NIST Training Assess & Manage Risk

Course: **00101**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Gouvernance, Risk and Compliance**
Price: **2000,00 €**

About Course

This NIST (National Institute of Standards and Technology) Cybersecurity Framework training course will teach US (United States) Government cybersecurity staff to protect their organization from unacceptable losses by effectively assessing and managing risk. Through NIST training, they will learn how to employ the NIST Cybersecurity Framework defined by The NIST and ensure their organization meets the cyber security laws and regulations imposed on all US Government agencies. • Attendees receive a complete set of course notes and a workbook containing all the course workshops • Every source document used in developing the course may be downloaded from the NIST Website free of charge

What you'll learn

- Implement the NIST Risk Management Framework for assessing and managing your organization's information infrastructure risks.
- Select and implement security controls that satisfy FISMA, OMB (Office of Management and Budget), and Department/Agency requirements.
- Maintain an acceptable security posture over the system life cycle.
- Apply FedRAMP-compliant cloud-based solutions.

Pre-requisites

None

Curriculum

Module 1: Introduction to Risk Assessment and Management

- Ensuring compliance with applicable laws, regulations, policies, and directives
- Protecting the organization from unacceptable losses
- Describing the NIST RMF (Risk Management Framework)
- Applying NIST risk management processes

Module 2: Characterizing System Security Requirements

- Defining the system
- Prescribing the system security boundary
- Pinpointing system interconnections
- Incorporating characteristics of ICS (Industrial Control Systems) and FedRAMP-compliant cloud-based systems
- Identifying security risk components
- Estimating the impact of compromises to confidentiality, integrity, and availability
- Adopting the appropriate model for categorizing system risk
- Specialized considerations for U.S. Government classified information
- 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 impact
- Determining the baseline from system security impact
- 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 controls
- Enhancing system robustness through selection of evaluated and validated components
- Coordinating implementation approaches to administrative, operational, and technical controls
- Providing evidence of compliance through supporting artifacts
- Implementing CNSSI-1253 for national security systems

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
- Preserving an acceptable security posture