€TRAINING

Risk Management in Information Security

8 - 19 December 2024
Istanbul (Turkey)

Risk Management in Information Security

REF: B2308 DATE: 8 - 19 December 2024 Venue: Istanbul (Turkey) - Fee: 8775 Euro

Introduction:

The Risk Management in Information Security course is designed to equip participants with the knowledge and skills necessary to identify, assess, and mitigate risks in information security environments. In today's rapidly evolving threat landscape, understanding risk management is crucial for organizations to safeguard their sensitive data and critical systems effectively.

Course Objectives:

Upon completing this course, participants will be able to:

- Understand the fundamental concepts of risk management in the context of information security.
- Identify potential threats and vulnerabilities in information systems.
- Apply risk assessment methodologies to prioritize security measures.
- Implement risk mitigation strategies and controls.
- Develop a risk management framework tailored to the organization's specific needs

Target Audience:

This course is ideal for:

- Information Security Professionals seeking to enhance their risk management skills.
- IT Managers and Decision-Makers responsible for overseeing information security strategies.
- System Administrators interested in understanding and addressing security risks.
- Compliance Officers aiming to ensure regulatory requirements are met.
- Anyone interested in pursuing a career in information security and risk management.

Course Outline:

Unit 1: Introduction to Risk Management

- Defining risk management and its significance in information security
- Understanding the components of risk management: Identification, Assessment, Mitigation, Monitoring
- Exploring the risk management lifecycle

Unit 2: Threats and Vulnerabilities

Identifying common information security threats:

- Malware and Ransomware
- Phishing and Social Engineering Attacks
- Insider Threats
- Denial of Service DoS Attacks
- Advanced Persistent Threats APTs

Recognizing vulnerabilities in information systems:

- Software Vulnerabilities
- Misconfigurations
- Weak Authentication Mechanisms
- Physical Security Weaknesses

Unit 3: Risk Assessment Methodologies

Overview of qualitative and quantitative risk assessment approaches

Conducting a risk assessment in an organization:

- Risk Identification
- Risk Analysis
- Risk Evaluation

Unit 4: Risk Identification and Categorization

Techniques for identifying and categorizing risks:

- Brainstorming Sessions
- SWOT Analysis Strengths, Weaknesses, Opportunities, Threats
- Asset Valuation and Prioritization

Creating a risk register:

- Documenting Identified Risks
- Assigning Ownership and Accountability

Unit 5: Risk Analysis and Prioritization

Analyzing the impact and likelihood of identified risks:

- Qualitative Risk Analysis
- Quantitative Risk Analysis

Prioritizing risks based on severity and criticality:

- Risk Scoring and Ranking

Unit 6: Risk Mitigation Strategies

Understanding risk response options:

- Risk Avoidance
- Risk Transfer
- Risk Mitigation
- Risk Acceptance

Implementing security controls to mitigate risks:

- Access Controls

- Encryption
- Security Awareness Training
- Business Continuity Planning

Unit 7: Developing Risk Management Plans

Building a risk management framework tailored to the organization:

- Establishing Risk Management Policies
- Defining Roles and Responsibilities

Integrating risk management into existing security policies:

- Aligning with Information Security Standards ISO 27001, NIST, etc.

Unit 8: Risk Communication and Reporting

Communicating risks effectively to stakeholders:

- Developing Risk Communication Strategies
- Presenting Risk Information to Non-Technical Audiences

Preparing risk reports for management and decision-makers:

- Executive Summary of Risks
- Risk Assessment Findings and Recommendations

Unit 9: Monitoring and Reviewing Risks

Establishing a risk monitoring and review process:

- Continuous Monitoring Techniques
- Key Risk Indicators KRIs

Updating risk management strategies as needed:

- Responding to Emerging Threats and Incidents

Unit 10: Case Studies and Practical Exercises

Analyzing real-world scenarios to apply risk management concepts:

- Incident Response Scenarios
- Business Impact Analysis

Hands-on exercises to reinforce learning and skills:

- Conducting a Risk Assessment for a Simulated Environment
- Developing a Risk Management Plan for a Fictitious Organization