

M7 Risk Management

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

OBJECTIVES

- Identify and assess risks from various sources, threats, and vulnerabilities to gauge impact on objectives.
- Use quantitative and qualitative methods to evaluate risk likelihood and consequences.
- Plan, implement, and review risk treatments, and assess residual risk acceptability.

CHARACTERISTICS

Languages

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

Duration & Workload

Live Training: 50 hours

Individual study: 25 hours



**FULLY ONLINE
OR BLENDED**



**3 ECTS
CREDITS**

POWERED BY



Vilnius
University



OLEMISEN
BALANSIA RI



ISTANBUL CYBER SECURITY CENTER

TEKNOPAK
ISTANBUL



IT
AKADEMIJA



WHAT YOU WILL LEARN



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.

TRAINING CONTENT (1/2)



1

Risk assessment

General risk management process; General risk management framework; Principles of risk management. Risk management standards.

2

Risk identification

Defining risk scope, context, and leadership role; Identifying risk sources, threats, vulnerabilities, and assets; Analyzing emerging risks, contextual changes, and consequences; Evaluating biases and information reliability.

3

Insider Threats

Learning the types and costs of insider threats; Building an insider threat mitigation program; Detecting and identifying insider threats; Assessing insider threats; Managing insider threats.

4

Risk measurement, evaluation models and methodologies

Assessing the likelihood and magnitude of consequences; Analyzing influencing factors like complexity, connectivity, and volatility; Evaluating the effectiveness of existing controls; Determining sensitivity and confidence levels of the analysis.

M7 Risk Management

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

OBJECTIVES

- Identify and assess risks from various sources, threats, and vulnerabilities to gauge impact on objectives.
- Use quantitative and qualitative methods to evaluate risk likelihood and consequences.
- Plan, implement, and review risk treatments, and assess residual risk acceptability.

CHARACTERISTICS

Languages

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

Duration & Workload

Live Training: 50 hours

Individual study: 25 hours



**FULLY ONLINE
OR BLENDED**



**3 ECTS
CREDITS**

TRAINING CONTENT (2/2)



5

Risk control

Formulating and selecting risk treatment options; Planning and implementing risk treatment; Assessing the effectiveness of that treatment; Deciding whether the remaining risk is acceptable; Monitoring and review; Recording and reporting.

Assessment

Self-assessment: 25%

Final knowledge test: 75%

POWERED BY

