

M5 Security Governance & Policy

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

OBJECTIVES

- Apply security governance frameworks aligned with business goals and regulations.
- Create and communicate security policies, including threat and incident management.
- Communicate cybersecurity needs to executives to support decisions, compliance, and ethics.

CHARACTERISTICS

Languages

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

Duration & Workload

Live Training: 75 hours

Individual study: 50 hours



**FULLY ONLINE
OR BLENDED**



**3 ECTS
CREDITS**

POWERED BY



WHAT YOU WILL LEARN



Learners will gain advanced 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.

TRAINING CONTENT (1/2)



Organizational context

1

Understand the evolution, major threats, and unique cybersecurity challenges faced by SMEs, and assess how cybersecurity impacts business strategy and regulatory compliance.

Privacy

2

Gain an understanding of privacy principles, data protection, and tools to ensure GDPR compliance and safeguard SME operations.

Laws, ethics, and compliance

3

Understand cybersecurity organizations, policies, standards, and legal requirements, including AI tools for enhancing governance and ensuring compliance in SMEs.

Security governance

4

Develop the ability to establish cybersecurity governance, define roles, assess maturity, integrate security into corporate strategy, and perform risk assessments and response planning in simulated crises.

Executive and board level communication

5

Acquire skills in cybersecurity communication, security reporting, data-driven decision-making, and crisis management, including handling AI-driven attacks and ransomware.

M5 Security Governance & Policy

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

OBJECTIVES

- Apply security governance frameworks aligned with business goals and regulations.
- Create and communicate security policies, including threat and incident management.
- Communicate cybersecurity needs to executives to support decisions, compliance, and ethics.

CHARACTERISTICS

Languages

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

Duration & Workload

Live Training: 75 hours

Individual study: 50 hours



**FULLY ONLINE
OR BLENDED**



**3 ECTS
CREDITS**

TRAINING CONTENT (2/2)



6

Managerial policy

Develop the ability to create, implement, monitor, and update security policies, emphasizing training and awareness to ensure compliance and mitigate risks.

Assessment

Self-assessment: 60%

Final knowledge test: 60%

POWERED BY

