Information Systems Certification and Accreditation Professional

KEY DATA

ACCREDITATIONS

Course Name:

Information Systems Certification & Accreditation Professional

Duration: 3 days

Language: English

Class Format Options:

- Instructor-led
- Live Virtual Training

Prerequisites:

- 12 months experience in information systems

Student Materials:

- Student Workbook

CPEs: 24 Hours

WHO SHOULD ATTEND?

- Information System Owners
- Information System Security Officers
- Authorizing Officials Information Owners
- Certifiers and Security Control Assessors
- System Managers
- Project Managers
- User and Business Representatives
- U.S. State and Local Governments

COURSE OVERVIEW

Mile2's vendor neutral **Information Systems Certification and Accreditation Professional** certificationtraining 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 certified 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 are 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.

IS Management Electives

C)ISSM™

ISCAP™*

C)ISRM™

All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)

  *in all technical classes
- Exam Prep Questions
- Exam

(ISCAP is CNSS NSTISSI-4015 National Training Standards for Systems Certifiers)

UPON COMPLETION

Upon completion, **Information Systems Certification and Accreditation Professional** students will be able to establish a certified and accredited (authorized) information system in any organization according to current best practices and Federal standards. Students will also be ready to take the ISCAP exam given by mile2.

EXAM INFORMATION

The Certified Information Systems Security Officer exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

COURSE CONTENT

I. **Introduction**
II. **Introduction to the Risk Management Framework**
III. **The Software Development Life Cycle**
IV. **Risk Management Framework Step 1**
V. **Risk Management Framework Step 2**
VI. **Risk Management Framework Step 3**
VII. **Risk Management Framework Step 4**
VIII. **Risk Management Framework Step 5**
IX. **Risk Management Framework Step 6**

DETAILED MODULE DESCRIPTION

Module 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

Module 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
Special Publications
800-39 Purpose
NIST SP 800-39
Information Systems
What is Risk?
Types of Risk
Security Risk
Information Security Risk
Core Documents
Risk Management
Risk Management Process
IS Risk Management
Threats
Objectives of the RMF
Effective Risk Management
Risk Tolerance / Acceptance
Risk Assessment
Risk Response
Risk Monitoring
Risk Management Process
Frame Risk
Multi-tiered Risk Management
Key Parts of Tier 1
Tier 2 Activities
Key Parts of Tier 2
IS Requirements Integration
Tier 3
Developing Trust
Trustworthiness
Frame Risk
Frame Risk Activities
Risk Assessment
Assess Risk Activities
Threat
Vulnerability
Likelihood
Adversarial Likelihood
Impact
Aggregation
Quantitative Risk
Qualitative Risk
Semi-Quantitative
Risk Assessment Process
Step 1 – Preparing for the Assessment
Conducting the Risk Assessment
Conducting the Risk Assessment
Communicating and Sharing Risk Assessment Information
Maintaining the Risk Assessment
Risk Management Process
Risk Responses
Risk Response Strategy
Risk Management Process
Monitoring Risk
Risk Monitoring Activities
Moving to the RMF
The RMF
Security Control Assessment

Module 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
Well-defined Boundaries
Correct Boundary Size
Size of Information System Boundaries
Key Words in Boundary Determination
Software Applications
Boundaries for Complex Systems
Complex System Boundaries
What is Security?
Allocation of Controls to Subsystems
Types of Controls
Architecture and Controls
Common Controls
Control Selection
Security Control Allocation
Summary

Module 4 - RMF Step 1

The RMF Tasks
RMF Tasks
Milestones
Sequence
The Last Step
Legacy Systems
Level of Effort Required
The RMF Process
Security Categorization
Categorization
Map Impact Levels
Influence of Architecture
Accuracy of Categorization
Impact–based Categorization
Categorization Levels
Format of Categorization
Categorization
Appropriate Controls
SSP
Information System Description
Information System Registration
System Registration
Milestone Checkpoint # 1
Summary

Module 5 - RMF Step 2

Common Control Identification
Common Controls
Supplementing Common Controls
Inheriting Controls
Common Control Providers
Documentation of Common Controls
Security Control Selection
Selection of Controls
Control Selection
Preparing for Monitoring
Monitoring Strategy
Control Monitoring
Effective Monitoring
Continuous Monitoring
Security Plan Approval
Milestone Checkpoint # 2

Module 6 - RMF Step 3

The RMF Process
Security Control Implementation
Security Controls
Security Control Assurance
Common Controls
Assessments
Security Control Documentation
Documentation
Functional Description
Milestone Checkpoint #3

Module 7 - RMF Step 4

The RMF Process
Assessment Preparation
The Assessment Plan
Purpose of the Plan
Type of Assessment
Approval of the Plan
External Providers
Assessor Competence
Assessor Independence
Security Control Assessment
Control Assessments
Timing of Assessments
Assess and Recommend Findings
Incremental Assessments
Access
Security Assessment Report
Assessment Report
Determination of Risk
Assessment Results
Remediation Actions
Report Findings
Response to Findings
Reassessment
Updating the Security Plan
The Updated Plan
Optional Addendum
Milestone #4

Module 8 - RMF Step 5

The RMF Process
Plan of Action and Milestones
PoA&M
Milestones
Monitoring the PoA&M
Documenting Weaknesses
PoA&M Not Required
Security Authorization Package
Common Controls
Updating the SSP
Risk Determination
Assess Current Security State
Risk Management Strategy
Risk Acceptance
Explicit Acceptance of Risk
Risk Decision
The Authorization Decision
Communicating the Decision
Authorization to Operate
Termination Date
Interim Authorization to Test
Interim Authorization to Operate
Type Authorization
Examples of Type Authorizations
Authorization Approaches
Authorization Rescission
Denial of Authorization
Authorization Decision Document
The Decision
Termination Date
Decision Document
Change in Authorizing Official
Acceptance of Previous Authorization
Milestone Checkpoint #5

Module 9 - RMF Step 6

The RMF Process
Information System and Environment Changes
Constant Change
Controlling Change
Record Changes
Impact on Security
Impact on Controls
Documenting Impact
Reauthorization
Ongoing Security
Control Assessments
Ongoing Monitoring
Continuous Monitoring
Control Monitoring
Ongoing Remediation Actions
Updated Assessments
Remediation Actions
Reassessing Controls
Key Updates
Updating the SSP
Updating the PoA&M
Supporting
Continuous Monitoring
Security Status Reporting
Reporting to
the Authorizing Official
Security Status Reports
Frequency of Reporting
Reauthorization
Ongoing Risk
Determination and Acceptance
Reviewing Reports
Metrics and Dashboards
Maintaining Security
Information System Removal and
Decommissioning
Disposal
Milestone Checkpoint #6