Course Name: Information Systems Certification & Accreditation Professional

Duration: 3 days
Language: English
Format: Instructor-led Live Virtual Training

Prerequisites:
- A minimum of 12 months experience in systems development or design

Student Materials:
- Course Book

COURSE OVERVIEW

Mile2’s Information Systems Certification and Accreditation Professional 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 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.

ACCREDITATIONS

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, 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 enjoy an in-depth course that is continuously updated to maintain and incorporate the ever-changing security and risk environment.

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

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
DETAILED MODULE DESCRIPTION

Module 0 – 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 1 - 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
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
Applying the RMF
Module 2 - 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

Module 3 - 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

Module 4 - 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

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

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

Monitoring Strategy
- Control Monitoring
- Effective Monitoring
- Continuous Monitoring
- Security Plan Approval
- Milestone Checkpoint # 2
### Module 5 - RMF Step 3

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

### Module 6 - RMF Step 4

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

### Module 7 - RMF Step 5

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

### Module 8 - RMF Step 6

| The RMF Process | Impact on Controls |
| Information System and Environment Changes | Documenting Impact |
| Constant Change | Reauthorization |
| Controlling Change | Ongoing Security |
| Record Changes | Control Assessments |
| Impact on Security | 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