EAGLE
DIGITAL SKILLS TRAINING

Project EAGLE

CovEring the trAining Gap in digital skills
for European SMEs manpowEr

This project has received funding from the European Union’s Digital Europe Programme (DIGITAL) under grant agreement No 101100660. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

EAGLE
DIGITAL SKILLS TRAINING

CovEring the trAining Gap in digital skills for European SMEs manpowEr

Objectives

- To provide access to high-level educative contents regarding digitalization and new technologies, specifically to SMEs managers and staff; contributing to bridge the digital divide between large, multinational companies and the rest of society.
- To strengthen the relationship between private companies, especially SMEs; and Higher Education Institutions.
- To contribute to digital transformation of businesses.
- To increase the number of professionals able to design, develop and deploy digital solutions in the economy and across sectors.

ABOUT

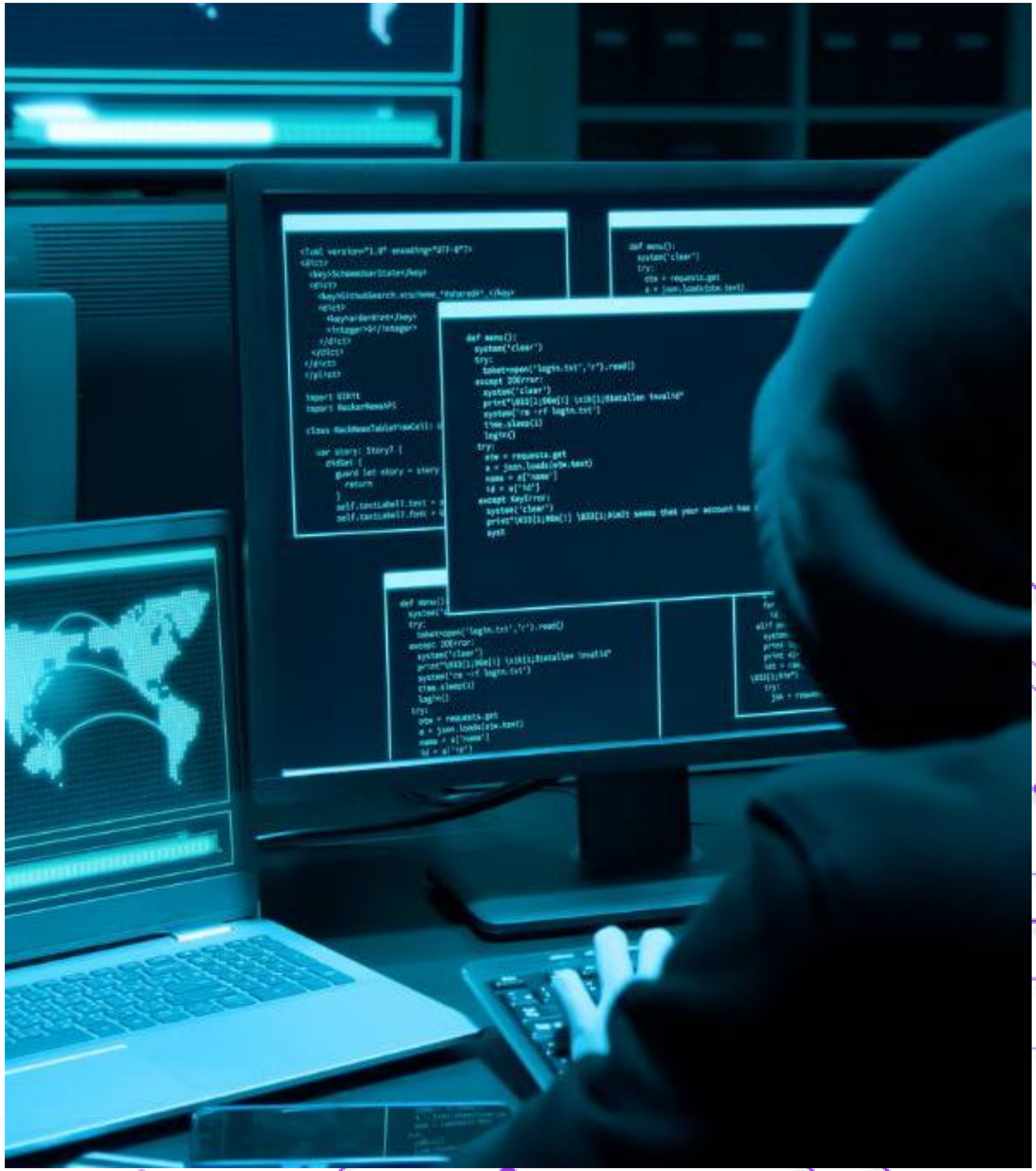
This project has received funding from the European Union’s Digital Europe Programme (DIGITAL) under grant agreement No 101100660. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Cybercrime, cyber threats and cybersecurity

Learning outcomes:

Upon the completion of the course, the participant will:

1. Understand main cybercrime and cybersecurity concepts.
2. Recognize cyberthreats (including hybrd-cyber threats) and be able to manage internal and external processes during (and after) a cyber incident.
3. Understand cybersecurity legal regulation and responsibilities of SME`s. To be able to aply cybersecurity legal norms in practice.
4. Know how to increase the cyber security culture in the organization, how to assess cybersecurity risks and apply risk mitigation measures.
5. Understand the essential organizational and technical cybersecurity measures. Be able to use automated cyber security risk assessment tools.
6. Understand the responsibilities and liability of different groups of employees in ensuring cyber security and prevention of cyber crimes. To be able to determine and control the performance of employees' duties in practice.

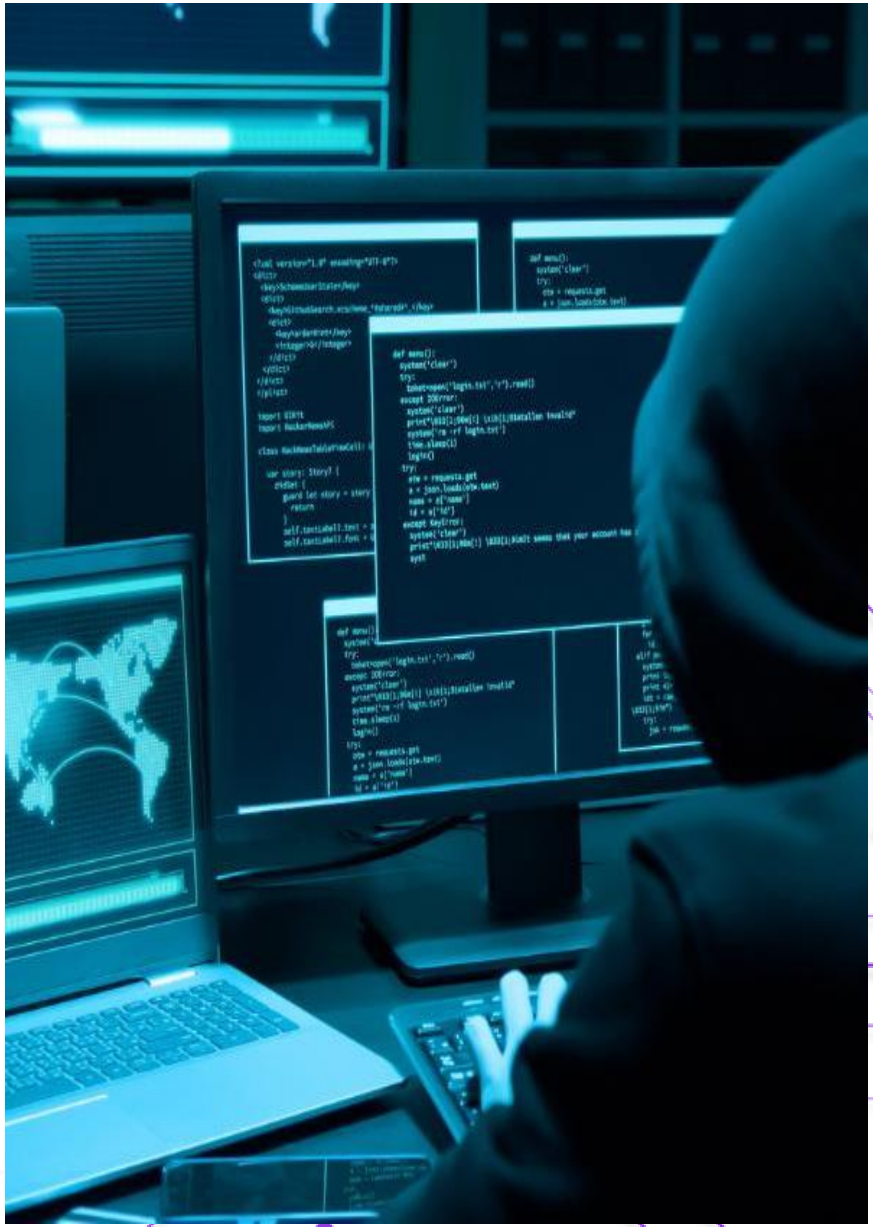


Co-funded by
the European Union

Cybercrime, cyber threats and cybersecurity

1. Cybercrime, cybersecurity management competence and awareness, employess responsibilities and legal liability

- Cybersecurity&data privacy and cybercrime: main concepts and definitions.
- Cybersecurity&data privacy and cybercrime: legal environment.
- Cyber threats: how to recognize cyber threats. Cyber threat trends. The most common vulnerabilities.
- Hybrid threats. Practical examples.
- What must the company and/or institution ensure in order to protect itself from cyber threats?
- Knowledge of managers in the field of cyber security and their communication to employees.
- Internal cybersecurity documents. Formal compliance - how to avoid it?
- Organizational and technical security measures. Business continuity plan, etc. The importance of cyber hygiene.
- Employee duties according to the relevant segmented groups. Employee`s liability.
- How to assess the readiness of employees to recognize cyber threats? Effective methods of protection against social engineering.

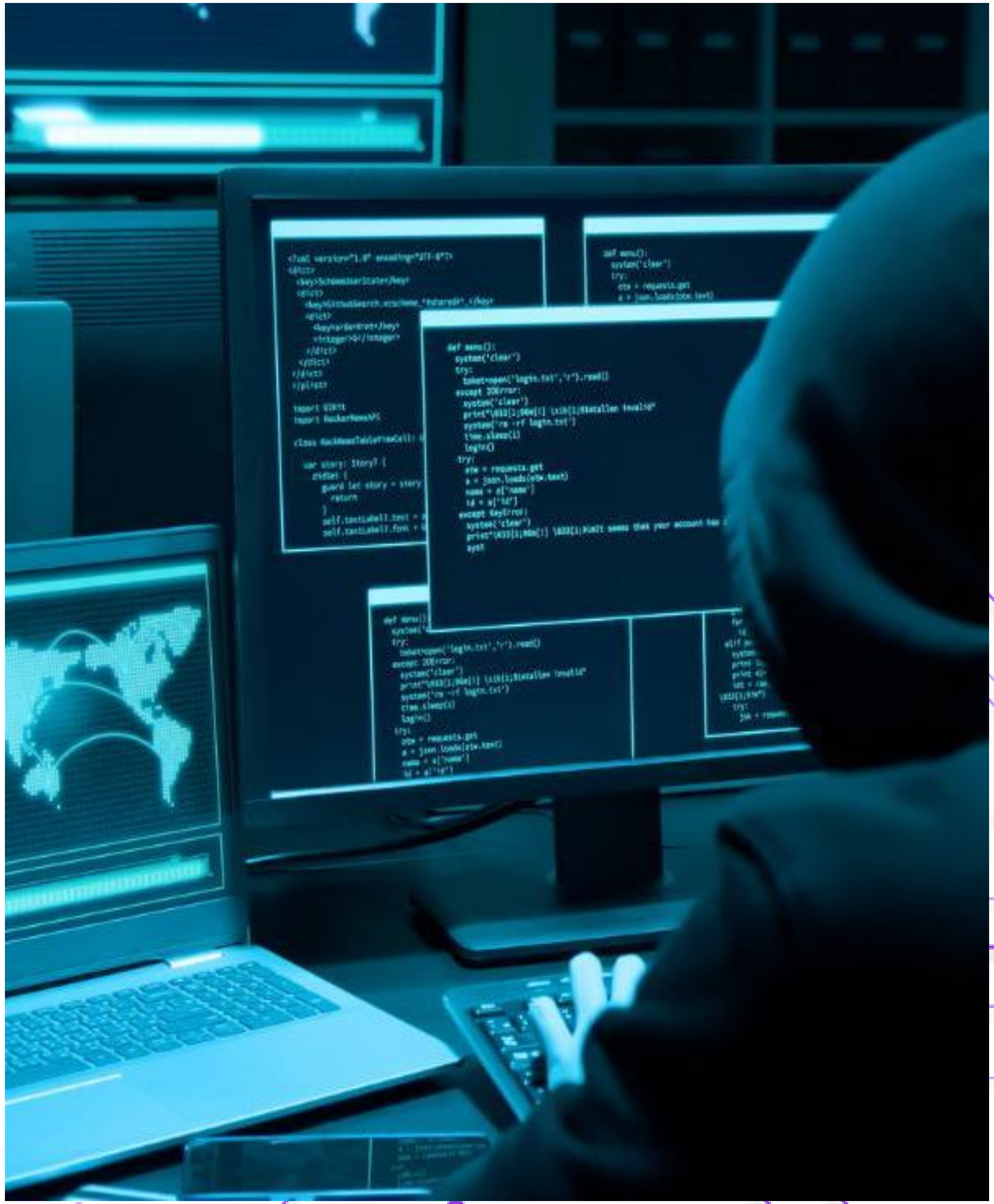


Co-funded by
the European Union

Cybercrime, cyber threats and cybersecurity

2. Cybersecurity risk assesment (data privacy impact assesment), cybersecurity incident management.

- Cybersecurity risk assesment. Risk assesment automatic tools.
- Assessment and control of suppliers' cyber security measures.
- Cyber incidents: types and duties during such incidents. How to internally and externally report a security incident. Relationship with cybercrime and personal data security breach.
- Responsible disclosure.
- How to deal with a crisis caused by a cyberattack? Practical examples.
- Awareness of cyber incidents / cybercrime and awareness through consequences.
- Institutions responsible for cybersecurity, cybercrime and data privacy. Their functions, examples of sanctions, etc.
- Practical part:
  1) Cybersecurity risk assesment using automatic risk assesment tool;
  2) Phishing exercise.



Co-funded by
the European Union

EAGLE

DIGITAL SKILLS TRAINING

When assessing the knowledge of participants who have completed the training, it is important to ensure that the assessment process is objective and adequately reflects the competences acquired by participants. This methodology is divided into two main evaluation methods, each of which will account for 50% of the final evaluation:

1. **Answering the questions and selecting the correct answer**:

- Number and format of questions: Participants will be asked to answer 15 questions. Each question will have between three and five answer choices, only one of which will be correct.
- Assessment: Participants will be required to select one correct answer for each question. Successful participants will be those who get at least 80% of the answers correct.

2. **Completion of the two practical exercises**:

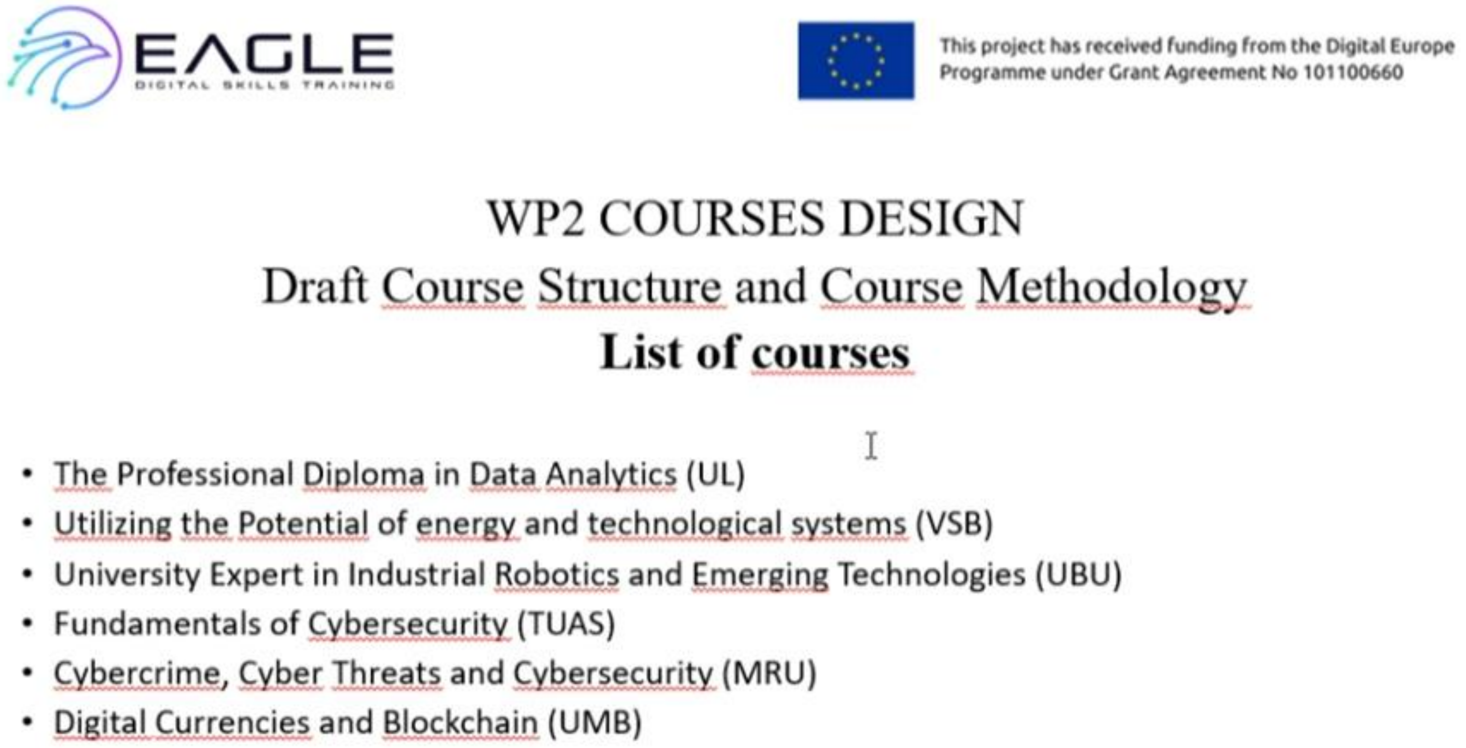
- Practical tasks. Participants will be required to complete two practical tasks which will be related to their training material and applied to their activity context:

✓ Cybersecurity risk assessment using automatic risk assessment tool;

✓ Phishing exercise.

- Assessment process: Successful completion of the exercises means that the participant has not only performed the exercises correctly (e.g. completed them to completion) but also presented the results adequately. This means that the evaluation will not only be based on the correctness of the tasks, but also on the quality of the presentation and the ability to communicate clearly.

Co-funded by
the European Union



EAGLE DIGITAL SKILLS TRAINING

This project has received funding from the Digital Europe Programme under Grant Agreement No 101100660

WP2 COURSES DESIGN

Draft Course Structure and Course Methodology

List of courses

- The Professional Diploma in Data Analytics (UL)
- Utilizing the Potential of energy and technological systems (VSB)
- University Expert in Industrial Robotics and Emerging Technologies (UBU)
- Fundamentals of Cybersecurity (TUAS)
- Cybercrime, Cyber Threats and Cybersecurity (MRU)
- Digital Currencies and Blockchain (UMB)

Co-funded by
the European Union