MERCURY

Cybersecurity Risk Management and Compliance

29 August – 2 September 2027
Kuala Lumpur (Malaysia)



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

MERCURY

Cybersecurity Risk Management and Compliance

Ref: 121334_1028230 **Date:** 29 August – 2 September 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 Euro

Introduction

Cybersecurity Risk Management and Compliance equip professionals with the knowledge and skills to identify, assess, and mitigate cybersecurity risks. The course emphasizes regulatory compliance, industry standards, and effective risk governance. Participants will learn to develop strategies to protect organizational assets and sensitive data. The program integrates risk assessment frameworks, compliance protocols, and incident response planning. It emphasizes practical applications in real-world scenarios. Participants will confidently lead cybersecurity initiatives.

Targeted Groups

This Cybersecurity Risk Management and Compliance targets professionals seeking specialized knowledge and skills:

- IT managers and cybersecurity leaders.
- Risk management professionals.
- Compliance officers.
- Security analysts and auditors.
- Network administrators.
- Professionals in finance, healthcare, and critical infrastructure sectors.
- Consultants supporting organizational security strategies.

Course Objectives

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

- Identify and assess cybersecurity risks.
- Understand global and local regulatory requirements.
- Implement risk management frameworks.
- Develop incident response plans.
- Ensure compliance with standards such as ISO 27001 and NIST.
- Protect sensitive organizational data.
- Enhance organizational security posture.
- Apply best practices in risk mitigation.
- Integrate cybersecurity strategies into business processes.
- Evaluate and improve existing security measures.

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

Targeted Competencies

Participants will gain the following competencies during the program:

- Risk identification and prioritization.
- Regulatory compliance knowledge.
- Threat detection and mitigation.
- Incident response planning.
- Security policy development.
- Data protection and privacy management.
- Audit and monitoring techniques.
- Vendor and third-party risk management.
- Cybersecurity governance and reporting.
- Continuous improvement of security frameworks.

Studying Scenarios

In this training, participants will develop their skills through the analysis of the following scenarios:

- Responding to a ransomware attack in a financial institution.
- Evaluating compliance gaps in healthcare data systems.
- Implementing ISO 27001 risk controls in a corporate network.
- Conducting risk assessments for cloud-based infrastructure.
- Developing an incident response strategy for a multinational company.
- Managing third-party vendor cybersecurity risks.
- Handling data breaches under regulatory scrutiny.

Course Content

Unit 1: Introduction to Cybersecurity Risk Management

- Definition and scope of cybersecurity risk management.
- Overview of cyber threats and vulnerabilities.
- Importance of cybersecurity in organizational resilience.
- Key regulatory requirements and standards.
- Roles and responsibilities in risk management.
- Risk assessment frameworks and methodologies.
- Understanding threat landscapes and emerging risks.

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

Unit 2: Risk Assessment and Mitigation

- Identifying organizational assets and critical systems.
- Risk identification and classification techniques.
- Performing qualitative and quantitative risk assessments.
- Vulnerability analysis and prioritization.
- Developing mitigation strategies.
- Implementing controls and safeguards.
- Monitoring and reviewing risk management processes.

Unit 3: Compliance and Regulatory Standards

- Overview of ISO 27001, NIST, and GDPR.
- Legal and regulatory obligations in cybersecurity.
- Compliance audits and reporting.
- Policy and procedure development.
- Integrating compliance into business operations.
- Documentation and evidence collection.
- Evaluating compliance effectiveness.

Unit 4: Incident Response and Management

- Designing an incident response plan.
- Identifying and classifying incidents.
- Containment and eradication strategies.
- Communication protocols during incidents.
- Post-incident analysis and reporting.
- Lessons learned and preventive measures.
- Collaboration with internal and external stakeholders.

Unit 5: Advanced Risk Strategies and Emerging Trends

- Managing third-party and supply chain risks.
- Cybersecurity governance and leadership.
- Risk management for cloud and hybrid environments.
- Threat intelligence and proactive monitoring.
- Emerging technologies and their security implications.
- Continuous improvement of security frameworks.
- Strategic decision-making for organizational resilience.

Final Insights & Key Takeaways

Participants will leave with practical skills to manage cybersecurity risks and ensure compliance. The course empowers professionals to strengthen security strategies and safeguard organizational assets.