

Information Systems Certification and Accreditation Professional

KEY DATA

Course Name: Information Systems Certification & Accreditation Professional

Duration: 5 days

Language: English

Format:

Instructor-led
Live Virtual Training

Prerequisites:

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

Student Materials:

- Student Workbook
- Student Reference Manual

COURSE OVERVIEW

Mile2's Certification, Review and Accreditation Process training quantifies the process of certifying, reviewing and accrediting an information system by IT professionals. This certification is designed to provide, through its contents and referenced resources, a complete guide to establishing a certifiable and accredited information system in any organization.

This course was created as a standard to measure the set of skills that specific members of an organization is required to have for the practice of certifying, reviewing and accrediting the security of information systems. Specifically, this training was designed for the individuals who are responsible for creating and implementing the processes used to evaluate risk and institute security baselines and requirements. These critical decisions will be essential in making sure that the security of the information systems outweighs the potential risks to an organization from any internal or external threats.

Also available as:

LIVE VIRTUAL TRAINING

Attend live class from anywhere in the world!

- Live Presentations with Powerful functionality that delivers easy viewing of slides and other documents, shared Internet access, virtual whiteboard, and a media center all through an easy-to-use toolbar.
- Application, file, and desktop sharing enable you to view live demonstrations.
- Dedicated high spec remote PC per student with full access as if you are sitting in-front of the PC in the classroom.
- Instructor views each students session when you perform your hands on labs, the instructor can access your remote system to demonstrate and assist while you sit back to absorb the classroom style mentoring you expect.
- Public and private text chat allows for increased interactivity between students and instructor

UPON COMPLETION

Upon completion, Certification Review and Accreditation Process students will be able to establish a certifiable and accredited information system in any organization. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security environment.

COURSE DETAILS

- I. Introduction
- II. Phase I – Initiation
 - a. Prepare Documentation
 - b. Notify Officials and Identify Resources
 - c. Analyze, Update and Accept System Security Plan
- III. Phase II – Certification
 - a. Assess and Evaluate Security Controls
 - b. Document Security Certification
- IV. Phase III- Accreditation
 - a. Make Security Accreditation Decision
 - b. Document Security Accreditation
- V. Phase IV – Monitoring
 - a. Manage and Control Configuration
 - b. Monitor Security Controls
 - c. Report & Document Status

Who Should Attend?

- Information System Owners
- Information System Security Officers
- Certifiers
- System Managers
- U.S. State and Local Governments

DETAILED MODULE DESCRIPTION

Initiation of the System Authorization Process

Domain Objectives
 The pillars of C&A
 Domain Agenda
 Initiation Phase Tasks
 Information System Description
 Security Categorization
 Mission Based Information
 BRM - Business Reference Model 2.0
 FIPS 199 & the BRM
 NIST SP 800-60 A
 NIST SP 800-60
 NIST SP 800-60
 Privacy Information
 HIPAA (NIST SP 800-66)
 Trade Secrets
 Mission-Based Information
 FIPS 199
 Preparation – Threat Identification
 Accreditation Boundaries
 Identify Legal and Regulatory Requirements
 Preparation – Vulnerability
 Domain Agenda
 Preparation Phase – Security Control Identification
 Security Controls
 Selection Process
 Common Controls
 Specific Controls
 FIPS 200
 Special Publication 800-53
 Security Control Selection and Refinement
 Tailoring the Baseline
 Security Control Documentation
 Preparation Phase – Initial Risk Determination
 Domain Agenda
 Notification and Resource Identification - Notification
 Notification and Resource Identification - Planning
 Domain Agenda
 SSP – Security Categorization Review
 SSP- System Security Plan Analysis
 SSP -Update
 SSP Acceptance
 Summary of Initiation Phase Requirements
 System Security Plan Documentation

Domain Summary

Certification Phase

Objectives
 Information Security TRIAD
 Security Control Assessment
 Security Certification Phase
 Security Control Assessment- Documentation Phase
 Security Assessment Report (SARs)
 Plan of Action and Milestones
 Security Control Assessment- Methods
 Security Test and Evaluation
 Objectives of the Security Test and Evaluation
 Areas to consider in your plan
 Types of Tests – Strengths & Weaknesses
 The Cost Factor
 Security Control Assessment
 Testing Firewalls
 Testing Firewall Policies
 Document Results
 Details of the Security Assessment Report
 Certification – Findings and Recommendations
 System Security Plan Update
 Plan of Action and Milestones
 Accreditation Package Assembly
 Security Certification Phase Provides Answers
 Summary

Accreditation Phase

Domain Objectives
 The pillars of C&A
 Security Accreditation Phase
 Purpose of Accreditation Phase
 Basis for Security Accreditation Decision
 Final Risk Determination
 Risk Acceptability
 ATO (Authorization to Operate)
 Denial of Authorization to Operate
 Accreditation Decision
 Accreditation Documentation
 Security Accreditation Package Transmission

Continuous Monitoring Phase

Overview

Objectives

Objectives

Information Security TRIAD

TRIAD in Detail

Agenda

Continuous Monitoring

Continuous Monitoring Phase Tasks

Key Roles of Continuous Monitoring

Config Management/Config Control

Documentation of Information System Changes

Security Impact Analysis

Security Control Monitoring Objectives

Selected Security Control Assessment

Status Reporting and Documentation

System Security Plan Update

Plan of Action Updates

Continuous Monitoring Continues until the following have been answered

Domain Summary

