Certified Risk Manager Framework Analyst

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

Live Class Duration: 3 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:
(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).

Modules/Lessons

Introduction
Module 1 -Intro to the RMF
Module 2 -The RMF Integration into the Software Development Life Cycle
Module 3 – The Prepare Stage of the RMF Model
Module 4 – Categorize the System
Module 5 – Select Security Controls
Module 6 – Implement Security Controls
Module 7 – Assess Security Controls
Module 8 – Authorize Information System
Module 9 – Monitor Security Controls
Module 10 -RMF Process Deployment Considerations

Case Study Labs

Introduction
Lab 1 – RMF Structure
Lab2 – RMF Integration into the SDLC
Lab 3 – RMF Implementation: Prepare
Lab 4 – RMF Implementation: Categorize
Lab 5 – RMF Implementation: Select
Lab 6 – RMF Implementation: Implement
Lab 7 – RMF Implementation: Assess
Lab 8 – RMF Implementation: Authorize
Lab 9 – RMF Implementation: Monitor

Certified Risk Manager Framework Analyst

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 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.

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.

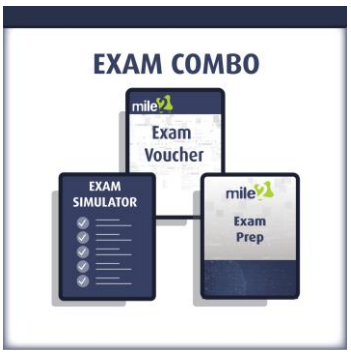
Question: Are all courses available as self-study courses?

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

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

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

Applying the RMF cont.

The RMF Process

Summary

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

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 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

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 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

Monitoring Strategy

Control Monitoring

Effective Monitoring

Continuous Monitoring

Security Plan Approval

Milestone Checkpoint # 2

Module 5 - 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 6 - 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 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

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

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779