MERCURY

Cyber Security Risk Management

09 - 13 Jun 2024
Cairo (Egypt)

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

Cyber Security Risk Management

Ref.: 15246_245900 **Date:** 09 - 13 Jun 2024 **Location:** Cairo (Egypt) **Fees:** 3500 **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 vital 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 aimed at safeguarding digital assets and mitigating cyber risks. In this course, 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, reputational damage, and legal consequences, understanding cyber risk management has never been more critical. This course empowers participants with the knowledge and skills needed to navigate the complex landscape of cyber threats, enabling them to make informed decisions to protect their organizations' digital environments.

By addressing topics ranging from threat detection and risk assessment to incident response and compliance with industry standards, this course equips participants with actionable insights to enhance their organizations' 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 to develop 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

Targeted Competencies:

- Understanding the cyber threat landscape and the evolving nature of cyber risks.
- Identifying vulnerabilities in digital systems and networks.
- Conducting thorough risk assessments and prioritizing risks.
- Developing and implementing effective cyber security strategies.
- Applying encryption, authentication, and access controls to protect data.
- Implementing incident response plans to mitigate the impact of cyber incidents.
- Ensuring compliance with industry regulations and standards.
- Educating employees and stakeholders about cyber security best practices.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

- Collaborating with cross-functional teams to address cyber security challenges.
- Monitoring and detecting cyber threats in real-time.

Course Objectives:

By the end of this 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.

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

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

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

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

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

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Registration form on the :
Cyber Security Risk Management

code: 15246 **From:** 09 - 13 Jun 2024 **Venue:** Cairo (Egypt) **Fees:** 3500 **Euro**

Complete & Mail or fax to Mercury Training Center at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng):
.....
Position:
.....
Telephone / Mobile:
.....
Personal E-Mail:
.....
Official E-Mail:
.....

Company Information

Company Name:
.....
Address:
.....
City / Country:
.....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng):
.....
Position:
.....
Telephone / Mobile:
.....
Personal E-Mail:
.....
Official E-Mail:
.....

Payment Method

☐ Please invoice me

☐ Please invoice my company