ISCAP: Information Security Accreditation & Certification Professional

Course ID #: 7000-816-ZZ-Z
Hours: 21

Course Content

Course Description:

In this course, you will cover the process of certifying, reviewing and accrediting an information system(IS). What does it take to have a certified and accredited information system in accordance with DIACAP Instruction 8510.01? This course is designed to provide a complete guide to establishing a certifiable and accredited information system in any organization. Therefore, it will give you standards to measure the skills required of specific members of an organization in order to certify, review and accredit the IS security. These critical decisions are essential in making sure that the security of the IS outweighs the potential risks to an organization from any internal or external threats.

Course Objectives:

Upon successful completion of this course students will be able to:

- Establish a certified and accredited (authorized) information system in any organization according to current best practices and Federal standards
- Take the Mile2 ISCAP exam

Prerequisites:

- Broad Understanding of Multiple Networking and Security Technologies
- 12 months experience in information systems

Target Audience:

- Security Officers
- Authorizing Officials Information Owners
- Certifiers and Security Control Assessors
- Auditors
- Information Systems Owners
- Project Managers
- User and Business Representatives
- Government Employees

ISCAP: Information Security Accreditation & Certification Professional

Course ID #: 7000-816-ZZ-Z
Hours: 21

Topics:

Lesson 1 – Introduction

- Logistics
- Introduction
- Class Rules
- The ISCAP Credential
- What information will be covered?
- Relationship to Other Processes
- Changes in Terminology
- Understanding the Risk Management Framework
- NIST SP800-37 Rev1
- Emphasis of SP800-37
- Multi-tiered Risk Management
- The Risk Management Framework
- What information will be covered?
- Summary

Lesson 2 - Introduction to the RMF

- What's covered in this domain?
- The RMF
- The pillars of CIA
- National Strategy on Cybersecurity
- Cyber Attacks
- Federal Policy
- Actions of Executive Agencies
- Federal Policies
- E-Government Act of 2002
- FISMA
- Applying NIST
- What is Risk?
- Risk Management
- Risk Management Process
- IS Risk Management
- Threats
- Objectives of the RMF
- Effective Risk Management
- Multi-tiered Risk Management
- Key Parts of Tier 1
- Tier 2 Activities
- Key Parts of Tier 2
- Tier 3
  - Developing Trust
  - Frame Risk
  - Risk Assessment Process
  - Risk Responses
  - Risk Response Strategy
  - Risk Management Process
  - Monitoring Risk
  - Risk Monitoring Activities
  - Moving to the RMF
  - The RMF
  - Security Control Assessment
  - Applying the RMF
  - Applying the RMF cont.
  - The RMF Process

ISCAP: Information Security Accreditation & Certification Professional

Course ID #: 7000-816-ZZ-Z
Hours: 21

Lesson 3 - The Software Development Life Cycle
- The RMF Process
- Purpose of SP800-37
- Definitions
- Guidelines for Implementing SP800-37
- Relationship with other SPs
- Tiered Risk
- Management Approach
- Steps of the RMF
- Effective Controls
- The SDLC
- Balancing all Considerations
- The Phases of the SDLC Security Requirements
- Benefits of Early Integration
- Integration
- Integrated Project Teams
- Role of ISSOs
- Reuse of Information
- Benefits of Reuse
- Identifying Boundaries
- What is Security?
- Types of Controls

Lesson 4 - RMF Step 1
- The RMF Tasks
- Milestones
- Sequence
- The Last Step
- Legacy Systems
- Level of Effort Required
- The RMF Process
- Categorization
- Appropriate Controls
- SSP
- Information System Description
- Information System Registration

Lesson 5 - RMF Step 2
- Common Control Identification
- Common Controls
- Supplementing Common Controls
- Selection of Controls
- Control Selection
- Preparing for Monitoring
- Monitoring Strategy
- Control Monitoring
- Effective Monitoring
- Continuous Monitoring
- Security Plan Approval

Lesson 6 - RMF Step 3
- Security Control Implementation
- Common Controls
- Assessments
- Security Control Documentation
- Documentation
- Functional Description

Lesson 7 - RMF Step 4
- Assessment Preparation
- Approval of the Plan
- External Providers
- Assessor Competence
- Assessor Independence
- Security Control Assessment
- Assess and Recommend Findings
- Report
- Assessments
- Reassessment
- Updating the Security Plan
- The Updated Plan

ISCAP: Information Security Accreditation & Certification Professional

Course ID #: 7000-816-ZZ-Z
Hours: 21

Lesson 8 - RMF Step 5

- Plan of Action and Milestones
- Milestones
- Monitoring the PoA&M
- Documenting Weaknesses
- PoA&M Not Required
- Security Authorization Package
- Common Controls
- Updating the SSP
- Risk Determination
- Risk Acceptance
- Explicit Acceptance of Risk
- Risk Decision
- The Authorization Decision
- Communicating the Decision
- Authorization to Operate
- Termination Date
- Type Authorization
- Authorization Decision Document
- The Decision
- Termination Date
- Decision Document
- Change in Authorizing Official
- Acceptance of Previous Authorization

Lesson 9 - RMF Step 6

- Information System and Environment Changes
- Monitoring
- Updated Assessments
- Remediation Actions
- Reassessing Controls
- Key Updates
- Updating the SSP
- Updating the PoA&M
- Continuous Monitoring
- Security Status Reporting
- Ongoing Risk
- Determination and Acceptance
- Reviewing Reports
- Metrics and Dashboards
- Maintaining Security
- Information System Removal and Decommissioning
- Disposal

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535