

## Description:

Mile2's Risk Management Framework Analyst training quantifies the process of certifying, reviewing, and accrediting an information system by IT professionals.

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.



**Annual Salary Potential \$120,077 AVG/year**

Key Course Information	Modules/Lessons	Case Study Labs
<p><b>Live Class Duration:</b> 5 Days  <b>CEUs:</b> 40  <b>Language:</b> English  <b>Class Formats Available:</b></p> <ul style="list-style-type: none"> <li>Instructor Led</li> <li>Self-Study</li> <li>Live Virtual Training</li> </ul> <p><b>Suggested Prerequisites:</b>                      (any one of the following)                      This is an advanced look into how the RMF applies to government systems. 4-5 years of information systems security management is suggested (or equivalent education).</p>	<p><b>Introduction</b>  <b>Module 1</b> -Introduction to the RMF  <b>Module 2</b> -The Software Development Life Cycle  <b>Module 3</b> – RMF Stage 1  <b>Module 4</b> – RMF Stage 2  <b>Module 5</b> - RMF Stage 3  <b>Module 6</b> – RMF Stage 4  <b>Module 7</b> – RMF Step 5  <b>Module 8</b> – RMF Step 6</p>	<p><b>Introduction</b>  <b>Lab 1</b> – RMF Structure  <b>Lab 2</b> – RMF Integration into the SDLC  <b>Lab 3</b> – RMF Implementation: Prepare  <b>Lab 4</b> – RMF Implementation: Categorize  <b>Lab 5</b> – RMF Implementation: Select  <b>Lab 6</b> – RMF Implementation: Implement  <b>Lab 7</b> – RMF Implementation: Assess  <b>Lab 8</b> – RMF Implementation: Authorize  <b>Lab 9</b> – RMF Implementation: Monitor</p>

## Upon Completion

Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the exam.

## Who Should Attend

- IS Security Owners
- Security Officers
- Ethical Hackers
- Information Owners
- Penetration Testers
- System Owners and Managers
- Cyber Security Engineers

## Accreditations



## Exam Information

The exam is taken online through Mile2's Learning Management System and is accessible on your 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.

## Re-Certification Requirements

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.

## Course FAQ's

**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).

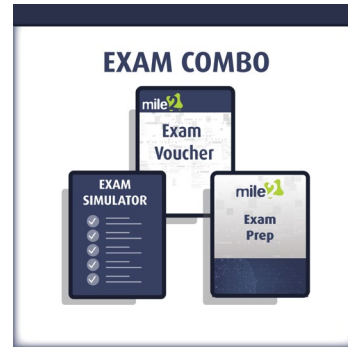
**Question:** Are all courses available as self-study courses?

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 and Certification Learning Options



## Detailed Outline:

### DETAILED MODULE DESCRIPTION

#### Module 0 – Introduction

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

#### Module 1 - Introduction to the RMF

What's covered in this domain?	Information Systems
The RMF	What is Risk?
The pillars of CIA	Types of Risk
National Strategy on Cybersecurity	Security Risk
Cyber Attacks	Information Security Risk
Federal Policy	Core Documents
Actions of Executive Agencies	Risk Management
Federal Policies	Risk Management Process
E-Government Act of 2002	IS Risk Management
FISMA	Threats
Applying NIST Special Publications	Objectives of the RMF
800-39 Purpose	Effective Risk Management
NIST SP 800-39	Risk Tolerance / Acceptance

Risk Assessment	Quantitative Risk
Risk Response	Qualitative Risk
Risk Monitoring	Semi-Quantitative
Risk Management Process	Risk Assessment Process
Frame Risk	Step 1 – Preparing for the Assessment
Multi-tiered Risk Management	Conducting the Risk Assessment
Key Parts of Tier 1	Conducting the Risk Assessment
Tier 2 Activities	Communicating and Sharing Risk Assessment Information
Key Parts of Tier 2	Maintaining the Risk Assessment
IS Requirements Integration	Risk Management Process
Tier 3	Risk Responses
Developing Trust	Risk Response Strategy
Trustworthiness	Risk Management Process
Frame Risk	Monitoring Risk
Frame Risk Activities	Risk Monitoring Activities
Risk Assessment	Moving to the RMF
Assess Risk Activities	The RMF
Threat	Security Control Assessment
Vulnerability	Applying the RMF
Likelihood	Applying the RMF cont.
Adversarial Likelihood	The RMF Process
Impact	Summary
Aggregation	

## Module 2 - The Software Development Life Cycle

The RMF Process	Benefits of Reuse
Purpose of SP800-37	Identifying Boundaries
Definitions	Well-defined Boundaries
Guidelines for Implementing SP800-37	Correct Boundary Size
Relationship with other SPs	Size of Information System Boundaries
Tiered Risk Management Approach	Key Words in Boundary Determination
Steps of the RMF	Software Applications
Effective Controls	Boundaries for Complex Systems
The SDLC	Complex System Boundaries
Balancing all Considerations	What is Security?
The Phases of the SDLC Security Requirements	Allocation of Controls to Subsystems
Benefits of Early Integration	Types of Controls
Integration	Architecture and Controls
Integrated Project Teams	Common Controls
Role of ISSOs	Control Selection
Reuse of Information	Security Control Allocation
	Summary

## Module 3 - RMF Step 1

The RMF Tasks	Security Categorization
RMF Tasks	Categorization
Milestones	Map Impact Levels
Sequence	Influence of Architecture
The Last Step	Accuracy of Categorization
Legacy Systems	Impact-based Categorization
Level of Effort Required	Categorization Levels
The RMF Process	Format of Categorization

Categorization

Appropriate Controls

SSP

Information System Description

## 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

## Module 5 - RMF Step 3

The RMF Process

Security Control Implementation

Security Controls

Security Control Assurance

Common Controls

## Module 6 - RMF Step 4

The RMF Process

Assessment Preparation

The Assessment Plan

Purpose of the Plan

Type of Assessment

Information System Registration

System Registration

Milestone Checkpoint # 1

Summary

Preparing for Monitoring

Monitoring Strategy

Control Monitoring

Effective Monitoring

Continuous Monitoring

Security Plan Approval

Milestone Checkpoint # 2

Assessments

Security Control Documentation

Documentation

Functional Description

Milestone Checkpoint #3

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 7 - 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

The RMF Process	Continuous Monitoring
Information System and Environment Changes	Control Monitoring
Constant Change	Ongoing Remediation Actions
Controlling Change	Updated Assessments
Record Changes	Remediation Actions
Impact on Security	Reassessing Controls
Impact on Controls	Key Updates
Documenting Impact	Updating the SSP
Reauthorization	Updating the PoA&M
Ongoing Security Control Assessments	Supporting Continuous Monitoring
Ongoing 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