Co-funded by the European Union

D3.1 TRAINING MODULES FOR HEI STUDENTS

CYBER AGENT 09.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Work Package 3: CyberAgent Learning resource development

Deliverable 3.1: Training modules for HEI students

Leader of WP3 – TIMTAL. Leader of D3.1 – VU.

CONTENT

INTRODUCTION

According to the D2.2 report, SMEs face a significant shortage of qualified cybersecurity specialists, and existing employees often lack the systemic knowledge required to respond appropriately to increasingly complex cyber threats. Therefore, it is particularly important in higher education to prepare specialists who can apply their knowledge in the SME environment – in both technical and managerial areas. In light of this, a competency-based learning pathway, divided into different thematic areas and focused on the development of practical skills, was created in the D2.3 document.

This document presents one of the main project deliverables – the training modules for higher education (HEI) students (D3.1). The objective of this activity is to create training syllabuses for higher education institutions (HEI) that cover the key areas of cybersecurity knowledge, skills, and competencies relevant to small and medium-sized enterprises (SMEs).

These modules are the result of consistent work based on a detailed needs analysis (D2.2), during which representatives from SMEs, vocational education and training (VET), and higher education institutions were surveyed, as well as a clearly defined learning pathway structure (D2.3).

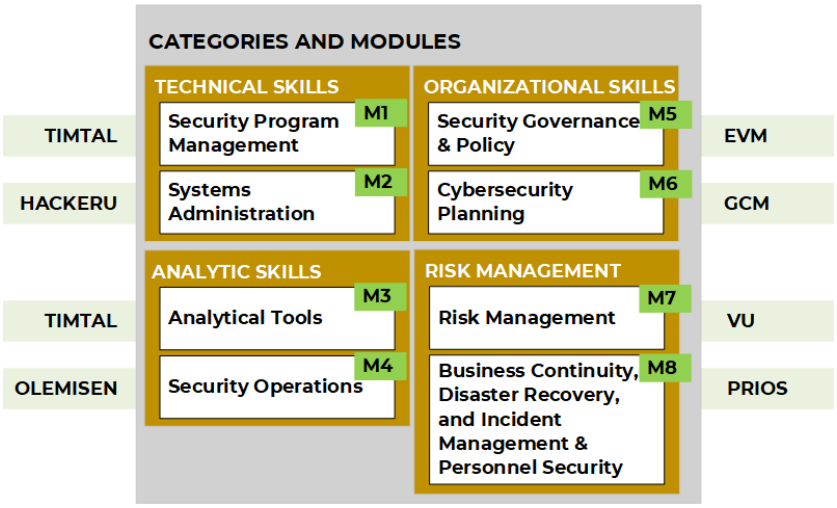
The training program, corresponding to the European Qualifications Framework (EQF) levels 5–6, is designed for higher education students and advanced SME employees. It consists of eight core modules and one inspirational module, covering four essential competency areas:

- **Technical Skills** (Security Program Management, Systems Administration).
- **Analytic Skills** (Analytical Tools, Security Operations).
- **Organizational Skills** (Security Governance & Policy, Cybersecurity Planning).
- **Risk Management** (Risk Management and Mitigation, Business Continuity, Disaster Recovery, and Incident Management & Personnel Security).

Each module is worth 3 ECTS credits (corresponding to a 75-hour student workload), is aligned with the principles of the Higher Education Area, and adheres to the methodological recommendations specified in D2.3: education is based on active learning methods (e.g., case studies, project-based learning) and self-directed learning, with learning outcomes clearly distinguished at the levels of knowledge, skills, and competencies.

Each 3 ECTS credit module was developed by different consortium partners, leveraging their specific field and professional experience.

The developed modules cover the following key areas, identified as critically important in the D2.2 report:



1. M1: SECURITY PROGRAM MANAGEMENT

Module title	Module code
SECURITY PROGRAM MANAGEMENT	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, hybrid	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75 hours	50 hours	25 hours

Purpose and outcomes of the module		
After finishing this course, students will be equipped with the skills to effectively manage security programs in response to cybersecurity threats. They will develop defence strategies against current threats such as phishing, ransomware, and DDoS attacks within the frameworks of project and resource management. Additionally, students will learn to apply security metrics and quality assurance methods, gaining the ability to optimize security programs, manage resources efficiently, and enhance organizational security by utilizing appropriate tools against evolving threats. This course will also build their competence in threat assessment, reporting, and communication, enabling them to implement cybersecurity strategies effectively within their organizations.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain practical knowledge on the latest cybersecurity threats, including phishing, ransomware, and DDoS attacks, and how to manage these through effective project and resource management, and implementation of quality assurance and control measures.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. theoretical lectures, guest speakers, quizzes, games, practical tasks/labs, peer-to-peer teaching and learning, self-guided learning etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests Knowledge assessment test

Skills: Learners will be skilled to utilize tools and software for protection against evolving cyber threats, and apply robust security practices in project and resource management to enhance the overall security metrics and quality control within their organizations.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. practical tasks/labs, hands-on activities, simulated environments, quizzes, games, case studies etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Practical assessments
Competences: Learners will be competent in assessing and mitigating potential security threats, effectively communicating cybersecurity issues, and accurately reporting threats and breaches through the appropriate channels within their organization.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. simulated environments, capture the flag competitions, 5Es, CBL, CL, POGIL, PBL etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Simulations Competitions

Module content: breakdown of the topics	**Contact work hours**					**Individual work hours and tasks**	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	**All contact**	**Individual**	**Tasks**
Project management • Project Planning • Defining Project Objectives • Defining Project Scope and Requirements • Preparing the Project Schedule • Project Management Tools • Current Cybersecurity Threats (DDoS, Ransomware, Malware, Phishing, Zero-Day, IoT attacks, etc.) • Threat Modelling and Vulnerability Analysis • Emergency and Incident Response Plans • Reporting Cybersecurity Threats and Incidents	8	0,5	3	0,5	**12**	**6**	• Plan a cybersecurity awareness project for SME employees. • Define clear objectives for the cybersecurity awareness project to enhance SME employees' understanding of potential security threats. • Outline the scope and requirements of the cybersecurity awareness project for SME employees, including training topics and necessary resources. • Prepare the timeline for the cybersecurity awareness project for SME employees.

							• Use project management tools to monitor progress and resource utilization for the cybersecurity awareness project aimed at SME employees. • Research current cybersecurity threats and compile the findings into a report. • Create a simplified threat model to help SME employees identify potential security vulnerabilities in their daily operations. • Find and review examples of emergency and incident response plans. • What steps should be considered when preparing a report on reporting cybersecurity threats and incidents? Research and summarize.
Resource management • Human Resources (Project Teams) Management • Security Awareness and Team Training • Hardware and Software Inventory Management • Security Tools and Software • Effective Use of Technological Resources • Budget and Resource Allocation	8	0,5	3	0,5	**12**	**6**	• Plan a resource management strategy to ensure the effective use of resources for a fictional SME. • Create a sample topic plan for cybersecurity awareness training. • Prepare a hardware and software inventory for a fictional SME. • Research commonly used security tools and software. • Create a sample budget and resource allocation plan for a hypothetical SME.
Security metrics • Security Metrics and Measurement Techniques • Data Collection with SIEM • Analysis of Security Metrics • Project Monitoring and Performance Evaluation	8	0,5	4	0,5	**13**	**6**	• Research the security metrics used to assess the cybersecurity posture in SMEs. • Research the sources from which SIEM software collects logs.

• Review of Actions and Project Adaptation • Reporting of Security Metrics							• Set up and examine an open-source SIEM software. • Analyze security metrics by collecting logs using SIEM software. • Report the analysis results of security metrics with graphs and visuals.
Quality assurance and quality control • Quality Management • Quality Standards in Cybersecurity • Compliance and Quality Audits • Testing and Validation Techniques • Evaluation and Improvement Recommendations	8	0,5	4	0,5	**13**	**7**	• How should quality assurance and quality control processes be planned to enhance the effectiveness of cybersecurity applications in SMEs? Research and summarize. • Research the Annex A Control Items of ISO/IEC 27001:2022. • Research and report on what testing and validation techniques are. • What benefits do continuous review and improvement of quality processes provide to SMEs?
Total	**32**	**2**	**14**	**2**	**50**	**25**	

Assessment strategy	**Comparative weight percentage**	**Assessment criteria**
Self-assessment test I	10%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers. 3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.
Self-assessment test II	10%	
Self-assessment test III	10%	
Self-assessment test IV	10%	
Knowledge assessment test	60%	

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading

Recommended reading
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: SYSTEMS ADMINISTRATION

Module title	Module code
SYSTEMS ADMINISTRATION	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, blended	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module
After finishing this course students will be able to continuously manage (identify, analyse, assess, estimate, mitigate) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Students will know Networking fundamentals to properly manage network devices, operate on both Linux and Windows servers managing and securing it. Also knowledge about Cloud and AI in the context of cybersecurity will be very useful for them to properly speed up tasks and perform automations and scaling. Students will also learn how to harden systems, perform threat hunting and make servers available (acronym from CIA triad).

Learning outcomes of the module	Teaching and learning methods	Assessment methods
Knowledge: Learners will gain knowledge in Network Administration, Operating Systems, Network Fundamentals, Network Administration Tools, Network devices security, Linux System Administration, Windows System Administration, Virtualization, Cloud Computing using AI for networking and cybersecurity procedures, Cybersecurity Procedures, Threat Detection, Threat Analysis, Threat Response, Threat Remediation, Cybersecurity Fundamentals, Defending organisation against attacks, Infrastructure & Network Security, Network Monitoring & Analysis, Incident Handling. They will be able to establish and describe effective system administration procedures ,operational routines tailored to the specific needs of SME workplaces in compliance standards.	To be selected by the lecturer, live classes, video recordings, presentations, virtual appliances (if applicable), literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring.	Self-assessment tests and knowledge assessment tests
Skills: Learners will be skilled to use methodologies and tools to design and implement secure system architectures—including operating systems, databases, networks, and cloud infrastructures for SME workplaces.	To be selected by the lecturer, live classes, video recordings, presentations, virtual appliances (if applicable), literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring.	Self-assessment tests and knowledge assessment tests
Competences: Learners will be competent to develop and implement strategic cybersecurity frameworks for system administration, leading projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.	To be selected by the lecturer, live classes, video recordings, presentations, virtual appliances (if applicable), literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring.	Self-assessment tests and knowledge assessment tests

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	All contact	Individual work	Tasks
Operating system administration • Operating Systems • Relationship Between Hardware and Software • Binaries, Hexadecimal Counting • Bits & Bytes • Command Line in OS • Windows & Linux Commands • Windows Client & Server • Applications, Processes, and Services in Windows • File Extensions & Types • Registry Keys and Values • Control Panel Settings • Users and Groups • Domain Structure & Server Manager • AD & GPO • Linux Interfaces & Kernel • Processes in Linux • File & Directory Naming Conventions • Linux Shells & Command Syntax • Manipulating Files & Folders • Working with Pipe & System Monitoring Commands • Process Management & Job Control • Service Management	4	0,5	2	0,5	**7**	**3,5**	Hexadecimal Counting Practicing Windows Commands Practicing Linux Commands Practicing the Task Manager Creation of files and management Modification and viewing Registry Keys and Values Modyfing Control Panel Settings Managing Users and Groups Managing Domain Structure Creating and deleting Active Directory Objects Managing Processes in Linux Manipulating Files & Folders Working with Pipe System Monitoring Commands Managing Linux Services
Database system administration • Repositories & Source Lists • Managing a Web Server • System Logs & Log Monitoring • Scheduling Tasks in Linux • Server & Network Troubleshooting • Backup & Recovery • Securing the GRUB • Firewalls • Active Directory Objects & GPO Management • DNS & DHCP • PowerShell Fundamentals	4	0,5	2	0,5	**7**	**3,5**	Managing repositories & Source Lists Managing a Web Server Verifing and managing system Logs & Log Monitoring Scheduling Tasks in Linux Server Troubleshooting Restoring Backups Securing the GRUB Managing DB services Setting up Password Policies

• Microsoft BitLocker, AppLocker & Firewall • LDAP & Kerberos • NTLM • Password & Lockout Policies • Authentication & Access Control • Internet Control Message Protocol (ICMP) • TCP vs UDP • NetBIOS & SMB • SSL & TLS • Certificates • Telnet and Secure Shell (SSH) Protocols • HTTP & HTTPS • Mail Systems Protocols • Domain Name System Protocol (DNS) • FTP & RDP • Encapsulation Vs. Decapsulation • Network Sniffers & Wireshark • TCP/UDP • DHCP, DNS							Setting up Account Lockout Policies Setting up Authentication & Access Control
Network administration • Network Types & Wireless Networks • Networks & Topologies • Devices Identity & Access Devices • Infrastructure & Security Devices • Specialized Devices & Network Architecture • Virtual Networks • Physical and Logical Addresses • OSI & Network Models • Data Encapsulation and Decapsulation • Network Protocols and Port Numbers • Network Media and Cables • Wireless Technologies • Network Administration Tools • Cisco Packet Tracer • Network Classes & Subnetting • Address Resolution Protocol (ARP) • Static vs. Dynamic IP Addressing • Network Address Translation (NAT) • Switches & Cisco IOS • Switch Port Security & Router Interfaces • Configuring VLANs & DTP • Inter-VLAN Routing • Introduction to ACLs	4	0,5	2	0,5	**7**	**3,5**	Creating Network Topologies Managing Network Devices Building the Network Securing Network Devices Creating Virtual Networks Setting up Network Protocols and Port Numbers Working with Cisco Packet Tracer Working with Address Resolution Protocol (ARP) Planning a Network Setting up Static and Dynamic IP Addressing Configuring DHCP and NAT Working with Cisco IOS Configuring VLANs Network Troubleshooting

• Network Troubleshooting							
Cloud administration • Hypervisors & Virtual Machines • Containers • Securing Virtual Environments • Backup & Recovery • Cloud Computing & CSPs • What Are Cloud Service Models • Cloud Deployment Types • Virtual Networks • AWS Compute Services • Amazon Elastic Compute Cloud (EC2) • Cloud Monitoring Tools • Automation and Orchestration Tools • Cloud Security Threats and Vulnerabilities • Identity and Access Management (IAM) • Role-Based Access Control (RBAC) • Multi-Factor Authentication (MFA) • Cloud Data Encryption • Virtual Private Cloud (VPC) • Docker & Kubernetes	4	0,5	2	0,5	**7**	**3,5**	Creating Virtual Machines Setting up Containers Securing Virtual Environments Working with Backups Cloud Network Management Configuring Virtual Networks Working with Cloud Monitoring Tools Implementing Automation and Orchestration Detecting Cloud Security Threats and Vulnerabilities Setting up Identity and Access Management (IAM) Implementing Cloud Data Encryption Working with Docker and Kubernetes
Cyber-physical system administration • Security & Access Controls • Authentication Types • TACACS+ and RADIUS • AAA Configuration • Risk Management Goals • Encryption & Decryption • Hashing & Rainbow Tables • MAC Spoofing & ARP Poisoning • VLAN Hopping & Rogue DHCP • ICMP Flood • TCP & UDP Flood • Session Hijacking • DNS Spoofing • Defense in Depth (DID) & Zero Trust • Demilitarized Zones (DMZs) • Honeypots & Network Hardening • Best Practices for a Secure Network • VPNs • SSH & VNC • Stateful vs. Stateless Firewalls • Host-Based vs. Network-Based • Hardware vs. Software Firewalls • Web Application Firewall (WAF) • AI in Firewalls	4	0,5	2	0,5	**7**	**3,5**	Setting up Infrastructure Main Components Implementing Security Controls Working with TACACS+ and RADIUS AAA Configuration Playing with Encryption and Decryption Analyzing common attacks and defence techniques Setting up Demilitarized Zones (DMZs) Researching Honeypots Hardening via Best Practices for a Secure Network Installing VPN Working with Secure Shell (SSH) Working with Virtual Network Computing (VNC) Firewall Working Techniques Implementing AI in Firewalls

• IDS & IPS • NIDS & HIDS • Snort • tcpdump							Using Snort and tcpdump for protection and detection
System hardening • GenAI Techniques • Code Generation • User Account Management and Access Control • Anomaly Detection and Trouble-shooting • Resolving Apache2 Service Errors • Patch Management & Updates • Automated Backup & Recovery • IT Asset Management and Inven-tory • Recovering Deleted Files with GenAI • Cybersecurity Procedures • Threat Detection & Analysis • Threat Response & Remediation • Leveraging AI for Real-Time Threat Detection • Validating and Testing GenAI Mod-els • Governance and Regulatory Frameworks • DNS Configuration & Security • DHCP Configuration & Security • PowerShell Fundamentals • Switch Port Security • Network Basic Input/Output Sys-tem (NetBIOS) • Server Message Block Protocol (SMB) • Secure Sockets Layer (SSL) & Transport Layer Security (TLS) • Security Certificates • Mail Systems Protocols • Domain Name System Protocol (DNS) • File Transfer Protocol (FTP) • Remote Desktop Protocol (RDP) • Scheduling Tasks in Linux • Server Troubleshooting • Network Troubleshooting • Backup & Recovery • Securing the GRUB • Setting Up & Securing Firewalls	4	0,5	2	0,5	**7**	**3,5**	Working with GenAI Techniques User Account Management and Access Control Anomaly Detection and Troubleshooting Resolving Apache2 Service Errors with GenAI Configuring Patch Management and Updates Setting up automated Backup and Recovery Managing IT Assets Recovering Deleted Files with GenAI Implementing DNS and DHCP Security Working with Microsoft BitLocker and Microsoft AppLocker Setting up Microsoft Firewall Setting up Switch Port Security Securing File Transfer Protocol (FTP) Securing Remote Desktop Protocol (RDP) Scheduling Security Tasks in Linux Securing the GRUB Setting Up & Securing Firewalls (iptables)
Availability • IR vs. SOC • Events and Incidents	4	0,5	3	0,5	**8**	4	Detecting Events and Incidents Performing Alert Triage

• Alert Detection & Alert Triage • Documentation and Reporting • What Are Web Attacks? • DoS and DDoS • SQL Injection & XSS • Command Injection & Local File Inclusion (LFI) • Cross-Site Request Forgery (CSRF) • Brute-Force & Credential Stuffing • Pass the Hash & Pass the Ticket • LDAP Reconnaissance • Broken Access Control • Ransomware • Computer Virus & Worm • Trojan Horse & Adware • Keylogger & Cryptojacking • Fileless Malware • Understanding the Spread of Malware • Static and Dynamic Malware Analysis • Safe Malware Analysis • Hybrid Analysis Malware Investigation • Performing Static and Dynamic Malware Analysis • Managing IOCs & Password Policies • Acceptable Use Policies (AUP) • Bring Your Own Device (BYOD) Policies • Remote Access Policies							Making Documentation and proper Reporting Implementing Post-Incident Activities PErforming and protecting against DoS and DDoS Detecting Web attacks and Spread of Malware Performing Safe Static and Dynamic Malware Analysis Managing IOCs Setting up Password Policies Setting up Bring Your Own Device (BYOD) Policies Setting up Remote Access Policies
Total	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Assessment strategy	**Comparative weight percentage**	**Assessment criteria**
Self-assessment test (1)	5%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers. 3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.
Self-assessment test (2)	5%	
Self-assessment test (3)	5%	
Self-assessment test (4)	5%	
Self-assessment test (5)	5%	
Self-assessment test (6)	5%	
Self-assessment test (7)	5%	
Knowledge evaluation test	65%	

3. M3: ANALYTICAL TOOLS

Module title	Module code
ANALYTICAL TOOLS	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, hybrid	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module		
After finishing this course, students will be equipped with the skills to protect organizational assets using performance metrics, data analytics, and security intelligence. They will learn to effectively apply analytical tools to identify potential cybersecurity risks and vulnerabilities, leverage data-driven insights to enhance security measures, and utilize performance metrics related to passwords, browser usage, email, and data processing applications. By the end of the module, participants will be able to evaluate and mitigate potential security threats using appropriate tools and report any threats or disruptions to the correct regulatory channels.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain practical knowledge in how to apply performance measurements, data analytics, and security intelligence to protect organizational assets.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. theoretical lectures, guest speakers, quizzes, games, practical tasks/labs, peer-to-peer teaching and learning, self-guided learning etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests Knowledge assessment test

Skills: Learners will be skilled in using analytical tools to identify potential cybersecurity risks and vulnerabilities, apply data driven insights to strengthen cybersecurity practices, and utilize performance metrics to evaluate and enhance the security of passwords, browsing, email, and data handling.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. practical tasks/labs, hands-on activities, simulated environments, quizzes, games, case studies etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Practical assessments
Competences: Learners will be competent in assessing and mitigating potential security threats using analytical tools, accurately reporting threats and breaches to the appropriate channels within their organization.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. simulated environments, capture the flag competitions, 5Es, CBL, CL, POGIL, PBL etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Simulations Competitions

Module content: breakdown of the topics	**Contact work hours**					**Individual work hours and tasks**	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	**All contact work**	**Individual work**	**Tasks**
Performance measurements (metrics) • Performance Metrics • System and Network Monitoring • Monitoring Performance Metrics • Network Mapping • Vulnerability Scanning • Network Traffic Analysis	10	0,5	5	0,5	**16**	**8,5**	• Conduct research on performance metrics and tools. Compare performance monitoring tools and identify their differences. • Complete the Zabbix installation and perform the basic configuration. • Create an application to monitor performance metrics with Zabbix. • Identify vulnerabilities in the target system using network mapping software (such as nmap, rustscan, etc.) • Perform a vulnerability scan on the target sys-

							tem using Nessus software. Prepare a vulnerability testing report. • Perform network traffic analysis using Wireshark.
Data analytics • Data Collection • Data Cleaning and Preprocessing • Data Analysis • Data Visualization • Analytical Tools • Applications of Data Analytics in Cybersecurity	10	0,5	5	0,5	**16**	**8,5**	• Perform data cleaning and preprocessing steps on a dataset related to cybersecurity issues prepared for a hypothetical SME. • Analyze the cleaned and preprocessed dataset from the hypothetical SME and visualize the results. • What are examples of data analysis applications in cybersecurity? Please research.
Security intelligence • Understanding Security Intelligence • Sources of Security Intelligence • Threat Intelligence Collection Methods • Threat Intelligence Frameworks • AI-Driven Security Intelligence Platforms • Case Studies on Security Intelligence Applications	10	0,5	7	0,5	**18**	**8**	• Investigate how security intelligence contributes to the proactive security strategies of SMEs. • What are the most common sources for obtaining security intelligence? How do you assess the reliability of these sources? • Define the advantages and limitations of each threat intelligence collection method. • Explain the core features of threat intelligence frameworks such as MITRE ATT&CK and the Cyber Kill Chain. • Examine a real case study where security intelligence was utilized. Describe the intelligence collection methods used in that case study.
Total	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Assessment strategy	Comparative weight percentage	Assessment criteria
Self-assessment test I	15%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers. 3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.
Self-assessment test II	15%	
Self-assessment test III	15%	
Knowledge assessment test	55%	

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
...
Recommended reading
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: SECURITY OPERATIONS

Module title	Module code
SECURITY OPERATIONS	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module		
After finishing this course, students will be able to effectively manage security operations within ICT infrastructures, systems, and services. They will gain the skills to monitor, detect, respond to, and recover from cybersecurity incidents by applying best practices, tools, and frameworks relevant to security operations.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain advanced knowledge of security operations, including monitoring, detection, incident response, and recovery. They will be able to establish and describe effective cybersecurity operational routines tailored to the specific needs of SME workplaces in compliance cybersecurity standards.	To be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. theoretical lectures, literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring etc.] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests Knowledge assessment test

Skills: Learners will be skilled in applying advanced methodologies and tools to perform security operations tasks, design and implement effective monitoring strategies, conduct incident response, and develop robust operational routines specifically tailored for SME workplaces.	To be selected by the lecturer, from Part 1.3. *[Teaching Methods, e.g. theoretical lectures, literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring etc.]* of D2.3 "*SME Cyber Security Change Agents Learning Pathway's Structure*"	Self-assessment tests Knowledge assessment test
Competences: Learners will be competent in developing and implementing strategic security operations policies and procedures for SME workplaces.	To be selected by the lecturer, from Part 1.3. *[Teaching Methods, e.g. theoretical lectures, literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring etc.]* of D2.3 "*SME Cyber Security Change Agents Learning Pathway's Structure*"	Self-assessment tests Knowledge assessment test

Module content: breakdown of the topics	**Contact work hours**					**Individual work hours and tasks**	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	All contact	Individual work	Tasks
Security Operations fundamentals - Understanding Security Operations and SOC (Security Operations Centre) - Roles and responsibilities in Security Operations - Overview of security operations tools and technologies	6	0,5	2	0,5	**9**	6	Identify and understand the structure and function of a SOC, analyse various roles within security operations, research tools used in security operations and analyse a case study.

Security Convergence - Understanding security convergence - Fundamentals of physical security (physical security principles, protecting physical assets, policies) - Case study highlighting security convergence principles	8	0,5	4	0,5	**13**	6	Review the definition and principles of security convergence, acknowledge the importance of integrating physical and digital security operations, Identify and assess risks across cyber and physical domains.
Security Information and Events Management - Review of security monitoring principles - Implementing SIEM solutions	8	0,5	4	0,5	**13**	6	Introduction to security monitoring and SIEM implementation. Ccore principles such as log types, detection methods, and monitoring lifecycle. Practical aspects of deploying a SIEM, including architecture, data collection, rule creation, and alert management.
Security Operations Practices - Identify data sources and optimize log collection - Centralising alerts with the SIEM - Testing your SIEM	4	0,5	10	0,5	**15**	7	Comprehensive and practice-oriented training program with essential knowledge and practical skills in log management, SIEM configuration, and threat detection across diverse IT environments.
Total	**26**	**2**	**20**	**2**	**50**	**25**	

Assessment strategy	Comparative weight percentage	Assessment criteria
Self-assessment test (1)	10%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers. 3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.
Self-assessment test (2)	10%	
Self-assessment test (3)	10%	
Self-assessment test (4)	10%	
Knowledge evaluation test	60%	

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
Cybellium (2024). *Study Guide to Security Operations Centers (SOC): A Comprehensive Guide to Learn Security Operations Centers (SOC)* Muniz, J. (2021). *The Modern Security Operations Center*. Pearson Education. ENISA (2017). *Strategies for Incident Response and Cyber Crisis Cooperation*. **Strategies for incident response and cyber crisis cooperation — ENISA (europa.eu)**
Recommended reading
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Open-Source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC. Cybellium (2023). Managing a security operations center (SOC).

5. M5: SECURITY GOVERNANCE & POLICY

Module title	Module code
SECURITY GOVERNANCE & POLICY	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face / Online / Hybrid	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module
The subject "Security Governance and Policy" aims to prepare students to face the challenges of cybersecurity in SMEs, integrating security governance into the business strategy and ensuring compliance with legal regulations, such as the GDPR. The module covers aspects such as identifying threats and vulnerabilities, designing robust and adaptive security policies, and managing incidents effectively. In addition, it focuses on developing governance structures that assign clear roles in the organization, aligning cybersecurity with strategic objectives. Students will acquire technical competencies in cyber risk assessment and mitigation, and develop analysis skills to propose improvements in security maturity. They will also become skilled in effectively communicating cybersecurity needs to executives, supporting informed decision making and ensuring regulatory compliance and ethics in cybersecurity. The "Security Governance & Policy" module also incorporates a focused examination of phishing prevention, AI-driven cyber attacks, and ransomware management, analyzing how these specific threats require an integrated approach to governance and compliance. The effectiveness of security policies will not only be measured by their ability to prevent incidents but also by their adaptability to emerging threats and compliance with current legal regulations.

Learning outcomes of the	Teaching and learning methods	Assessment methods

module		
Knowledge: Learners will gain advance knowledge in how to implement new cybersecurity routines and workflows within SME workplaces, incorporating current cybersecurity principles, trends, and compliance with national and international legislation relevant to their industry. Gain advanced knowledge on how to integrate phishing prevention, manage AI-driven threats, and respond to ransomware within SME environments	**Lectures (Directed Readings):** Lectures will provide a solid conceptual foundation in cybersecurity, governance, privacy and compliance, encouraging active student participation. Includes interactive lectures that incorporate regular Q&A sessions, polls, and live problem-solving exercises. Using tools like Mentimeter amd Poll Everywhere, **Participation in Discussions and Forums:** Participation in discussions and forums will allow students to debate and critically analyze cybersecurity issues, fostering their argumentative skills. It will be applied to issues related to ethics, policies and decision making in cybersecurity. **Case Studies:** The case studies will allow students to analyze cybersecurity situations in SMEs, applying theoretical knowledge to solve real problems. They will focus on topics such as data breach management, ransomware, phishing, AI Driven Attacks, security policy implementation and governance.	**Self-assessment tests:** Self-tests allow students to assess their understanding of each subtopic through a variety of questions, providing continuous feedback to identify areas for improvement. They do not affect the final grade, but are key to self-directed learning. **Final Exam (Optional):** The final exam is optional and allows students to obtain a certificate of completion by evaluating their overall understanding of the course through developmental questions, case analysis and multiple choice. Passing it is required to obtain the certificate of completion, while those who do not take it will receive a certificate of attendance.
Skills: Learners will be skilled in using advanced methodologies to conduct risk assessments, design and implement new cybersecurity routines, and prepare response strategies, ensuring effective governance and compliance within SME workplaces. Develop skills in designing and implementing comprehensive cybersecurity routines that address advanced threats and ensure organizational	**Hands-on Workshops:** The hands-on workshops will allow students to apply cybersecurity concepts through exercises such as policy development and incident simulations, with real-time feedback from the instructor. They are designed to strengthen practical skills and prepare students to apply what they have learned in real situations. **Practical Work and Individual Projects:** Practical work and individual projects will allow students to apply cybersecurity concepts through tasks such as policy writing and risk analysis,	**Practical Assessments:** Practical assessments throughout the course will allow students to apply theoretical knowledge to simulated situations, such as cybersecurity policy development and incident simulations, with the objective of assessing their ability to solve real problems in the context of SMEs. **Group Projects:** Group projects will allow students

compliance.	developing autonomous work skills and practical application of theoretical knowledge. **Collaborative Projects:** Collaborative projects will allow students to work in teams to develop cybersecurity solutions for SMEs, including security policies and governance models. They will encourage teamwork, project management and practical application of acquired knowledge, with feedback from teachers and peers.	to develop a comprehensive cybersecurity project, from risk identification to the proposal of governance models and incident response plans, evaluating both the quality of the content and the ability to collaborate. This project is key to the final assessment and integrates all course learning.
Competences: Learners will be competent in developing and implementing strategic cybersecurity policies, leading initiatives to establish new routines and workflows at SME workplaces, and making ethical decisions that align with organizational goals and compliance requirements. Become competent in formulating and executing cybersecurity policies that prevent sophisticated cyber threats and ensure compliance with international cybersecurity regulations.	**Scenario Simulations:** Scenario simulations will allow students to manage cybersecurity incidents in virtual environments that replicate real attacks, making strategic decisions under pressure. This method enhances skills in crisis management and incident response, and is key to teaching security policy evaluation and decision making in critical situations. Students will need to demonstrate how they would apply governance policies to prevent or respond to specific incidents such as phishing attacks, Ransomware and AI Driven Attacks; assessing their understanding of the relevant regulatory framework.	**Simulations and Incident Management:** Students will be evaluated on their ability to manage cybersecurity incidents in simulations that replicate real crises in an SME. The objective is to measure their ability to handle pressure, make strategic decisions and execute response plans in real time, evaluating their practical application in dynamic situations.

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	All contact	Individual	Tasks
Organizational context -Evolution of cybersecurity in SMEs -Current major threats and vulnerabilities -Impact of cybersecurity on business strategy -Specific challenges of cybersecurity in SMEs versus large enterprises - Understand the regulatory implications of cybersecurity practices and how they align with governance structures. - Common cybersecurity challenges specific to SMEs, such as limited budgets, lack of dedicated security staff, and practical methods for prioritizing cybersecurity investments.	5	0,5	3	0,5	**9**	**4**	Reading, research, case study preparation
Privacy -Privacy principles in cybersecurity -Personal data protection and GDPR -Impact of privacy on SME operations -Tools and techniques for privacy protection	4	0,5	3	0,5	**8**	**4**	Policy analysis, individual assignment
Laws, ethics, and compliance -Cybersecurity Organizations, Policies and Standards -Relevant national and international legislation -Regulatory compliance in SMEs -Ethics in Cybersecurity -Legal consequences of non-compliance in cybersecurity - Analysis of how AI-based tools can be utilized to strengthen cybersecurity governance and ensure compliance through continuous monitoring and automated threat response.	5	0,5	3	0,5	**9**	**5**	Case study, legislation analysis
Security governance -Cybersecurity governance structure -Roles and responsibilities in security management -Cybersecurity maturity models -Integration of cybersecurity into corporate governance	4	0,5	3	0,5	**8**	**4**	Risk management scenario analysis

- Enhance abilities in conducting risk assessments and formulating strategic response plans under simulated crisis conditions (Ransomware, phishing attack, ...)							
Executive and board level communication -Cybersecurity communication strategies -Security reporting to senior management -Decision making based on security data -Crisis management and communication in cybersecurity - Master crisis management and decision-making skills in high-stress scenarios involving AI-driven attacks and ransomware.	4	0,5	3	0,5	**8**	**4**	Presentation preparation, stakeholder communication
Managerial policy -Security policy development -Policy implementation and monitoring -Evaluation and continuous improvement of policies -Adaptation of security policies to technological and regulatory changes - Exploration of how effective training and awareness policies can be a crucial component of regulatory compliance and risk mitigation.	4	0,5	3	0,5	**8**	**4**	Writing and revision of a policy document
Total	**26**	**3**	**18**	**3**	**50**	**25**	

Assessment strategy	**Comparative weight percentage**	**Assessment criteria**
Self-test I	10%	Assessment of fundamental concepts on organizational context.
Self-test II	10%	Assessment of fundamental concepts on privacy.
Self-test III	10%	Evaluation of laws, ethics and compliance policies.
Self-test IV	10%	Evaluation of cybersecurity policies.
Self-test V	10%	Assessment of executive-level communication.
Self-test VI	10%	Evaluation of managerial policies and policy creation in security.
Knowledge evaluation test	40%	Final exam covering integrative questions on all course topics.
10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers.		

6 points – 55-64 % correct answers.
5 points – 45-54 % correct answers.
4 points – 35-44 % correct answers.
3 points – 25-34 % correct answers.
2 points – 15-24 % correct answers.
1 points – 0-14 % correct answers.

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*

Required reading

...

"EU Cybersecurity Law: Governing Resilience and Coherence in the Digital Age" by Luisa Marin

- This book provides an in-depth analysis of the EU's cybersecurity laws and policies, crucial for understanding how cybersecurity governance is structured and implemented within the EU context.

"Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy" by George Christou

- This book explores the governance frameworks and policy-making processes for cybersecurity within the EU, helping students understand the dynamic interplay between different governance levels.

"Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers

- While not EU-specific, this book's detailed exploration of phishing techniques and countermeasures can be contextualized within the EU by focusing on GDPR compliaanddata protection principles.

"European Cybersecurity Law and Regulation" edited by Nadya Purtova and Bert-Jaap Koops

- This edited volume covers the legal and regulatory measures specific to cybersecurity in the European Union, including compliance challenges and frameworks like the NIS Directive and GDPR.

"Ransomware: Understanding Digital Extortion and its Threat to Your Organization" by Allan Liska and Timothy Gallo

- This text, supplemented with EU-specific case studies and examples, will help students understand the implications of ransomware attacks under EU regulations.

Recommended reading

"The EU General Data Protection Regulation (GDPR): A Commentary" by Lukas Feiler and Nikolaus Forgó

- This commentary provides detailed insights into GDPR, essential for understanding the regulatory landscape in the EU and its impact on cybersecurity practices.

"Data Protection and Cybersecurity in Europe: Legal Frameworks and Practical Considerations" by Paul Lambert

- This book offers practical insights into the alignment of data protection and cybersecurity strategies in the EU, including compliance with regulations and best practices for security measures.

"Network and Information Security: European and International Perspectives" edited by Jeanne Pia Mifsud Bonnici and Joe Cannataci

- This collection examines the network and information security landscape from both European and international perspectives, providing a broader context for the EU's cybersecurity efforts.

"Artificial Intelligence in Cybersecurity: Practices, Challenges, and Ethics" by Elena Fersman and Martin Fredriksson

- A comprehensive overview of the integration of AI technologies in cybersecurity, addressing ethical, operational, and regulatory challenges, especially pertinent in the EU context.

"Cybersecurity in the Digital Age: Tools, Techniques, and Applications" by Gregory B. White, Eric A. Fisher, and James L. Antonakos

- While not exclusively focused on the EU, this book covers a wide range of modern cybersecurity too

Studies material *(HackerU and Cybint original materials)*
Required reading
• TCP/IP Network Administration: Help for Unix System Administrators 3rd Edition, by Craig Hunt (O'Reilly) • Essential System Administration Pocket Reference: Commands and File Formats (Pocket Administrator) by Eleen Frisch (O'Reilly) • Computer Networking: The Beginner's guide for Mastering Computer Networking, the Internet and the OSI Model by Ramon Nastase
Recommended reading
• CompTIA A+ Certification All-in-One For Dummies (Computer/Tech) 5th Edition by Glen E. Clarke, Edward Tetz, Timothy L. Warner • Coding All-in-One For Dummies 1st Edition by Nikhil Abraham • Information Technology Essentials Volume 1: Introduction to Information Systems by Eric Frick • IT Architecture For Dummies 1st Edition by Kalani Kirk Hausman, Susan L. Cook • Cybersecurity For Dummies (Computer/Tech) 1st Edition by Steinberg • Linux For Dummies, 10th Edition 10th Edition by Richard Blum • Windows 10 For Dummies, 3rd Edition (Computer/Tech) 3rd Edition by Rathbone • Networking For Dummies 12th Edition by Doug Lowe

6. M6: CYBERSECURITY PLANNING

Module title	Module code
CYBERSECURITY PLANNING	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
-

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module		
After finishing this course, students will be able to understand and apply core principles of cybersecurity planning and management. They will gain the ability to implement international standards and frameworks, develop long-term security strategies, manage operational and tactical cybersecurity measures, and plan for secure network architectures such as cloud and zero trust. Furthermore, students will be equipped to design effective incident response plans and implement business continuity strategies, ensuring organizational resilience and effective cybersecurity measures in the face of evolving threats.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain advance knowledge in how to integrate advanced cybersecurity principles and current trends into strategic planning and operational management	Lectures, Case Studies, Group Discussions, Self-Directed Learning	Self-assessment tests, Knowledge assessment tests
Skills: Learners will be skilled in strategic planning and operational management, enabling them to effectively design and implement cybersecurity strategies that address emerging risks and ensure robust tactical responses	Practical exercises, Workshops, Case studies	Project-based assessments, Practical evaluations
Competences: Learners will be competent in developing and implementing strategic cybersecurity frameworks, leading and managing cybersecurity initiatives	Workshops, Seminars, Role-Playing Exercises	Continuous assessment, Scenario-based testing

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	**All contact work**	**Individual work**	**Tasks**
1. Introduction to Cybersecurity Planning: Data, human and societal security - data security - Information Storage Security, Investigatory process - data security - Password attack techniques -human security -Awareness and Understanding - Societal security – what are Cybercrime, Cyber ethics - Societal security - Cyberlaw- Digital evidence, Digital contracts, Multinational conventions (accords)	8	0,5	6	0,5	**15**	**8**	Define the legal aspects of data, human and societal security, laws and policies that govern data in SME's. Classify types of cyberattacks relevant to SME's Identify useful tools to prevent cyberattacks
2. Strategic Planning -Defining Cybersecurity Goals and Objectives -SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats) -Developing Long-Term Security Strategies -Setting Key Performance Indicators (KPIs) -Reviewing and Updating the Security Strategy	8	2	6	2	**18**	**8**	Define cybersecurity goals relevant to SME's using a SWOT analysis, develop long-term strategies to address risks, allocate resources and budget accordingly, set KPIs to measure progress, and regularly update the strategy based on new threats.
3. Operational and Tactical Management -Implementing Access Controls -Patch Management and Software Up-dates -Continuous System Monitoring - Employee Security Awareness Training	8	1	6	2	**17**	**9**	Implement access control measures to restrict unauthorized access, maintain systems through patch management, set up monitoring for unusual activities and provide employees with cybersecurity awareness training.
Total	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Assessment strategy	Comparative weight percentage	Assessment criteria
Self-assessment test (1)	10%	10 points - 96-100% correct answers.9 points – 91-95 % correct answers. 8 points – 86-90 % correct answers.7 points - 80-85 % correct answers.6 points – 70-79 % correct answers.5 points – 60-69 % correct answers.4 points – 50-59 % correct answers.3 points – 40-49 % correct answers.2 points – 30-39 % correct answers. 1 point – 0-29 % correct answers.
Self-assessment test (2)	10%	
Self-assessment test (3)	10%	
Knowledge evaluation test	70%	

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
1. Nair, A., & Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited. 2. Falco, G. J., & Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press. 3. The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, February 26, 2024
Recommended reading
1. Mehta, S. (2023). *ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide*. Packt Publishing Limited. 2. Gregory, P. H. (2021). *CISM Certified Information Security Manager All-in-One Exam Guide*. McGraw-Hill. 3. ISACA. (2021). *CRISC Review Manual, 7th edition*. ISACA. 4. European Parliament and Council. (2022, December 14). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. 5. Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office

7. M7: RISK MANAGEMENT AND MITIGATION

Module title	Module code
RISK MANAGEMENT AND MITIGATION	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module		
After finishing this course students will be able to continuously manage (identify, analyse, assess, estimate, mitigate) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain advance knowledge of risk management processes, including risk identification, assessment, and control, enabling them to establish and describe effective cybersecurity routines tailored to the specific needs of SME workplaces in compliance with national and international standards	To be selected by the lecturer, from Part 1.3. *[Teaching Methods, e.g. theoretical lectures, literature analysis, guest speakers, peer-to-peer teaching and learning, mentoring etc.]* of D2.3 "*SME Cyber Security Change Agents Learning Pathway's Structure*"	Self-assessment tests Knowledge assessment test
Skills: Learners will be skilled to apply advanced methodologies and tools to conduct comprehensive risk assessments, design and implement effective risk management strategies, and develop robust cybersecurity routines specifically tailored for SME workplaces	To be selected by the lecturer, from Part 1.3. *[Teaching Methods, e.g. practical tasks/labs, quizzes, games, technical video analysis, case studies, hands-on activities etc.]* of D2.3 "*SME Cyber Security Change Agents Learning Pathway's Structure*"	Self-assessment tests Knowledge assessment test
Competences: Learners will be competent in developing and implementing strategic cybersecurity policies for SME workplaces	To be selected by the lecturer, from Part 1.3. *[Teaching Methods, e.g. competitions, CTF, simulated environments, 5Es, CBL, CL, PBL etc.]* of D2.3 "*SME Cyber Security Change Agents Learning Pathway's Structure*"	Self-assessment tests Knowledge assessment test

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	All contact work	Individual work	Tasks
Risk assessment General risk management process General risk management framework Principles of risk management Risk management standards Practical examples	2	0	2	0	**4**	5	Briefly outline the key steps in the risk management process, including risk identification, assessment, and control. Define the internal and external contexts of risk management for an SME. Specify the scope of the risk assessment and identify key risk factors. Develop risk criteria specific to the chosen SME.
Risk identification Leadership and commitment in risk management Defining the scope of risk management activities External and internal context of the risk management context tangible and intangible sources of risk Causes and events Threats and opportunities Vulnerabilities and capabilities Changes in the external and internal context Indicators of emerging risks The nature and value of assets and resources Consequences and their impact on objectives Limitations of knowledge and reliability of information Biases, assumptions and beliefs	4	0	4	0	**8**	5	Identify both tangible and intangible sources of risk for SME. Categorize risks based on causes, events, threats, and opportunities. Analyze the SME's internal vulnerabilities and capabilities, and evaluate how changes in both the external and internal contexts might affect the business. Identify potential emerging risks for the SME and propose indicators to monitor them. Consider how the nature and value of assets and resources impact this analysis

of those involved Practical examples and case studies							
Insider threats Definition and types of an insider threats The costs of insider threats Building an insider threat mitigation program Detecting and identifying insider threats Assessing insider threats Managing insider threats Practical examples and case studies	6	0	6	0	**12**	5	Define and classify different types of insider threats relevant to SMEs. Discuss the potential costs these threats could impose on the business. Develop a basic insider threat mitigation program for an SME. Highlight key components such as detection, identification, and management strategies. Propose a method to assess insider threats, and outline steps to manage these threats effectively in an SME context
Risk measurement and evaluation models and methodologies Quantitative and qualitative risk assessment models and methodologies The likelihood of events and consequences The nature and magnitude of consequences Complexity and connectivity; Time-related factors and volatility Evaluation of the effectiveness of existing controls Sensitivity and confidence levels Practical examples and case studies	6	0	6	0	**12**	5	Compare and contrast one quantitative and one qualitative risk assessment model. Assess the likelihood of a risk event and the nature and magnitude of its consequences for an SME. Consider how complexity, time-related factors, and volatility influence this assessment. Evaluate the effectiveness of current controls in managing identified risks. Include an analysis of sensitivity and confidence levels in the control measures
Risk control Formulating and selecting risk treatment options Planning and implementing risk	6	0	6	0	**12**	5	Identify and select appropriate risk treatment options for SME. Justify your selection based on

treatment Assessing the effectiveness of that treatment Deciding whether the remaining risk is acceptable Monitoring and review recording and reporting Practical examples and case studies							the nature of the risks involved. Develop a brief risk treatment plan, outlining how the selected treatment options will be implemented in an SME environment. Propose a method for assessing the effectiveness of the risk treatment and determining if the remaining risk is acceptable
Total	**24**	**2**	**24**	**0**	**50**	**25**	

Assessment strategy	**Comparative weight percentage**	**Assessment criteria**
Self-assessment test (1)	5%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers. 3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.
Self-assessment test (2)	5%	
Self-assessment test (3)	5%	
Self-assessment test (4)	5%	
Self-assessment test (5)	5%	
Knowledge evaluation test	75%	

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*

Required reading

1. Adarsh Nair and Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management
2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford university press, eBook
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Implementing Enterprise Risk Management: Case Studies and Best Practices. John Wiley & Sons
- ENISA (2022) Risk Management Standards
4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
5. ISO 31000 Risk management — Guidelines

Recommended reading
- Shobhit Mehta (2023) ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management** - Peter H. Gregory (2021) CISM Certified Information Security Manager All-in-One Exam Guide. McGraw-Hill - ISACA (2021) CRISC Review Manual 7th edition. ISACA - Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

8. M8: BUSINESS CONTINUITY, DISASTER RECOVERY, AND INCIDENT MANAGEMENT & PERSONNEL SECURITY

Module title	Module code
BUSINESS CONTINUITY, DISASTER RECOVERY, AND INCIDENT MANAGEMENT & PERSONNEL SECURITY	

Lecturer (s)	Institution or department where module is delivered

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish*

Prerequisites
None

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	75	50	25

Purpose and outcomes of the module		
Upon completion of this course, students will be able to formulate and administer comprehensive business continuity and disaster recovery (BC/DR) plans, develop a functional incident management program, and establish a strong and effective personnel security policy. Students will learn how to safeguard assets, ensure the avoidance of excessive loss experiences, prevent downtime, avoid or limit crisis situations and crises management environments. Upon completion of this course the students will be able to write and monitor the sustained implementation of a thorough cybersecurity handbook for SMEs using advanced cybersecurity principles and technologies integrated in accordance with all national & international statutes. The students will also follow-up enforcement.		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Knowledge: Learners will gain advance knowledge of how to create and implement a comprehensive SME workplace cybersecurity handbook, incorporating advanced cybersecurity principles, the latest defense mechanisms, and adherence to national and international legislation and standards in incident management, business continuity, and personnel security	To be selected by the lecturer, from Part 1.3. [Teaching Methods] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests, Knowledge assessment test

Skills: Learners will be skilled to create and maintain an SME workplace cybersecurity handbook, using advanced methodologies to assess risks, design effective risk management and incident response strategies, and develop comprehensive business continuity plans tailored to their organization's needs.	To be selected by the lecturer, from Part 1.3. [Teaching Methods] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests, Knowledge assessment test
Competences: Learners will be competent in developing and implementing a cybersecurity handbook for SMEs, leading security projects and teams effectively, ensuring alignment with organizational objectives and compliance obligations	To be selected by the lecturer, from Part 1.3. [Teaching Methods] of D2.3 "SME Cyber Security Change Agents Learning Pathway's Structure"	Self-assessment tests, Knowledge assessment test

Module content: breakdown of the topics	**Contact work hours**					**Individual work hours and tasks**	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	**All contact work**	**Individual work**	**Tasks**
Incident response - Definition and importance of incident response in cybersecurity - Key components of an effective incident response recovery - Overview of common cybersecurity threats (phishing, insider threats,) - Developing Incident Response Plan (IRP) - Roles and responsibilities in the Incident Response Team - Simulating the Incident: conducting a mock plan.	5	0,5	3	0,5	**9**	**5**	Develop a detailed Incident Response Plan for your SME, including the roles, responsibilities, and steps to take during a cybersecurity incident. Simulate an incident and conduct a mock drill to test the effectiveness of your plan.
Disaster recovery - Understanding Disaster Recovery - Developing a Disaster Recovery Plan - Roles and responsibilities in Disaster Recovery - Recovery steps after disaster	5	0,5	3	0,5	**9**	**5**	Create a Disaster Recovery Plan that outlines procedures for restoring IT infrastructure and data after a catastrophic event. Include a timeline for recovery and assign responsibilities to team members for each phase of the process.

Business continuity - Understanding business continuity - Developing Business Continuity Plan (BCP) - Roles and responsibilities in business continuity - Business Impact Analysis - Testing and improving BCP	5	0,5	3	0,5	**9**	**5**	Design a Business Continuity Plan that ensures critical business functions remain operational during and after a disruption. Identify essential services and resources and outline contingency strategies to maintain them under various scenarios.
Security awareness, training and education - Understanding security awareness - Developing security training program - Employee responsibilities in cybersecurity - Measuring the effectiveness of security awareness -	1	0,5	2	0,5	**4**	**1**	Develop a security awareness training program for your SME, focusing on key cybersecurity policies and best practices. Conduct a training session for employees and assess their understanding through quizzes or interactive activities.
Security hiring practices - Defining security roles requirements - Conducting throughout background checks - Interviewing for security components - Ongoing evaluation and development	1	0,5	2	0,5	**4**	**1**	Establish security-focused hiring practices, including background checks and interview questions designed to assess candidates' cybersecurity awareness. Create a checklist of essential security qualifications and traits for prospective employees.
Security termination practices - Revoking access immediately - Data and device retrieval - Exit interview for security insights - Notifying relevant teams - Legal and compliance considerations	1	0,5	2	0,5	**4**	**2**	Draft a secure termination procedure that includes steps for revoking access, recovering company assets, and conducting exit interviews. Implement a mock termination scenario to evaluate the effectiveness of your procedure.

Third-party security - Assessing third-party risk - Due diligence in vendor selection - Implementing contrasts and security requirements - Ongoing monitoring and auditing - Incident response and communication	2	0,5	2	0,5	**5**	**2**	Identify potential risks associated with third-party vendors and create a security assessment checklist for evaluating their compliance with your SME's cybersecurity standards. Draft a contract template that includes security requirements and penalties for non-compliance.
Security in review processes - Incorporating security into reviews - Conducting regular security audits - Vulnerability assessment and penetration testing - Post-incident reviews	1	0,5	1,5	0,5	**3,5**	**2**	Develop a process for regularly reviewing and updating your SME's cybersecurity policies and procedures. Schedule and conduct a mock audit to ensure all security measures are up-to-date and compliant with relevant standards.
Special issue in privacy of employee personal information - Data collection limitations - Storage and access control - Compliance with privacy regulations - Data sharing and third parties - Employee consent and rights	2	0,5	2	0,5	**5**	**2**	Draft a privacy policy for handling employee personal information, ensuring compliance with data protection laws and best practices. Conduct a risk assessment to identify potential vulnerabilities in how employee data is stored and processed.
Total	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Assessment strategy	**Comparative weight percentage**	**Assessment criteria**
Self-assessment test (1)	5%	10 points - 95-100% correct answers. 9 points – 85-94 % correct answers. 8 points – 75-84 % correct answers. 7 points - 65-74 % correct answers. 6 points – 55-64 % correct answers. 5 points – 45-54 % correct answers. 4 points – 35-44 % correct answers.
Self-assessment test (2)	5%	
Self-assessment test (3)	5%	
Self-assessment test (4)	5%	
Self-assessment test (5)	5%	
Knowledge evaluation test	75%	

		3 points – 25-34 % correct answers. 2 points – 15-24 % correct answers. 1 points – 0-14 % correct answers.

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, eBook. - Michael Wallace, Lawrence Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*. AMACOM. - National Institute of Standards and Technology (NIST). *Contingency Planning Guide for Information Technology Systems*. NIST SP 800-34 Rev. 1. - Cochran, K.A. (2024). Incident Response, Business Continuity, and Disaster Recovery. In: Cybersecurity Essentials. Apress, Berkeley, CA. **https://doi.org/10.1007/979-8-8688-0432-8_14**
Recommended reading
- ISACA (2023). *CISM Review Manual 15th Edition*. ISACA. - Peter H. Gregory (2021). *CISM Certified Information Security Manager All-in-One Exam Guide*. McGraw-Hill. - IT Governance (2022). *ISO 22301:2019 – Business Continuity Management Systems. Requirements*. - M. Souppaya, L. Feldman, G. Witte [2024], Guide for Cybersecurity Incident Recovery, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology U.S. Department of Commerce - Ihab Hanna Sawalha [2021]. Views on business continuity and disaster recovery. International Journal of Emergency Services

ANNEXES

TEMPLATE FOR SYLLABUS

MODULE DESCRIPTION

Module title	Module code
...	

Lecturer (s)	Institution or department where module is delivered
...	...

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, ...*

Prerequisites
...

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
3	...	...	...

Purpose and outcomes of the module		
...		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**

Facilitate resources (equipment, software, technology)
...

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI)	Consultations	Practice (HEI)	Tests	**All contact work**	**Individual work**	**Tasks**
1							
…							
n							
Total							

Assessment strategy	Comparative weight percentage	Assessment criteria
Self-test I		…
…		…
Self-test n		…
Knowledge evaluation test		…

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
…
Recommended reading
…

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau