

M6 Cybersecurity Planning

Part of the CyberAgent Training Programme, more info at CyberAgent.eu

OBJECTIVES

- Define the legal aspects of cybersecurity that govern data in SME's.
- Define cybersecurity goals relevant to SME's using a SWOT analysis.
- Provide SME employees with cybersecurity awareness training.

CHARACTERISTICS

Languages

Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish.

Duration & Workload

Live Training: 20 hours

Individual study: 60 hours



**FULLY ONLINE
OR BLENDED**



**3 ECTS
CREDITS**

POWERED BY



WHAT YOU WILL LEARN



At the end of this module, learners 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.

TRAINING CONTENT



Introduction to Cybersecurity Planning

1

Defining the legal aspects of data, human and societal security, laws and policies that govern SME's. Classifying types of cyberattacks relevant to SME's. Identifying useful tools to prevent cyberattacks.

Strategic Planning

2

Defining Cybersecurity Goals and Objectives; Preparing SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats); Developing Long-Term Security Strategies ; Setting Key Performance Indicators (KPIs); Reviewing and updating the Security Strategy.

Operational and Tactical Management

3

Implementing Access Controls; Patch Management and Software Updates; Continuous System Monitoring; Employee Security Awareness Training.

Assessment

Self-assessment: 40%

Final knowledge test: 60%