MERCURY

# Cyber Security Risk Management Course

3 – 7 January 2027
Cairo (Egypt)



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

# Cyber Security Risk Management Course

**Ref:** 15246_266935 **Date:** 3 – 7 January 2027 **Location:** Cairo (Egypt) **Fees:** 4000 Euro

## Introduction:

In today's rapidly evolving digital landscape, cyber threats have become increasingly sophisticated and pervasive, affecting organizations of all sizes and industries. The importance of protecting sensitive information, ensuring business continuity, and maintaining customer trust has led to the rise of Cyber Security Risk Management as an essential discipline.

The course Cyber Security Risk Management offers a comprehensive exploration of strategies and practices for safeguarding digital assets and mitigating cyber risks. Participants will delve into the dynamic world of cyber threats, learning how to proactively identify vulnerabilities, assess potential risks, and implement robust security measures.

In a world where cyberattacks can result in significant financial losses, reputation has never been more critical. This Cyber Security Risk Management course empowers participants with the knowledge and skills to navigate the complex landscape of cyber threats, enabling them to make informed decisions to protect their organization's digital environments.

This course addresses topics ranging from threat detection and risk assessment to incident response and compliance with industry standards, equipping participants with actionable insights to enhance their organization's cyber resilience. Whether you're an IT professional, manager, executive, or anyone concerned about the security of digital assets, this course provides a valuable platform for developing expertise in managing cyber risks effectively.

## Targeted Audience:

- IT Managers and Professionals.
- Cyber Security Analysts.
- Risk Management Professionals.
- Chief Information Security Officers CISOs.
- Compliance Officers.
- Business Executives and Managers.
- Information Security Officers.
- Network Administrators.
- Anyone responsible for protecting sensitive digital assets.

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

## Targeted Competencies:

At the end of this Cyber Security Risk Management training, participants competencies will:

- Understand the cyber threat landscape and the evolving nature of cyber risks.
- Identify vulnerabilities in digital systems and networks.
- Conduct thorough risk assessments and prioritize risks.
- Develop and implement effective cyber security strategies.
- Apply encryption, authentication, and access controls to protect data.
- Implement incident response plans to mitigate the impact of cyber incidents.
- Ensure compliance with industry regulations and standards.
- Educate employees and stakeholders about cyber security best practices.
- Collaborate with cross-functional teams to address cyber security challenges.
- Monitor and detect cyber threats in real-time.

## Course Objectives:

By the end of this Cyber Security Risk Management course, participants will be able to:

- Understand the fundamentals of cyber security risk management.
- Identify and assess potential cyber security vulnerabilities and threats.
- Develop and implement effective cyber security strategies and policies.
- Execute risk assessment techniques to prioritize cyber threats.
- Implement encryption, authentication, and access control measures.
- Plan and execute incident response procedures to minimize cyber risks.
- Ensure compliance with relevant industry regulations and standards.
- Educate employees about cyber security best practices.
- Collaborate with various stakeholders to manage cyber risks.
- Monitor and respond to real-time cyber threats effectively.

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

MERCURY

## Understanding the Cyber Security Risk Management Approach:

Within the sweeping domain of Cyber Security Risk Management, participants will be equipped with a structured approach to protecting their organizations' digital infrastructure. Embracing a risk management plan is crucial to identifying the most alarming cyber threats and devising a meticulously crafted response strategy.

This Cyber Security Risk Management course will lead professionals through the labyrinth of cyber security risk management tools and practices, honing their ability to shield their enterprises against the ever-changing digital age threats. The Cyber Security Risk Management process is central to an organization's strategic defense mechanisms.

This course will illustrate constructing a fortified cyber security risk management framework, ensuring a resilient posture against potential attacks. Attendees will receive rigorous cyber security risk management training, sharpening their capacity to bolster the importance of risk management in cyber security within their respective organizations.

## Course Content:

### Unit 1: Introduction to Cyber Security Risk Management:

- Understanding Cyber Security and Its Importance.
- Evolution of Cyber Threats and Attack Vectors.
- Cyber Security Risk Management Frameworks.

### Unit 2: Identifying and Assessing Cyber Risks:

- Types of Cyber Security Threats.
- Vulnerability Assessment and Penetration Testing.
- Risk Assessment Methodologies.

### Unit 3: Developing Effective Cyber Security Strategies:

- Security Policies and Procedures.
- Security by Design Principles.
- Security Awareness Training.

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

## Unit 4: Implementing Cyber Security Controls:

- Encryption and Data Protection.
- Authentication and Access Controls.
- Network Security Measures.

## Unit 5: Incident Response and Recovery:

- Incident Response Planning and Execution.
- Business Continuity Planning.
- Legal and Regulatory Considerations.

## Unit 6: Compliance and Standards:

- Industry Regulations GDPR, HIPAA, etc..
- International Security Standards ISO 27001.
- NIST Cybersecurity Framework.

## Unit 7: Collaborating and Communicating About Cyber Risks:

- Cross-Functional Collaboration.
- Communication Strategies for Cyber Security.

## Unit 8: Monitoring and Emerging Threats:

- Real-Time Threat Monitoring.
- Threat Intelligence and Analysis.
- Adapting to New Cyber Threats.

## Unit 9: Building a Culture of Cyber Security:

- Employee Training and Awareness.
- Creating a Security-Conscious Workforce.
- Embedding Security in Organizational Culture.

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

## Unit 10: Future Trends in Cyber Security Risk Management:

- Emerging Technologies and Their Security Implications.
- Predictive Analytics and Cyber Threat Prevention.
- Ethical Considerations in Cyber Security.