MERCURY

Cybersecurity and Enterprise Risk Management

13 – 17 September 2027
Amsterdam (Netherlands)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Cybersecurity and Enterprise Risk Management

Ref: 16102_1006356 **Date:** 13 – 17 September 2027 **Location:** Amsterdam (Netherlands) **Fees:** 6200 Euro

Introduction

The Cybersecurity and Enterprise Risk Management training course equips professionals with the knowledge and practical skills required to safeguard enterprise assets against evolving digital threats. It explores the integration of cybersecurity with enterprise risk management ERM strategies to create a resilient organizational environment.

Participants will gain expertise in assessing cyber risks, implementing effective controls, and designing enterprise-wide risk frameworks. The Cybersecurity and Enterprise Risk Management program emphasizes threat prevention, incident response, and business continuity planning to ensure operational stability. Real-world case studies illustrate breaches, their consequences, and the importance of proactive risk management.

Participants will enhance analytical, strategic, and decision-making capabilities to address complex cybersecurity challenges. This Cybersecurity and Enterprise Risk Management course also examines compliance with international standards and legal frameworks. Learners will understand how to align cybersecurity initiatives with corporate objectives and develop a sustainable security culture.

Targeted Groups

This Cybersecurity and Enterprise Risk Management training targets professionals seeking knowledge and skills:

- Cybersecurity officers within enterprises.
- Enterprise risk management specialists.
- IT and network administrators.
- Security analysts and digital strategy experts.
- Digital transformation leaders.
- Risk and compliance consultants.
- System and infrastructure project managers.
- Data protection and privacy officers.
- Aspiring information security professionals.
- Professionals in the finance, energy, and healthcare sectors.

Training Course Objectives

Participants will achieve the following objectives by completing the Cybersecurity and Enterprise Risk Management course:

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Analyze cyber threats and assess their potential impact on enterprise operations.
- Identify vulnerabilities in digital systems and propose mitigation strategies.
- Design actionable cybersecurity strategies aligned with organizational goals.
- Implement robust information security controls in line with global standards.
- Evaluate operational, financial, and reputational consequences of cyber risks.
- Develop and execute incident response plans to manage digital crises.
- Enhance business continuity planning for critical enterprise functions.
- Integrate cybersecurity practices into corporate culture and strategic initiatives.
- Make informed decisions in high-risk, fast-changing cyber environments.
- Ensure compliance with national and international regulations.
- Monitor security systems continuously to detect emerging threats.
- Apply best practices in governance, risk, and compliance GRC management.
- Raise organizational awareness of cybersecurity and enterprise risk management.
- Implement proactive defense mechanisms to reduce the likelihood of breaches.
- Utilize cyber risk management frameworks to strengthen enterprise resilience.

Targeted Competencies

Participants will gain the following competencies during the Cybersecurity and Enterprise Risk Management program:

- Conduct advanced cybersecurity risk assessment and analysis.
- Develop and maintain enterprise security risk management strategies.
- Integrate cybersecurity governance and risk management into business operations.
- Execute cyber incident response and digital crisis handling effectively.
- Apply enterprise risk and cybersecurity strategy to decision-making.
- Assess compliance and regulatory requirements in information security.
- Design, monitor, and improve cyber security risk management systems.
- Evaluate the impact of cyber risk on organizational performance.
- Embed integrated risk management cybersecurity practices across departments.
- Utilize business continuity and disaster recovery techniques in cyber environments.
- Enhance strategic thinking for cyber risk and compliance initiatives.

Studying Scenarios

In this Cybersecurity and Enterprise Risk Management training, participants develop skills through the following scenarios:

- Assessing a simulated enterprise environment for cyber vulnerabilities.
- Responding to a multi-layered ransomware attack with defined protocols.
- Evaluating risk exposure in IT infrastructure and recommending mitigation plans.
- Conducting cyber risk management exercises aligned with organizational strategy.
- Reviewing case studies of international security breaches and compliance lapses.
- Simulating incident response coordination between IT and executive teams.
- Applying integrated risk management cybersecurity frameworks to enterprise scenarios.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Course Content

Unit 1: Fundamentals of Cybersecurity

- Overview of cybersecurity in modern business operations.
- Core concepts of information security and digital asset classification.
- Differentiating cyber threats, attacks, and breaches.
- Categories of cyberattacks and methods of execution.
- Authentication, encryption, and integrity principles.
- Network security protocols and layered defense strategies.
- Understanding malware, phishing, ransomware, and advanced persistent threats.
- Evaluating operational and financial consequences of cyber incidents.
- Reviewing case studies of high-profile security breaches and lessons learned.
- Introduction to cybersecurity risk management for organizations and enterprises.

Unit 2: Introduction to Enterprise Risk Management

- Definition and classification of enterprise risks.
- Integration of cybersecurity and enterprise risk management frameworks.
- Risk evaluation, prioritization, and likelihood-impact analysis.
- Tools and frameworks for risk analysis: ISO 31000, SWOT, and COSO ERM.
- Developing effective risk response strategies.
- Embedding ERM practices into daily business operations.
- Governance structures supporting enterprise cyber risk management.
- Monitoring and updating risk registers for emerging threats.
- Conducting risk workshops and stakeholder engagement sessions.
- Linking cyber risk and compliance requirements to organizational objectives.

Unit 3: Compliance and Global Standards

- Role of compliance in cybersecurity and ERM.
- Overview of ISO/IEC 27001, NIST, and other cybersecurity standards.
- GDPR and global data protection frameworks.
- Organizational readiness and maturity assessment for compliance.
- Internal audit and verification of cybersecurity policies.
- Establishing governance structures for security oversight.
- Designing cybersecurity risk frameworks for enterprise applications.
- Performing gap analyses and remediation planning.
- Aligning enterprise risk and cybersecurity strategy with regulatory expectations.
- Integrating advanced cybersecurity risk management practices into policy management.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 4: Incident Response and Emergency Management

- Classifying cyber incidents and understanding threat vectors.
- Incident response methodologies and frameworks.
- Formation and management of CSIRTs Computer Security Incident Response Teams.
- Digital forensics and evidence collection processes.
- Crisis communication with internal and external stakeholders.
- Threat detection and rapid response tools.
- System recovery and restoration techniques.
- Post-incident reviews and process improvements.
- Integrating cybersecurity risk management for business leaders in incident planning.
- Implementing continuous improvement in cyber risk and compliance processes.

Unit 5: Business Continuity and Disaster Recovery

- Concepts of business continuity in the context of cyber threats.
- Business Impact Analysis BIA methodology and principles.
- Identifying and protecting critical enterprise functions.
- Designing and implementing Disaster Recovery Plans DRP.
- Testing, evaluating, and optimizing continuity plans.
- Cloud computing strategies for enhanced disaster recovery.
- Coordination between IT teams, leadership, and stakeholders.
- Revisiting policies, risk levels, and security postures after incidents.
- Embedding enterprise security risk management into continuity planning.
- Leveraging cybersecurity risk assessment results for future resilience.

Unit 6: Building a Cybersecurity Culture

- Leadership roles in promoting cybersecurity awareness.
- Implementing effective awareness and training programs.
- Encouraging secure digital behavior across organizational levels.
- KPIs for measuring cybersecurity culture effectiveness.
- Assessing training outcomes and awareness metrics.
- Aligning security initiatives with strategic corporate objectives.
- Using AI and automation to enhance security awareness initiatives.
- Incorporating cybersecurity considerations into HR processes and evaluations.
- Developing internal and external strategic partnerships for security.
- Creating sustainable enterprise cyber risk management practices.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Final Insights & Key Takeaways

This Cybersecurity and Enterprise Risk Management course equips participants with actionable strategies to protect organizational assets. Learners will understand how to integrate cybersecurity governance and risk management into enterprise operations. The program enhances skills in cyber risk assessment, incident response, and business continuity planning. Participants leave prepared to build resilient, secure, and compliant enterprise systems.