BLACKBIRD FOR TRAINING

Cyber Security Risk Assessment and Management

17 – 21 May 2027
Vienna (Austria)



Cyber Security Risk Assessment and Management

Ref: 3255588_205760 **Date:** 17 – 21 May 2027 **Location:** Vienna (Austria) **Fees:** 5900 GBP

Introduction

This Cyber Security Risk Assessment and Management course is designed to teach you how to conduct a comprehensive security risk assessment to protect your organization. You will gain knowledge of the laws and regulations that impose strict cybersecurity requirements on organizations and acquire the skills to develop a compliance assessment plan while employing a standards-based risk management process to maintain a strong security posture. This course assumes a basic understanding of business processes and technology concepts, but no specialized technical knowledge is required.

Course Objectives

By the end of this course, participants will be able to:

- Implement standards-based, proven methodologies for assessing and managing risks to their organization's information infrastructure.
- Select and implement security controls that ensure compliance with applicable laws, regulations, policies, and directives.
- Extend security protection to Industrial Control Systems ICS and cloud environments.
- Understand the importance of cybersecurity risk management and how to implement it effectively in an organizational context.
- Differentiate between risk management and risk assessment in the realm of cybersecurity.

Course Outlines

Day 1: Introduction to Risk Assessment and Management

- Ensuring compliance with applicable regulatory drivers.
- Protecting the organization from unacceptable losses.
- Understanding the Risk Management Framework RMF.
- Applying NIST and ISO risk management processes.
- Characterizing System Security Requirements:
    - Defining the system.
    - Outlining system security boundaries.
    - Pinpointing system interconnections.
    - Incorporating unique characteristics of Industrial Control Systems ICS and cloud-based systems.



Day 2: Selecting Appropriate Security Controls

- Investigating security control families.
- Determining the baseline from system security risk.
- Tailoring the baseline to fit the system.
- Examining the structure of security controls, enhancements, and parameters.
- Binding control overlays to the selected baseline.
- Gauging the need for enhanced assurance.

Day 3: Reducing Risk Through Effective Control Implementation

- Maximizing security effectiveness by “building in” security.
- Reducing residual risk in legacy systems via “bolt-on” security elements.
- Developing an assessment plan:
    - Prioritizing depth of control assessment.
    - Optimizing validation through sequencing and consolidation.
    - Verifying compliance through tests, interviews, and examinations.
- Formulating an authorization recommendation.

Day 4: Authorizing System Operation

- Aligning authority and responsibility within the organization.
- Quantifying organizational risk tolerance.
- Elevating authorization decisions in high-risk scenarios.
- Weighing residual risk against operational utility.
- Issuing Authority to Operate ATO.

Day 5: Maintaining Continued Compliance

- Measuring the impact of changes on the system security posture.
- Executing effective configuration management.
- Performing periodic control reassessment.
- Preserving an acceptable security posture:
    - Delivering initial and routine follow-up security awareness training.
    - Collecting ongoing security metrics.
    - Implementing vulnerability management, incident response, and business continuity processes.



Why Attend This Course: Wins & Losses!

- Practical training in Cybersecurity Risk Assessment and Management, using proven methodologies and tools.
- A deep understanding of risk management in cybersecurity, ensuring you're prepared to handle potential security threats.
- Knowledge of how to conduct a thorough cybersecurity risk assessment and ensure the security of your organization's information infrastructure.
- The ability to implement security controls in line with relevant laws and regulations to ensure compliance.
- Insight into ICS and cloud-based security concerns, an essential skill in today's interconnected world.

Conclusion

This course provides an essential foundation in cybersecurity risk assessment and management, enabling you to enhance the security of your organization’s systems and data. By understanding and implementing risk management techniques, you will be well-equipped to protect against the increasing number of cyber threats.

Enroll in this Cybersecurity Risk Assessment and Management course today, and ensure your organization remains secure and compliant in an ever-evolving cyber landscape.

