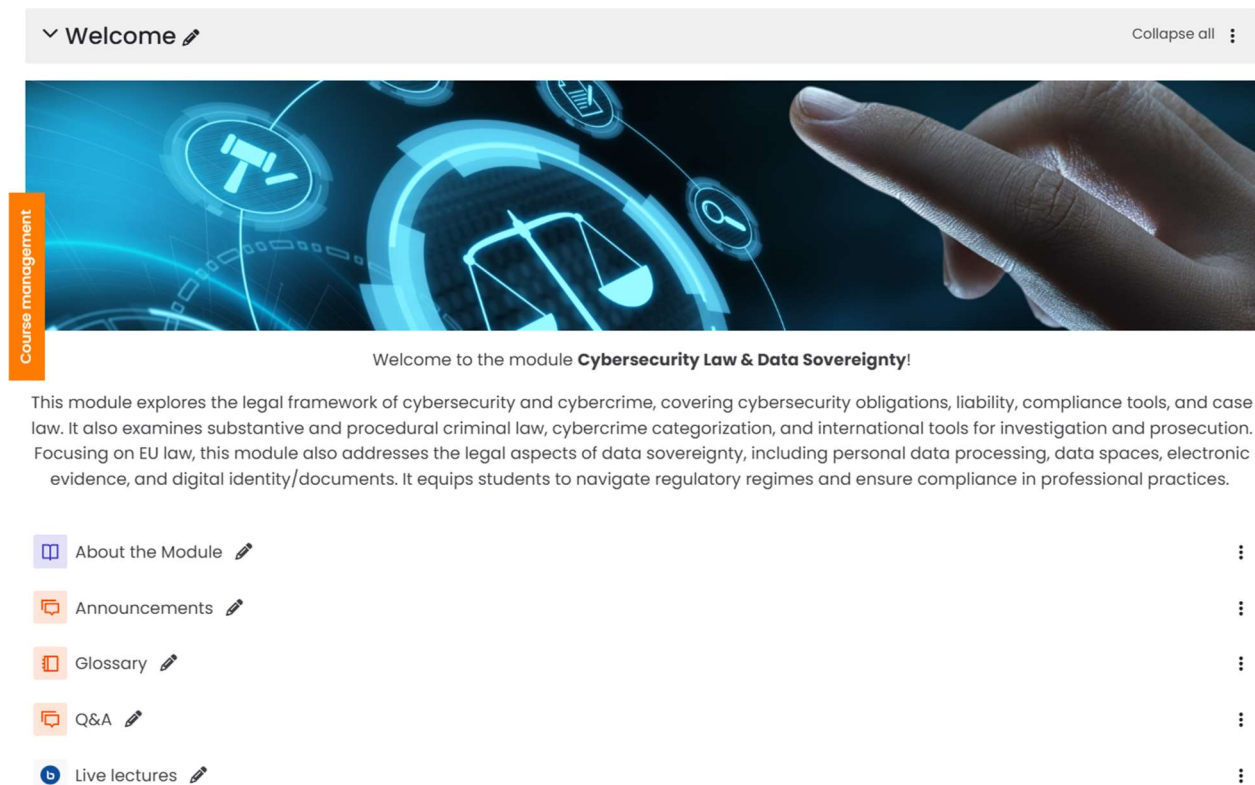
II. Consistency Across Modules

Each module is structured uniformly to maintain a predictable and intuitive learning environment. Consistent naming conventions for sections, activities, and resources help learners navigate seamlessly across modules. A standardized visual style - using cohesive fonts, colours, and icons - ensures a professional appearance while reducing cognitive load.

Key features of each module include the following:

Welcome Message

Each module begins with a visually appealing and concise welcome message. This message briefly introduces the module, outlines its purpose, and sets the tone for the learning journey. The design emphasizes clarity and engagement, using professional visuals and a warm, encouraging tone.



The screenshot shows a Moodle module interface. At the top, there is a header bar with a dropdown arrow and the text 'Welcome' followed by an edit icon. On the right side of the header, there is a 'Collapse all' button with a three-dot menu icon. Below the header is a large banner image featuring a hand pointing towards a futuristic digital interface with glowing blue icons of a scale of justice, a magnifying glass, and a document. To the left of the banner is a vertical orange bar with the text 'Course management'. Below the banner, the text reads: 'Welcome to the module **Cybersecurity Law & Data Sovereignty!**'. This is followed by a paragraph of introductory text: 'This module explores the legal framework of cybersecurity and cybercrime, covering cybersecurity obligations, liability, compliance tools, and case law. It also examines substantive and procedural criminal law, cybercrime categorization, and international tools for investigation and prosecution. Focusing on EU law, this module also addresses the legal aspects of data sovereignty, including personal data processing, data spaces, electronic evidence, and digital identity/documents. It equips students to navigate regulatory regimes and ensure compliance in professional practices.' Below the text is a list of module activities, each with an icon and an edit icon: 'About the Module', 'Announcements', 'Glossary', 'Q&A', and 'Live lectures'. Each activity has a vertical three-dot menu icon to its right.

Figure 4: Screenshot of a visually designed welcome message with a brief introduction to the module.

"About the Module" Section

A dedicated "About the Module" section provides essential information to orient learners, including:

1. Module Objectives and Learning Outcomes: Clearly defined goals and outcomes to help learners understand what they will achieve by completing the module.
 - Who Is This Module For?: A brief description of the target audience, ensuring learners know the module's relevance to their academic and professional needs.
 - ECTS Credits: Information on the credit value of the module to align with academic requirements.

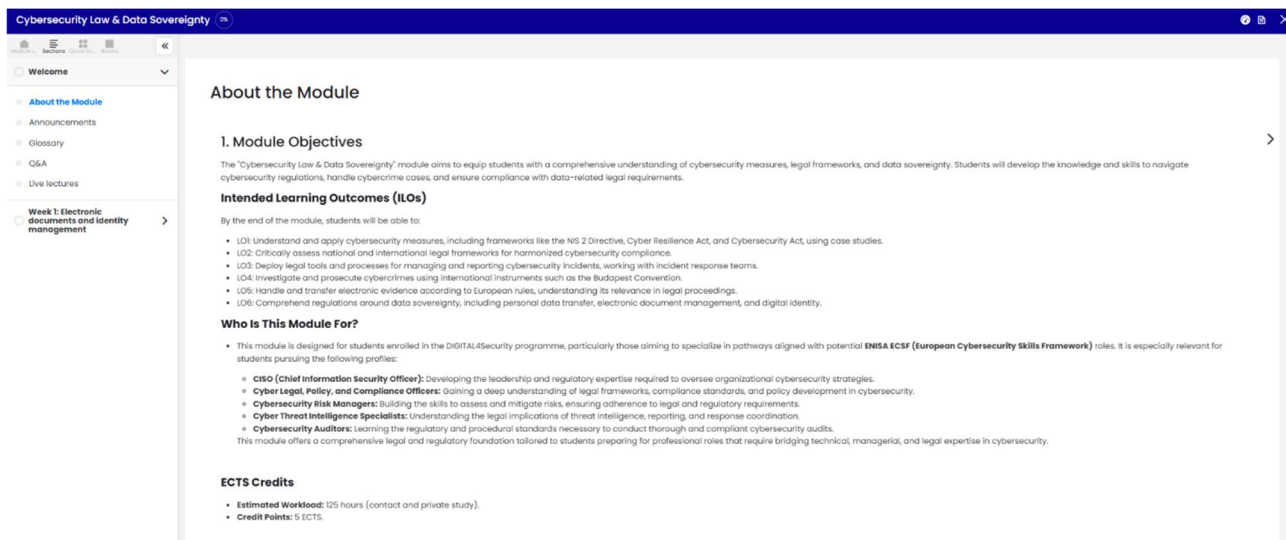


Figure 5: Screenshot of the section containing module objectives, learning outcomes, and weekly structure.

2. Structure of the Module

This subsection outlines the module's weekly breakdown over 12 weeks, detailing what students will learn each week. It serves as a roadmap, providing an overview of topics and activities to ensure learners can plan their study schedule effectively.

3. How to Successfully Complete This Module

This part offers all the information learners need to succeed, including:

- Module Workload and Learning Commitment: Guidance on the time and effort required.
- Exams and Assessment Formats: A detailed explanation of the assessment criteria, including the types of exams, assignments, and their weightage.
- Study and Examination Requirements: Expectations for attendance, participation, and preparation.

- Resits and Repeat Assessments: Clear policies for students needing additional opportunities to pass.

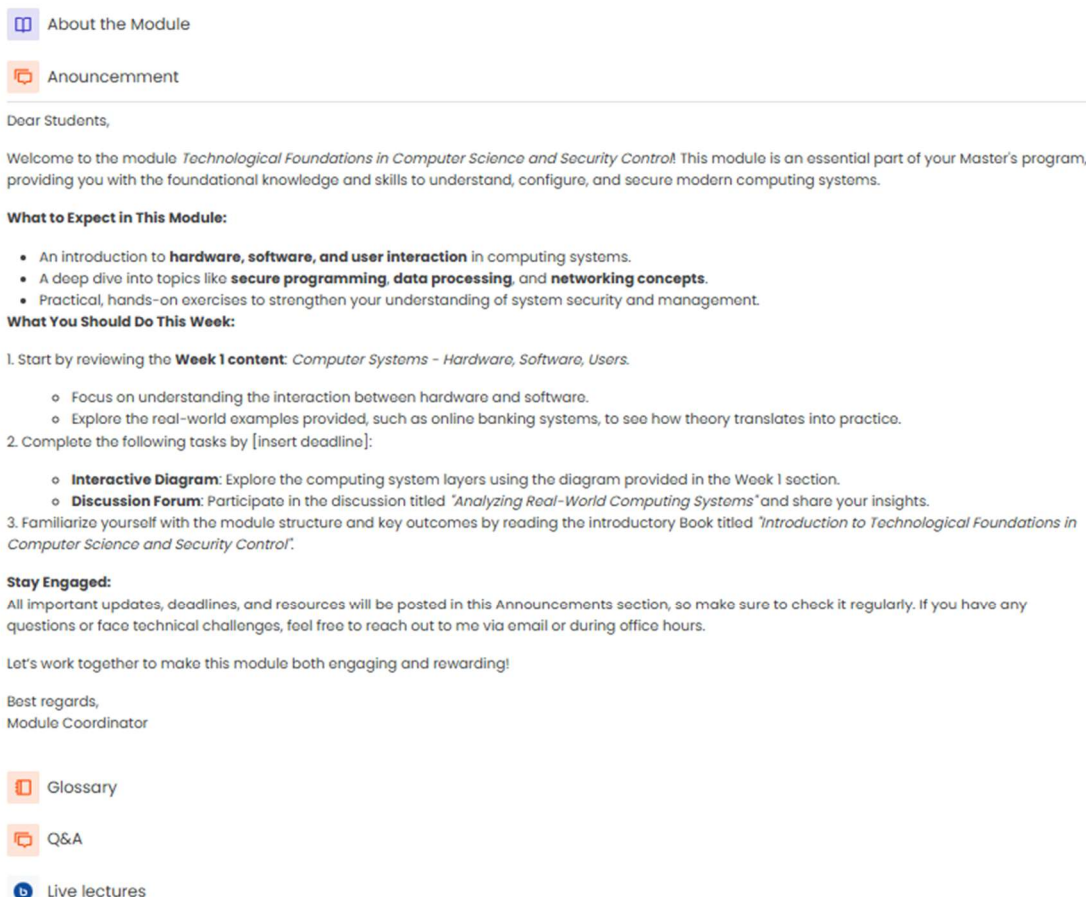
4. How to Successfully Participate in This Module



This subsection includes practical guidance to help students make the most of the module:

- Technical Prerequisites: Minimum technology requirements for accessing content and participating in activities.
- Time Management and Module Access: Tips for effective time management and clear instructions for accessing module resources.
- Code of Conduct: Rules and expectations to foster a respectful and collaborative learning environment.

Announcements

A dedicated Announcements section serves as a central hub for important updates from lecturers. New announcements are prominently displayed to ensure students stay informed about live sessions, assignment deadlines, and other critical information.



 About the Module
 Announcement

Dear Students,

Welcome to the module *Technological Foundations in Computer Science and Security Control*! This module is an essential part of your Master's program, providing you with the foundational knowledge and skills to understand, configure, and secure modern computing systems.

What to Expect in This Module:

- An introduction to **hardware, software, and user interaction** in computing systems.
- A deep dive into topics like **secure programming, data processing, and networking concepts**.
- Practical, hands-on exercises to strengthen your understanding of system security and management.

What You Should Do This Week:

1. Start by reviewing the **Week 1 content**: *Computer Systems – Hardware, Software, Users*.
 - Focus on understanding the interaction between hardware and software.
 - Explore the real-world examples provided, such as online banking systems, to see how theory translates into practice.
2. Complete the following tasks by [insert deadline]:
 - **Interactive Diagram**: Explore the computing system layers using the diagram provided in the Week 1 section.
 - **Discussion Forum**: Participate in the discussion titled *'Analyzing Real-World Computing Systems'* and share your insights.
3. Familiarize yourself with the module structure and key outcomes by reading the introductory Book titled *'Introduction to Technological Foundations in Computer Science and Security Control'*.

Stay Engaged:
All important updates, deadlines, and resources will be posted in this Announcements section, so make sure to check it regularly. If you have any questions or face technical challenges, feel free to reach out to me via email or during office hours.

Let's work together to make this module both engaging and rewarding!

Best regards,
Module Coordinator




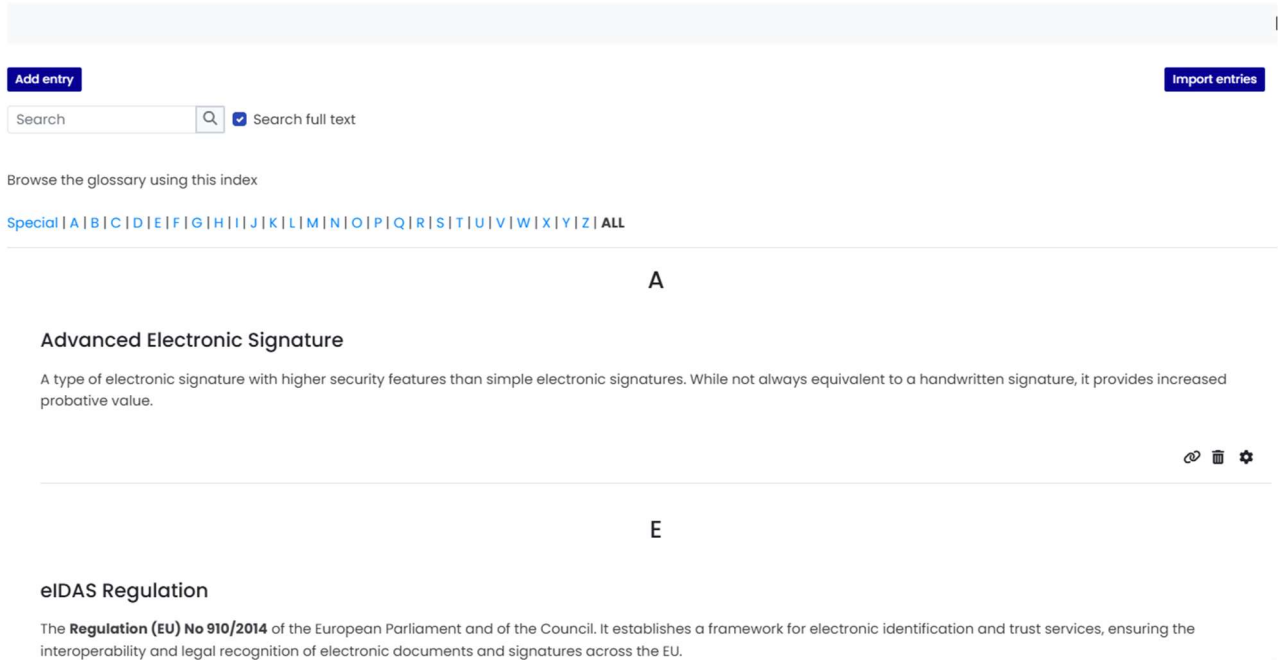
 Glossary
 Q&A
 Live lectures

Figure 6: Screenshot showing an example of a recent announcement displayed prominently

Glossary

Each module includes a comprehensive glossary of key terms, providing students with quick and easy access to definitions of technical and subject-specific terminology.

Glossary



The screenshot shows a web interface for a glossary. At the top, there is a search bar with a magnifying glass icon and a checkbox labeled "Search full text". To the left of the search bar is a blue button labeled "Add entry", and to the right is another blue button labeled "Import entries". Below the search bar, the text "Browse the glossary using this index" is followed by a horizontal list of letters: "Special | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | ALL". The main content area is divided into two sections. The first section is titled "A" and contains the entry "Advanced Electronic Signature". The definition for this entry reads: "A type of electronic signature with higher security features than simple electronic signatures. While not always equivalent to a handwritten signature, it provides increased probative value." To the right of the definition are three small icons: a link icon, a trash can icon, and a gear icon. The second section is titled "E" and contains the entry "eIDAS Regulation". The definition for this entry reads: "The Regulation (EU) No 910/2014 of the European Parliament and of the Council. It establishes a framework for electronic identification and trust services, ensuring the interoperability and legal recognition of electronic documents and signatures across the EU."

Figure 7: Screenshot of the glossary interface with sample terms and definition

Forum and Q&A Section

A dedicated **Q&A forum** allows students to post questions and engage in discussions. This encourages peer-to-peer interaction and provides a collaborative space for addressing common concerns.

Live Sessions via BigBlueButton

Each module includes a link to **BigBlueButton** for live sessions. These sessions are scheduled and announced in advance through the announcements section, ensuring students have ample notice to attend.

Module structure (Weekly Structure)

Content is divided into 12 weeks, with each week containing:

1. **Core Reading Content:** Designed for independent study and additional literature and references to deepen understanding.
2. Self-Assessment Quizzes or Questions (**Check your understanding**): Interactive quizzes or reflection prompts to reinforce learning.
3. **PowerPoint presentations** summarizing the live sessions are uploaded immediately before the lecture to ensure they reflect the latest trends and updates on the subject: A PowerPoint presentation summarizing the live session, uploaded for reference.
4. **Reading List:** A comprehensive Reading List provides links to additional literature and resources that students need to review for a deeper understanding of the module content. These resources are curated to align with the learning outcomes and assessment requirements.

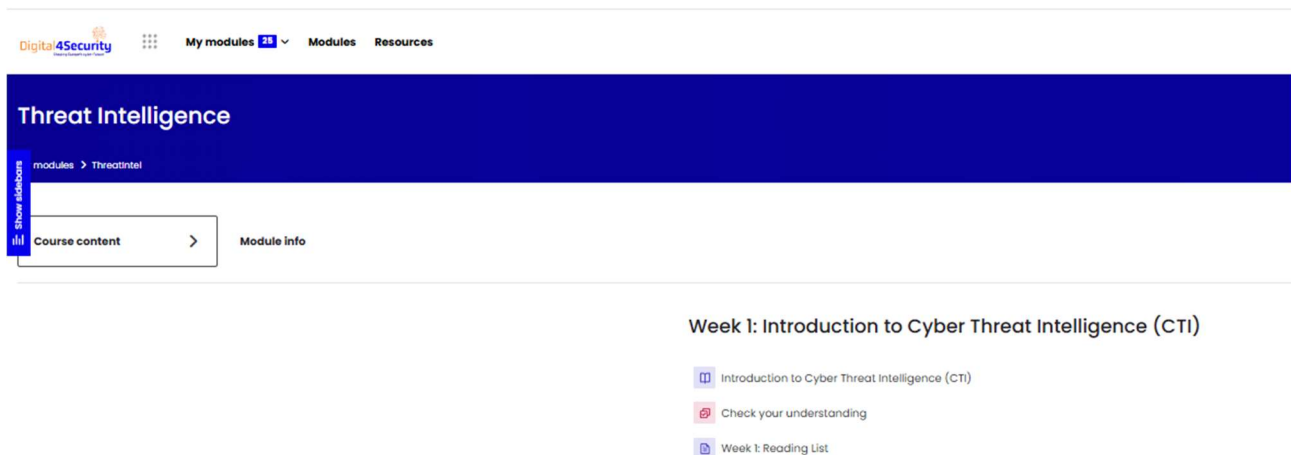


Figure 8: Screenshot of a weekly page showing content, self-assessment quizzes, and downloadable presentations.

Exam and Assessment Format

The final section of each module explains all requirements for successful completion. It includes detailed descriptions of:

- Assessment Formats: Types of assessments (e.g., quizzes, case studies, final exams).
- Criteria for Passing: Clear expectations and benchmarks for success.
- Weightage and Deadlines: Distribution of marks across various assessments and their respective timelines.

Assignments

Topic	Assignments	Due date	Submission	Grade
Week 2: Tools and Common Applications of Computer Systems	Exploring Tools and Applications in Modern Computer Systems	Monday, 2 December 2024, 12:00 AM	0	Needs grading: 0
Exams and Assessment Formats	Practice exercises with applications and files (10%)	Thursday, 28 November 2024, 12:00 AM	0	Needs grading: 0
	Practice exercises on a networked system (10%)	Thursday, 28 November 2024, 12:00 AM	0	Needs grading: 0
	Team project (20%)	Thursday, 28 November 2024, 12:00 AM	0	Needs grading: 0
	Practical Exam (30%)	Thursday, 28 November 2024, 12:00 AM	0	Needs grading: 0

Figure 9: Screenshot of the assessment format description, showing criteria, deadlines, and expectations.

III. Learner-Centred Design

The content and activities are tailored to the needs of the learners, emphasizing clarity in objectives, real-world application, and active engagement. Each module begins with clearly stated learning outcomes, providing learners with a clear understanding of what they will achieve. Activities such as case studies, simulations, and problem-solving tasks foster critical thinking and practical skills development.

IV. Interactive Tools

Moodle's rich suite of interactive tools enhances engagement and retention. Features like **H5P** enable the creation of interactive quizzes, drag-and-drop activities, and flashcards. Forums facilitate peer interaction and collaboration, while quizzes and assignments provide immediate feedback and assessment opportunities.

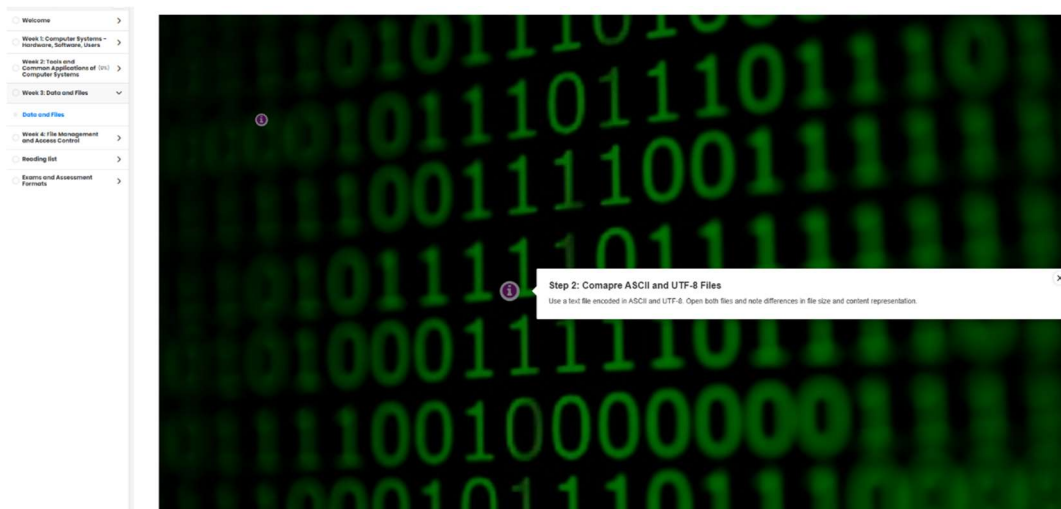


Figure 10: H5P activity interface showing hot spot image.

V. Accessibility

The modules are designed with accessibility in mind, adhering to the **Web Content Accessibility Guidelines (WCAG)**. This includes ensuring compatibility with screen readers, using descriptive alt text for images, and providing captions for videos. The platform's structure supports learners with disabilities, making the content universally accessible.

VI. Visual Cues and Navigation

Icons, images, and structured layouts guide learners through their activities. Visual elements provide quick cues about the nature of each resource or activity, making navigation straightforward. Key sections like "Introduction," "Activities," and "Assessments" are visually distinct and easy to locate.

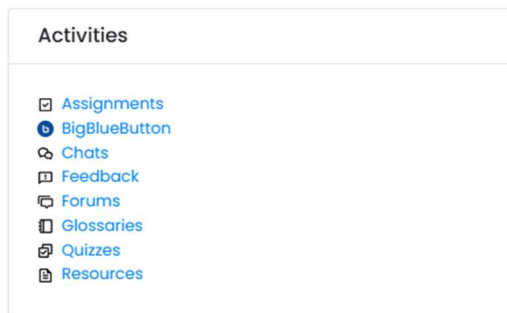


Figure 11: Screenshot of the activity block showcasing shortcuts to the main activities within each module.

VII. Completion Tracking

Activity completion tracking is enabled to guide learners and provide a sense of achievement as they progress. Learners can see their completed activities immediately, motivating them to stay on track. Course completion dashboards summarize progress and highlight remaining tasks.



Moodle & Ready-to-Use Online Training Material

The Consortium has chosen Moodle as the platform for delivering the Digital4Security masters. All ready-to-use online training materials will be developed within Moodle. It is one of the world's most widely used learning management systems, with large-scale installations that demonstrate its scalability. Many of our academic partners are already familiar with the Moodle, as it is used regularly in their institutions, which reduces the learning curve.

Key features of Moodle include:

- User-friendly and designed with a user-centric approach.
- Comprehensive accessibility system to accommodate users with special requirements, so they can easily navigate and use the platform.
- Facilitates collaborative learning.
- Offers powerful analytics and reporting tools.
- Extensible with a global community of developers.
- Highly modular and open source.
- Supports a wide variety of plugins and integrations.

As of October 2024, Moodle had more than [155,753 active sites](#) registered across 239 countries, with nearly 430 million users.

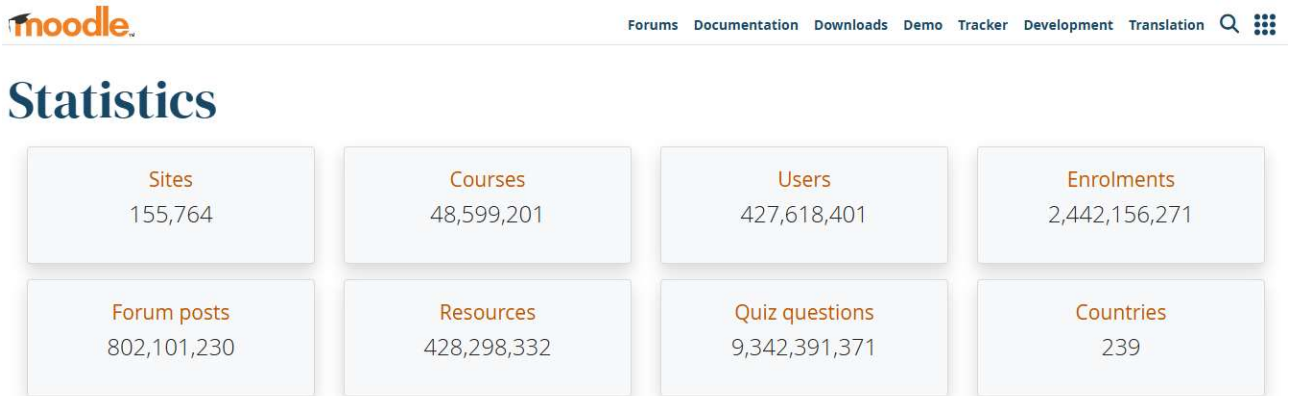


Figure 12: Moodle statistics according to <https://stats.moodle.org>.

Among the universities using Moodle are *POLITEHNICA* Bucharest, our project coordinator, UNIR, Politecnico di Milano, National College of Ireland and MRU, all members of our Consortium.



Figure 13: Partner universities using Moodle

Moodle framework

Moodle¹ is an open-source learning management system (LMS) designed to provide educators, administrators and learners with a secure and integrated environment for creating personalised learning experiences. It has been customised to meet the needs of Digital4Security. We have enhanced the system by integrating several third-party tools and plugins, adding interactive elements and AI-driven features. The Moodle LMS platform will be built out as follows:

- Technical architecture.
- Information architecture.
- User interface design for key pages.
- Assets for landing pages and modules.
- Setup and deployment of Moodle infrastructure.
- Integration of third-party plugins and licences.
- User access and administration.
- Moodle on-boarding and training.
- QA and testing.

¹ <https://moodle.org>



Instructional Design of Ready-to-Use Online Training Materials

Instructional design plays a critical role in shaping effective and engaging curricula and content for master's Programmes in cybersecurity, where the complexity of the subject demands a structured and learner-centred approach. In this context, instructional design ensures that educational experiences are tailored to equip students with both theoretical knowledge and practical skills essential for addressing advanced cybersecurity challenges. By systematically aligning module objectives with industry standards and the specific needs of cybersecurity professionals, instructional design facilitates the integration of cutting-edge topics such as cryptography, ethical hacking, and network defence. Moreover, it incorporates technology-enhanced tools like simulations, virtual labs, and interactive case studies, allowing students to apply concepts in real-world scenarios. This targeted approach ensures that graduates are prepared to tackle the evolving landscape of cybersecurity threats and solutions. There are several models of instructional design. Most known is ADDIE, but that model is more appropriate for corporate learning. For this Digital4Security we choose Merrill's Principles of Instruction.

Merrill's Principles of Instruction, developed by M. David Merrill (2002), present a learner-centred approach to designing effective educational experiences. At the core of Merrill's model is the idea that learning is most effective when it is problem-centred and involves real-world tasks that learners find meaningful. Merrill identifies five interrelated principles as it is shown of figure 14:

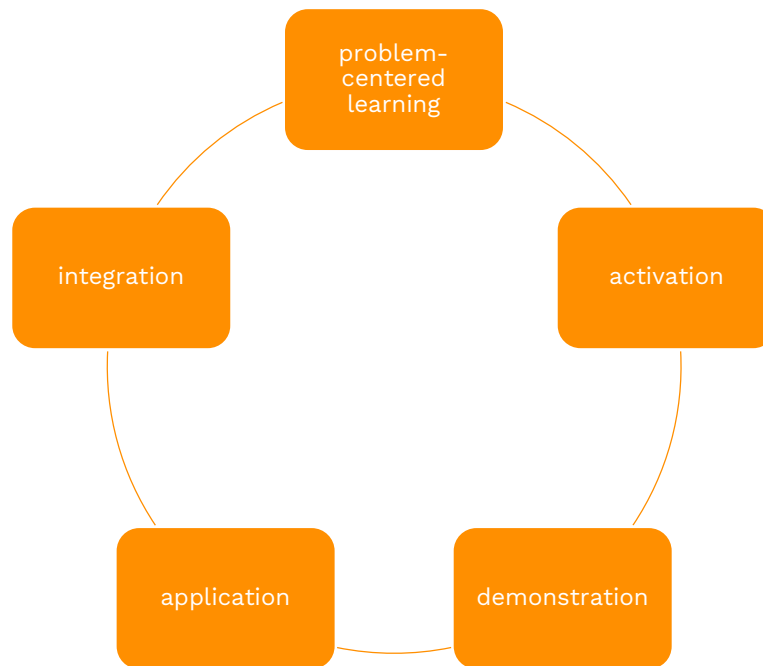


Figure 14: Merrill identifies five interrelated principles

These principles emphasize a holistic approach to teaching, ensuring that learners not only acquire knowledge but also develop the skills to apply it in relevant contexts.

The first principle, problem-centred learning, posits that instruction should revolve around solving authentic problems. By engaging with real-world scenarios, learners are more likely to find the material meaningful and develop skills that transfer to their professional environments. For example, in a cybersecurity modules, students could be tasked with identifying vulnerabilities in a network system and proposing mitigation strategies. This problem-based approach fosters critical thinking and ensures that learning is grounded in practical application.

The other principles: activation, demonstration, application, and integration, build upon problem-centred learning. Activation involves drawing upon learners' prior knowledge to create a foundation for new learning. In our case, it is very important because, we will have for sure existing experts whose skills will be upped. Demonstration requires instructors to showcase concepts and processes, often using multimedia tools to enhance understanding. That is possible with on-line materials. Application is critical, as it allows learners to practice and refine their skills through activities such as simulations or hands-on exercises. Finally, integration ensures that learners can internalize and apply their knowledge in diverse settings, often through collaborative projects or reflective discussions. Merrill's model, supported by empirical studies, underscores the importance of active participation and meaningful engagement in learning (Merrill, 2002).



Key Considerations for Designing Online Content for Adult Learners in a European Masters Programme

Adult learners are unique in that they bring diverse experiences and established skills to the learning environment. Unlike younger learners, adults have typically undergone various forms of formal education while also benefiting from non-formal and informal learning experiences. These experiences often equip them with skills and competencies acquired through years of workplace activities and tasks. Moreover, adult learners tend to be acutely aware of their educational needs and seek learning opportunities that have direct, practical applications in their professional and personal lives. Therefore, educational Programmes tailored for adults must emphasize relevance, practicality, and applicability.

Adult education must align with learners' goals and needs, ensuring that its relevance is clear and immediate. Programmes should identify specific goals and needs, recognizing the significance of education in achieving them (Knowles, 1980). Additionally, they must promote the applicability of learning content by ensuring it supports learners' professional tasks and daily situations. Emphasizing the value of education, in terms of personal development and career advancement, is critical. As Merriam and Bierema (2013) note, adult learners are particularly motivated when they see tangible benefits in their learning.

Motivation plays a central role in adult learning, driven by aspirations for personal growth and practical outcomes. Practical relevance is crucial, and learning activities should address real-world challenges faced by learners (Knowles, Holton, & Swanson, 2011). Active engagement techniques, such as case studies, problem-solving tasks, and discussions, maintain interest and commitment. Furthermore, fostering a sense of achievement and autonomy empowers learners to take control of their educational journey (Deci & Ryan, 2000).

Reflective learning enables adults to connect theoretical knowledge with real-life contexts. Encouraging problem identification allows learners to reflect on challenges in their work or personal lives and consider potential solutions (Schön, 1983). Kolb highlighted that facilitating the creation of portfolios to document learning progress helps reinforce the connection between learning and practical application.

Adult learning should prioritize practical knowledge and skills over abstract theoretical content. A skills-based curriculum is essential, focusing on competencies that directly benefit learners in their professional or personal lives (Brookfield, 2013). The integration of digital tools enhances engagement and provides learners with practical resources for applying knowledge in real-world scenarios.

Recognizing that adult learners often balance work, family, and education, educational Programmes should be flexible and efficient. Time management is vital, respecting learners' schedules by offering concise, relevant, and adaptable learning opportunities. A variety of motivational strategies, including rewards, peer collaboration, and real-world simulations, can be employed to help achieve learning outcomes (Merriam et al., 2007).

The education of adult learners requires an approach that prioritizes relevance, practicality, and learner-centred strategies. By focusing on application, fostering motivation, encouraging reflective learning, and respecting their commitments, educators can create effective and engaging learning experiences that meet the unique needs of adult learners.



Demonstration of Ready-to-Use Materials

The structure and sample materials for all modules within the Digital4Security Master's Programme are available at the following link: <http://learn.digital4security.eu/>. This demonstration provides an overview of the module layouts, interactive features, and the consistent design principles applied across the platform.

To access the content, users must sign in to the platform.

Once logged in, reviewers will be able to explore the modular structure, sample materials, and interactive elements currently available.

It is important to note that the development process for the Ready-to-Use Online Training Materials is actively underway. A comprehensive roadmap for material development has been established by the academic partners, who are responsible for drafting the written content for each module. Once the materials are delivered, Profil Klett ensures their seamless integration into Moodle. This process includes adhering to a standardized structure, creating interactive elements, and rigorously applying the design guidelines outlined in this document.

The collaborative effort between academic partners and Profil Klett ensures a cohesive and high-quality teaching and learning experience. The modular structure, as demonstrated in the link, reflects the foundational framework that supports the consistent and effective delivery of content within the Digital4Security Programme. As the development progresses, each module will be populated with the finalized content, ensuring that it meets the highest standards of pedagogy, interactivity, and accessibility.



Roles in development of Ready-to-Use Online Training Material and Process

We identify several roles in process of development of Ready-to-Use Online Materials. They are as it follows:

1. Author

Author of every material is person who writes content for module. She/He is an expert for module content. She/He is responsible for incorporating knowledge and skills in content, developing reflective and integrative activities, suggesting interactive elements, and designing demonstrative content. Author is mostly module owner, but it is not necessarily.

2. Module owner

Module owner needs to define learning outcomes of module. Also, she/he ensures that these objectives align with the broader Programme goals and address the needs of the target audience. Module owner outlines module structure and delivery methods. Module owner is also responsible for monitoring and enhancing module effectiveness.

3. Editor

We define six main editor's tasks. Editor is responsible for: reviewing and refining content; ensuring consistency across material, validating information, enhancing visual and interactive elements, preparing content for final delivery, coordinating revision. Editor is coordinating all roles and responsibilities.

4. Reviewer

Reviewer must evaluate content alignment with learning objectives. Reviewers are instructed to guide their content evaluation based on the theory of constructive alignment. Reviewers give constructive feedback, ensuring that content gives current research, industry standards and best practices.

5. Content manager

Content manager is planning and organising, also suggesting interactive content. Content manager also oversees content quality and consistency. She/He also optimises content performance.

6. Instructional designer

Instructional designer is responsible for design modules – she/he is defining the scope of the instructional materials to address identified gaps effectively; with content manager she/he incorporates interactive elements, multimedia tools, and real-world applications to create engaging and learner-centred experiences. She/He will refine the content, activities, and assessments based on the feedback to enhance usability and effectiveness.

7. proof-reader

The proof-reader will review all content to identify and correct errors in grammar, punctuation, spelling, and formatting. She/He will ensure the text adheres to the required style guide and maintains consistency throughout the document. Additionally, she/he will verify that the final version is free of typos or inconsistencies, ensuring a polished and professional presentation. The proof-reader will collaborate with the content team to address any unclear or ambiguous areas in the text. She/He will also cross-check any references, tables, or figures for accuracy and alignment with the accompanying content.

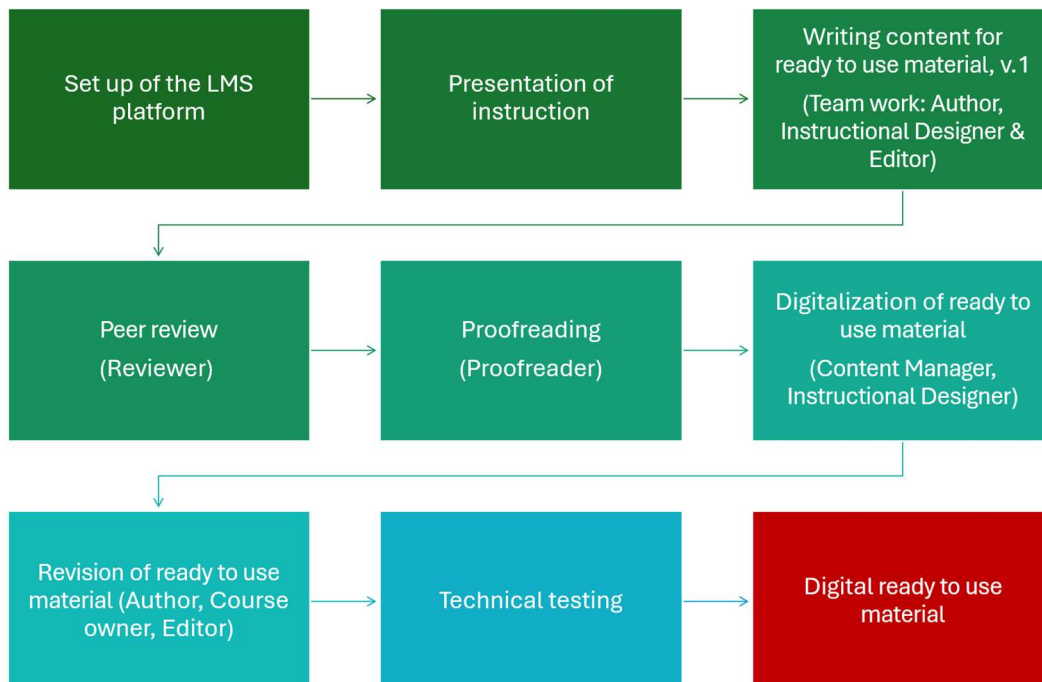


Figure 15: Roles in development of Ready-to-Use Online Training Material and Process scheme



Sustainability and Future Updates

Ensuring the sustainability and adaptability of the Digital4Security Master's Programme is a key priority. Interim Deliverable D3.2 has been developed with a forward-looking approach to accommodate planned updates, support long-term maintenance, and ensure scalability to meet future educational and industry demands.

As part of the project lifecycle, a comprehensive curriculum **review and update are scheduled for Year 3**. This process is designed to keep the Programme aligned with the latest advancements in cybersecurity by addressing emerging threats, technologies, and industry standards. Planned updates include refining module content based on feedback from learners and instructors, incorporating the latest research and tools, adjusting assessment formats to reflect current practices, and enhancing interactivity and accessibility to further engage learners. This iterative process ensures the Programme remains relevant and prepares learners to address the dynamic challenges of the cybersecurity field.

To support the longevity of the Programme, a robust maintenance strategy is in place. This includes **regular content audits to verify the accuracy and relevance of materials, continuous monitoring and updates to the Moodle platform** and its integrated tools to maintain smooth functionality, and ongoing collaboration with industry experts, academic partners, and alumni to align the curriculum with evolving needs and trends. Supplementary resources, such as reading lists and glossaries, are also reviewed and updated regularly to ensure their continued relevance.

The Programme's design is inherently scalable, enabling seamless adaptation to future needs. The modular structure allows for the addition or modification of content to address new topics or emerging technologies in cybersecurity. The Moodle platform is equipped to integrate future plugins, tools, and features that enhance the learning experience, while the Programme itself is structured to accommodate a growing number of students and to expand its reach to learners in new geographical or professional contexts. Additionally, interdisciplinary integration is planned, with potential modules linking cybersecurity to emerging fields such as artificial intelligence and other cutting-edge technologies. This approach to sustainability ensures that the Digital4Security

Master's Programme remains at the forefront of cybersecurity education, meeting the needs of learners and industry for years to come.

Appendices

A. References and Bibliography

1. Biggs, J., & Tang, C. (2011). *Teaching for Quality Learning at University*. Open University Press.
2. Brookfield, S. D. (2013). *The Skillful Teacher: On Technique, Trust, and Responsiveness in the Classroom*. Jossey-Bass.
3. Deci, E. L., & Ryan, R. M. (2000). Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *American Psychologist*, 55(1), 68–78.
4. Hilton, J. (2016). Open educational resources and college textbook choices: A review of research on efficacy and perceptions. *Educational Technology Research and Development*, 64(4), 573–590.
5. Johnson, L., Becker, S. A., Estrada, V., & Freeman, A. (2014). *Horizon Report: 2014 Higher Education Edition*. New Media Consortium.
6. Knowles, M. S. (1980). *The Modern Practice of Adult Education: From Pedagogy to Andragogy*. Cambridge Books.
7. Knowles, M. S., Holton, E. F., & Swanson, R. A. (2011). *The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development*. Elsevier.
8. Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Prentice Hall.
9. Lattuca, L. R., Voigt, L. J., & Fath, K. (2004). Does Interdisciplinarity Promote Learning? Theoretical Support and Researchable Questions. *The Review of Higher Education*, 28(1), 23–48.
10. Mayer, R. E. (2009). *Multimedia Learning*. Cambridge University Press.
11. Means, B., Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2010). *Evaluation of Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies*. U.S. Department of Education.
12. McLoughlin, C., & Lee, M. J. W. (2007). Social software and participatory learning: Pedagogical choices with technology affordances in the Web 2.0 era. *ICT: Providing choices for learners and learning*, 665–675.
13. Merriam, S. B., & Bierema, L. L. (2013). *Adult Learning: Linking Theory and Practice*. Jossey-Bass.
14. Merriam, S. B., Caffarella, R. S., & Baumgartner, L. M. (2007). *Learning in Adulthood: A Comprehensive Guide*. Jossey-Bass.
15. Merrill, M. D. (2002). First Principles of Instruction. *Educational Technology Research and Development*, 50(3), 43–59.
16. Schön, D. A. (1983). *The Reflective Practitioner: How Professionals Think in Action*. Basic Books.

17. Siemens, G. (2013). Learning Analytics: The Emergence of a Discipline. American Behavioral Scientist.
18. UNESCO. (2019). Education for Sustainable Development.

B. List of Modules and Descriptions

The Programme is designed with a flexible curriculum structure that accommodates both part-time and full-time online Master's students.

The full-time Programme comprises 120 ECTS, to be completed over two years across four semesters. The part-time Programme also consists of 120 ECTS but is spread over three years, completed across six semesters.

Once European accreditation is obtained, the Digital4Security consortium furthermore aims to offer the Programme modules as micro-credentials under national accreditation regulations, expanding the Programme's reach yet further and offering students even more flexible study options.

Table 1: The Joint Degree Programme Includes 23 Modules Conveying Distinct Cybersecurity Skills

No.	SUBJECT	ECTS	MAND/ELECT	PARTNER
1	AI & Emerging Topics in Cybersecurity	10	Mandatory	UDS
2	Business Resilience, Incident Management, and Threat Response	10	Mandatory	NCI
3	Cybersecurity Culture, Strategy & Leadership	5	Mandatory	VMU
4	Dissertation / Internship	25	Mandatory	UNI KO
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	10	Mandatory	MTU
6	Law, Compliance, Governance, Policy, and Ethics	10	Mandatory	UNIBS
7	Research Methods	5	Mandatory	UNI KO
8	Security Operations	10	Mandatory	CY CERGY
9	Technological Foundations for CS & Security Controls	10	Mandatory	UPB
10	Automation of Security Tasks and data analytics	5	Elective	UNIRI
11	CISO and Crisis Communication	5	Elective	VMU
12	Risk Management of Cyberphysical Systems	5	Elective	POLIMI/CEFRIEL
13	Cybersecurity Auditing	5	Elective	VMU
14	Cybersecurity Economics & Supply Chain	5	Elective	MRU
15	Cybersecurity Education & Training Delivery I	5	Elective	BUT
16	Cybersecurity Education & Training Delivery II	5	Elective	UPB
17	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	Elective	POLIMI
18	Cybersecurity Law & Data Sovereignty	5	Elective	BUT
19	Machine and Deep Learning in Cybersecurity	5	Elective	UNIRI
20	Digital Forensics, Chain of Custody and eDiscovery	5	Elective	NCI
21	Ethical Hacking & Penetration Testing	5	Elective	UNIR
22	Malware Analysis	5	Elective	UNIR
23	Threat Intelligence	5	Elective	UPB

The development of the modules has been an iterative process, incorporating quality assurance through extensive peer review. Initially, each module's foundational content was outlined by its owners, specifying teaching methods (such as lectures versus lab work), defining the workload (including contact vs. self-study hours), and allocating credit points. Prerequisites were identified alongside intended learning outcomes encompassing knowledge, skills, and competencies. The content was organized weekly, incorporating varied assessment formats for grading and establishing clear passing criteria, supplemented by a reading list.

To ensure flexibility in terms of educational pathways, meeting diverse learners and industry needs, the curriculum has been designed in such a way as to equip students with the necessary skills for various ENISA profiles. ENISA (the European Union Agency for Cybersecurity) outlines specific competencies and skills relevant to different job roles in the cybersecurity field.

Based on the market analysis conducted in collaboration with industry partners, several job profiles have been identified, and corresponding curricula have been developed to ensure professional preparation. A final poll among all HEIs confirmed the inclusion of six profiles in the Master's Programme. This enables students to specialize in areas such as:

1. **Chief Information Security Officer (CISO)** - Focused on strategic leadership and management of an organization's cybersecurity approach (Fig. 1).
2. **Cyber Legal, Policy, and Compliance Officer** - Concentrating on the legal and regulatory aspects of cybersecurity, ensuring compliance with relevant laws and policies (Fig. 2).
3. **Cybersecurity Risk Manager** - Dedicated to identifying, assessing, and mitigating risks to information security (Fig. 3).
4. **Cyber Threat Intelligence Specialist** - Specializing in gathering and analyzing threat intelligence to inform defensive strategies (Fig. 4).
5. **Cybersecurity Educator** - Aiming to teach and promote cybersecurity awareness and best practices within organizations (Fig. 5).
6. **Cybersecurity Auditor** - Focused on evaluating and improving an organization's cybersecurity policies, practices, and controls (Fig. 6).

Fig. 1: A 120 ECTS Master's Programme Preparing for the Role of *Chief Information Security Officer (CISO)* - Possible Pathway in a 2-Year Full Time Programme

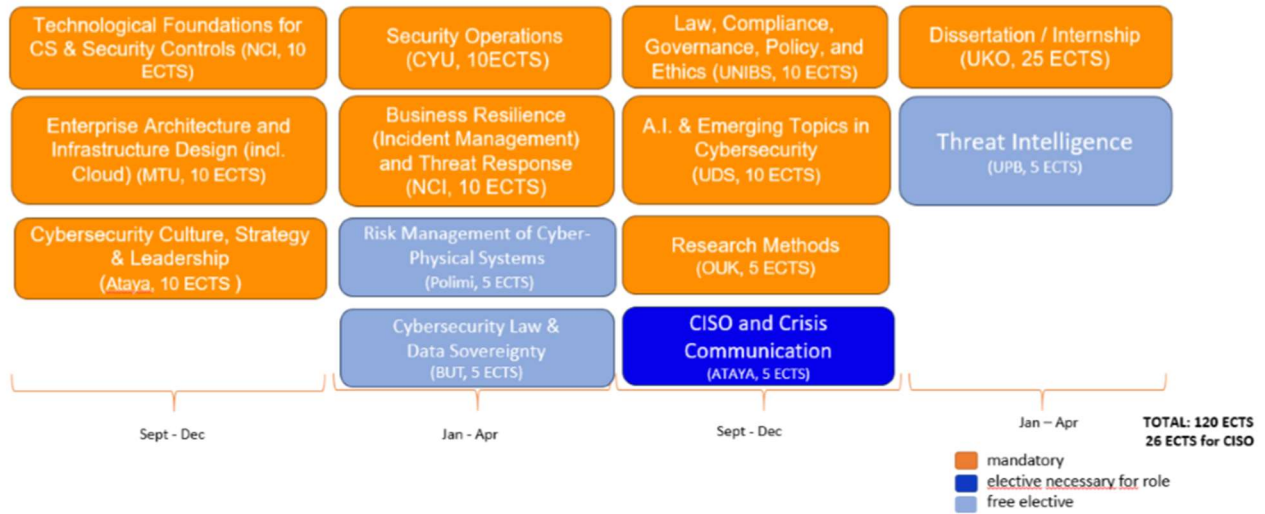


Fig. 2: A 120 ECTS Master's Programme Preparing for the Role of *Cyber Legal, Policy, and Compliance Officer* - Possible Pathway in a 2-Year Full Time Programme



Fig. 3: A 120 ECTS Master's Programme Preparing for the Role of *Cybersecurity Risk Manager* - Possible Pathway in a 2-Year Full Time Programme

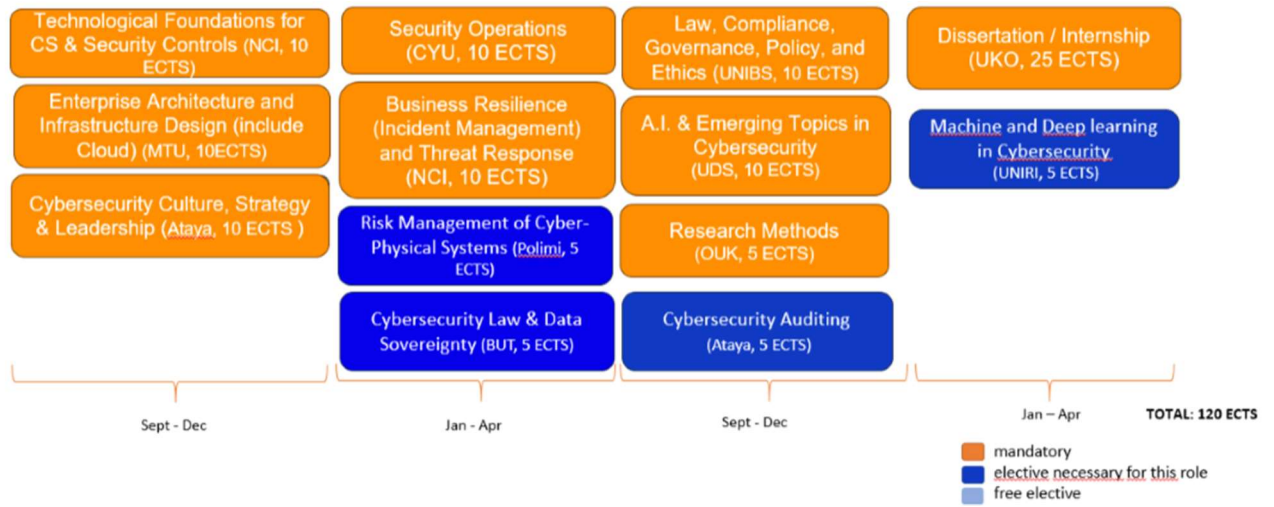


Fig. 4: A 120 ECTS Master's Programme Preparing for the Role of *Cyber Threat Intelligence Specialist* - Possible Pathway in a 2-Year Full Time Programme

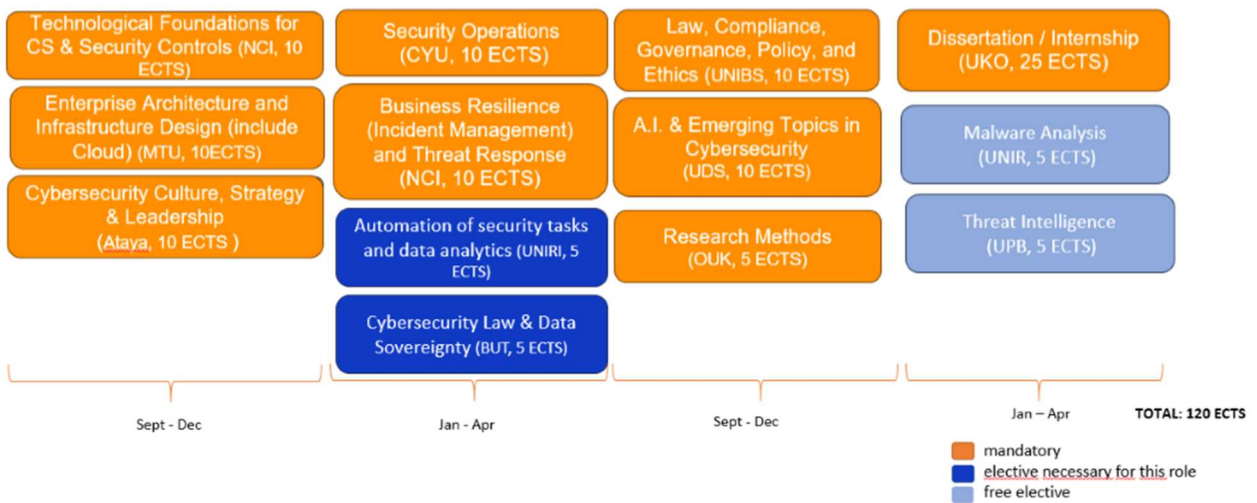


Fig. 5: A 120 ECTS Master's Programme Preparing for the Role of *Cybersecurity Educator* - Possible Pathway in a 2-Year Full Time Programme

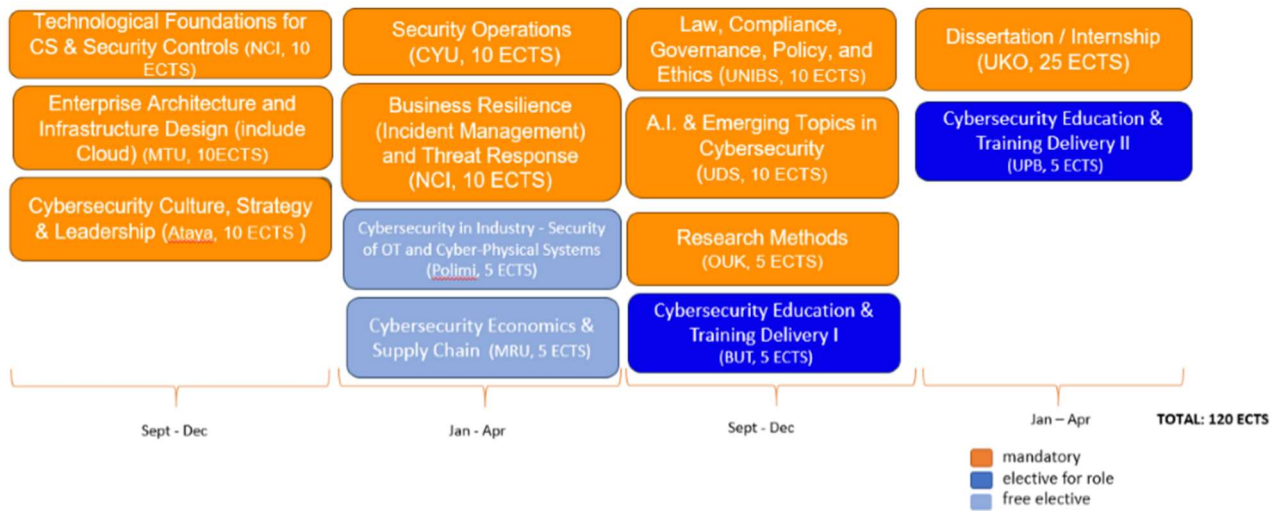
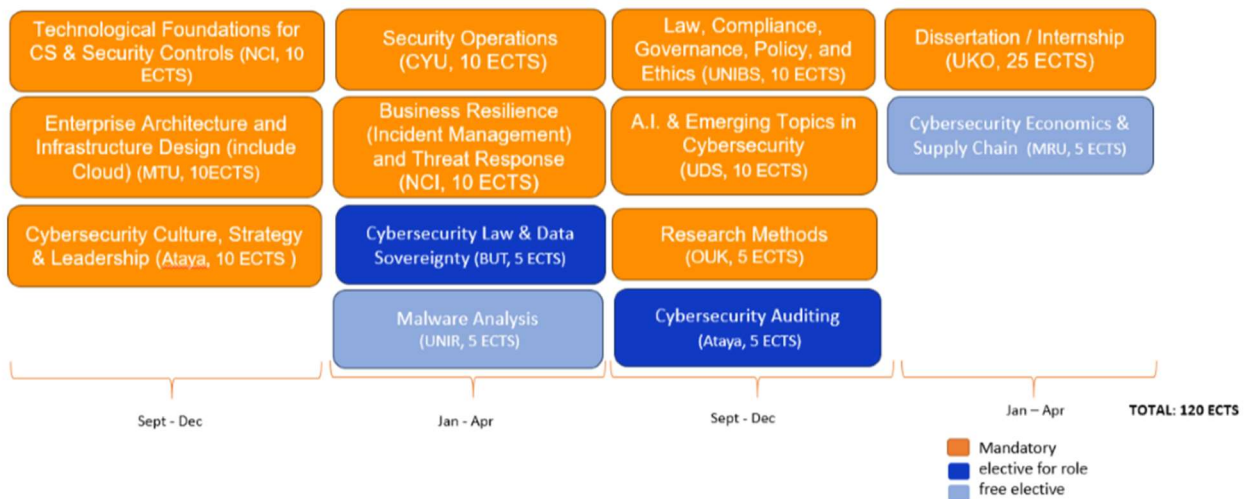


Fig.6: A 120 ECTS Master's Programme Preparing for the Role of *Cybersecurity Auditor* - Possible Pathway in a 2-Year Full Time Programme



C. Technical Specifications of Moodle Setup

The Moodle platform serving as the backbone of the Digital4Security Master's Programme has been meticulously set up to provide a scalable, secure, and user-friendly environment. The technical specifications and configurations of this setup are thoroughly detailed in Deliverable D3.1 Digital Learning Platform and Teaching Tools.

The platform is hosted on a secure cloud-based infrastructure to ensure reliability, data integrity, and 24/7 availability. It leverages the latest version of Moodle, enhanced with custom plugins to support interactive learning and advanced analytics. The Moodle environment has been optimized for accessibility, scalability, and seamless integration with third-party tools such as BigBlueButton for live sessions and H5P for interactive content.

Key aspects of the Moodle setup include:

- A robust hosting environment to support a high number of concurrent users.
- Advanced security measures, including HTTPS encryption and GDPR-compliant data handling.
- A modular and flexible design to accommodate future updates and expansions.
- Integration with tools for collaboration, assessment, and learner analytics.

For a complete overview of the technical setup, including system architecture, server specifications, and security protocols, please refer to the detailed documentation in Deliverable D3.1.

D. Accessibility and Compliance Reports

The accessibility and compliance measures implemented in the Digital4Security Digital Learning Platform are comprehensively detailed in Deliverable D3.1 Digital Learning Platform and Teaching Tools. This document provides an in-depth overview of how the Moodle Learning Management System (LMS) was configured to adhere to the Web Content Accessibility Guidelines (WCAG), ensuring the platform is inclusive for all learners.

The accessibility features described include support for screen readers, the use of descriptive alt text for images, captioning for multimedia content, and a navigation structure designed to accommodate individuals with disabilities. These measures ensure that the platform provides a seamless and equitable learning experience for all users, regardless of their abilities.

Deliverable D3.1 outlines the platform's compliance with GDPR regulations. This includes detailed descriptions of how data collection, processing, and storage align with European Union legal requirements. Specific areas covered include data encryption protocols, the safeguarding of user rights (such as access, rectification, and deletion of personal data), and the implementation of privacy disclaimers and cookie management processes.

For a complete technical description of these measures, Deliverable D3.1 serves as the primary reference, offering exhaustive details and supporting documentation on accessibility and compliance standards.

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Copyright © 2023 by Digital4Security Consortium



Digital4Security

Shaping Europe's cyber future

