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.

Description:

Mile2's IS Certification & Accreditation Professional training teaches 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.



,663,6629

Icon

Description automatically generated

Annual Salary Potential $91,000 AVG/year





Logo

Description automatically generated

\* Security Officers

\* Authorizing Officials Information Owners

\* Certifiers and Security Control Assessors

\* Auditors

\* Information Systems Owners

\* Project Managers

\* User and Business Representatives

\* Government Employees

Modules/Lessons

Who Should Attend

**Live Class Duration:** 3 Days

**CEUs:** 24

**Language:** English

**Class Formats Available:**

Instructor Led

Self-Study

Live Virtual Training

**Suggested Prerequisites:**

- Broad Understanding of Multiple Networking and Security Technologies

- 12 months experience in information systems.

Key Course Information



Module 1 - Introduction

Module 2 - Introduction to the Risk Management Framework

Module 3 - The Software Development Life Cycle

Module 4- RMF Step 1

Module 5 - RMF Step 2

Module 6 - RMF Step 3

Module 7 - RMF Step 4

Module 8 - RMF Step 5

Module 9 - RMF Step 6

Key Course Information

Accreditations

Re-Certification Requirements

Upon Completion

The Information System Certification and Accreditation Professional exam is taken online through Mile2’s Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1. Pass the most current version of the exam for your respective existing certification
2. Earn and submit 20 CEUs per year in your Mile2 account.

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.

**Question:** Do I have to purchase a course to buy a certification exam?

Answer: No

**Question:** Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at [www.mile2.com](http://www.mile2.com).

**Question:** Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

**Question:** Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course FAQ’s

Exam Information

Course and Certification Learning Options

Graphical user interface, application

Description automatically generated





Detailed Outline:

Module 1 – Introduction

1. Logistics
2. Introduction
3. Class Rules
4. The ISCAP Credential
5. What information will be covered?
6. Relationship to Other Processes
7. Changes in Terminology
8. Understanding the Risk Management Framework
9. NIST SP800-37 Rev1
10. Emphasis of SP800-37
11. Multi-tiered Risk Management
12. The Risk Management Framework
13. What information will be covered?
14. Summary

Module 2 - Introduction to the RMF

1. What’s covered in this domain?
2. The RMF
3. The pillars of CIA
4. National Strategy on Cybersecurity
5. Cyber Attacks
6. Federal Policy
7. Actions of Executive Agencies
8. Federal Policies
9. E-Government Act of 2002
10. FISMA
11. Applying NIST
12. What is Risk?
13. Risk Management
14. Risk Management Process
15. IS Risk Management
16. Threats
17. Objectives of the RMF
18. Effective Risk Management
19. Multi-tiered Risk Management
20. Key Parts of Tier 1
21. Tier 2 Activities
22. Key Parts of Tier 2
23. Tier 3
    1. Developing Trust
    2. Frame Risk
    3. Risk Assessment Process
    4. Risk Responses
    5. Risk Response Strategy
    6. Risk Management Process
    7. Monitoring Risk
    8. Risk Monitoring Activities
    9. Moving to the RMF
    10. The RMF
    11. Security Control Assessment
    12. Applying the RMF
    13. Applying the RMF cont.
    14. The RMF Process

Module 3 - The Software Development Life Cycle

1. The RMF Process
2. Purpose of SP800-37
3. Definitions
4. Guidelines for Implementing SP800-37
5. Relationship with other SPs
6. Tiered Risk
7. Management Approach
8. Steps of the RMF
9. Effective Controls
10. The SDLC
11. Balancing all Considerations
12. The Phases of the SDLC Security Requirements
13. Benefits of Early Integration
14. Integration
15. Integrated Project Teams
16. Role of ISSOs
17. Reuse of Information
18. Benefits of Reuse
19. Identifying Boundaries
20. What is Security?
21. Types of Controls

Module 4 - RMF Step 1

1. The RMF Tasks
2. Milestones
3. Sequence
4. The Last Step
5. Legacy Systems
6. Level of Effort Required
7. The RMF Process
8. Categorization
9. Appropriate Controls
10. SSP
11. Information System Description
12. Information System Registration

Module 5 - RMF Step 2

1. Common Control Identification
2. Common Controls
3. Supplementing Common Controls
4. Selection of Controls
5. Control Selection
6. Preparing for Monitoring
7. Monitoring Strategy
8. Control Monitoring
9. Effective Monitoring
10. Continuous Monitoring
11. Security Plan Approval

Module 6 - RMF Step 3

1. Security Control Implementation
2. Common Controls
3. Assessments
4. Security Control Documentation
5. Documentation
6. Functional Description

Module 7 - RMF Step 4

1. Assessment Preparation
2. Approval of the Plan
3. External Providers
4. Assessor Competence
5. Assessor Independence
6. Security Control Assessment
7. Assess and Recommend Findings
8. Report
9. Assessments
10. Reassessment
11. Updating the Security Plan
12. The Updated Plan

Module 8 - RMF Step 5

1. Plan of Action and Milestones
2. Milestones
3. Monitoring the PoA&M
4. Documenting Weaknesses
5. PoA&M Not Required
6. Security Authorization Package
7. Common Controls
8. Updating the SSP
9. Risk Determination
10. Risk Acceptance
11. Explicit Acceptance of Risk
12. Risk Decision
13. The Authorization Decision
14. Communicating the Decision
15. Authorization to Operate
16. Termination Date
17. Type Authorization
18. Authorization Decision Document
19. The Decision
20. Termination Date
21. Decision Document
22. Change in Authorizing Official
23. Acceptance of Previous Authorization

Module 9 - RMF Step 6

1. Information System and Environment Changes
2. Monitoring
3. Updated Assessments
4. Remediation Actions
5. Reassessing Controls
6. Key Updates
7. Updating the SSP
8. Updating the PoA&M
9. Continuous Monitoring
10. Security Status Reporting
11. Ongoing Risk
12. Determination and Acceptance
13. Reviewing Reports
14. Metrics and Dashboards
15. Maintaining Security
16. Information System Removal and Decommissioning
17. Disposal