Cyber Security Risk Assessment Training

Course: **00070**
Filter: **Beginner**
Duration: **4 days**
Category:: **Cyber Security**
Price: **3000,00 €**

About Course

This risk assessment training course will teach you how to conduct a security risk assessment to protect your organization. You will learn about the laws and regulations that impose strict cybersecurity requirements on all organizations. You will also gain the skills to develop a compliance assessment plan and employ a standards-based risk management process while maintaining a satisfactory security posture.

What you'll learn

- Implement standards-based, proven methodologies for assessing and managing your organization's information infrastructure risks.
- Select and implement security controls that ensure compliance with applicable laws, regulations, policies, and directives.
- Extend security protection to ICS (Industrial Control Systems) and the cloud.

Pre-requisites

- Attendees should have a basic knowledge of business processes and technology concepts. No specialized technical knowledge is assumed.

Curriculum

Module 1: Introduction to Risk Assessment and Management

- Ensuring compliance with applicable regulatory drivers
- Protecting the organization from unacceptable losses
- Describing the RMF (Risk Management Framework
- Applying NIST/ISO risk management processes

Module 2: Characterizing System Security Requirements

- Defining the system
- Outlining the system security boundary
- Pinpointing system interconnections
- Incorporating the unique characteristics of Industrial Control Systems and cloud-based systems
- Identifying security risk components
- Estimating the impact of compromises on confidentiality, integrity, and availability
- Adopting the appropriate model for categorizing system risk
- Setting the stage for successful risk management
- Documenting critical risk assessment and management decisions in the SSP (System Security Plan)
- Appointing qualified individuals to risk governance roles

Module 3: Selecting Appropriate Security Controls

- Assigning a security control baseline
- 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
- Distinguishing system-specific, compensating, and non-applicable controls

Module 4: Reducing Risk Through Effective Control Implementation

- Specifying the implementation approach
- Maximizing security effectiveness by "building in" security
- Reducing residual risk in legacy systems via "bolt-on" security elements

- Applying NIST/ISO controls
- Enhancing system robustness through the selection of evaluated and validated components
- Coordinating implementation approaches to administrative, operational, and technical controls
- Providing evidence of compliance through supporting artifacts

Module 5: Assessing Compliance Scope and Depth

- 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
- Evaluating overall system security risk
- Mitigating residual risks
- Publishing the POA&M (Plan of Action and Milestones), the risk assessment, and recommendation

Module 6: Authorizing System Operation

- Aligning authority and responsibility
- Quantifying organizational risk tolerance
- Elevating authorization decisions in high-risk scenarios
- Forming a risk-based decision
- Appraising system operational impact
- Weighing residual risk against operational utility
- Issuing ATO (Authority to Operate)

Module 7: Maintaining Continued Compliance

- Justifying continuous reauthorization
- Measuring the impact of changes on 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