



# Federal Risk Management Framework (RMF) Implementation 4.0: DoD/IC Edition

**Days of Training: 4**

## **Course Description**

*Federal Risk Management Framework (RMF) Implementation 4.0* focuses on the Risk Management Framework prescribed by NIST Standards. This courseware covers most but not all of the objectives of the ISC2 Certified Authorization Professional (CAP) certification exam. It can be used as an aid in CAP exam preparation, but if your goal is primarily to prepare students for that exam, you should use our other RMF course, [Federal Risk Management Framework \(RMF\) Implementation 4.0 and CAP Exam Prep](#).

The 4.0 edition of the course is current as of August 2017. This edition incorporates the revisions to DODI 8510.01 CHANGE 1 from 2016, the development and publication of the CNSSI-1254 for the IC, additional NIST Special Publications produced to support RMF steps and activities, updated JSIG published in 2016, and newly developed service component actions and updates from the RMF Knowledge Service which have been uploaded and made available for all DOD components to use and implement during their RMF authorization efforts.

Downloadable ancillary materials include a study guide and a References and Policies handout.

## **Outline**

### Introduction

- Introductions
- About the CAP exam
- Table of contents

### Chapter 1: Introduction

- RMF overview
- DoD and Intelligence Community specific guidelines
- Key concepts including assurance, assessment, authorization
- Security controls

### Chapter 2: Cybersecurity Policy Regulations and Framework

- Security laws, policy, and regulations
- DIACAP to RMF transition
- ICD 503
- CNSSI-1253
- SDLC and RMF
- Documents for cyber security guidance

### Chapter 3: RMF Roles and Responsibilities



Tasks and responsibilities for RMF roles  
DoD RMF roles

#### Chapter 4: Risk Analysis Process

DoD organization-wide risk management  
RMF steps and tasks  
RMF vs. C&A

#### Chapter 5: Step 1: Categorize

Step 1 key references  
Sample SSP  
Task 1-1: Security Categorization  
Task 1-2: Information System Description  
Task 1-3: Information System Registration  
Registering a DoD system  
Lab Step 1: Categorize

#### Chapter 6: Step 2: Select

Step 2 key references  
Task 2-1: Common Control Identification  
Task 2-2: Select Security Controls  
Task 2-3: Monitoring Strategy  
Task 2-4: Security Plan Approval  
Lab Step 2: Select Security Controls

#### Chapter 7: Step 3: Implement

Step 3 key references  
Task 3-1: Security Control Implementation  
Task 3.2: Security Control Documentation  
Lab Step 3: Implement Security Controls

#### Chapter 8: Step 4: Assess

Step 4 key references  
About Assessment  
Task 4-1: Assessment Preparation  
Task 4-2: Security Control Assessment  
Task 4-3: Security Assessment Report  
Task 4-4: Remediation Actions  
Lab Step 4: Assessment Preparation

#### Chapter 9: Step 5: Authorize

Step 5 key references  
Task 5-1: Plan of Action and Milestones  
Task 5-2: Security Authorization Package



Task 5-3: Risk Determination

Task 5-4: Risk Acceptance

Lab Step 5: Authorizing Information Systems

#### Chapter 10: Step 6: Monitor

Step 6 key references

Task 6-1: Information System and Environment Changes

Task 6-2: Ongoing Security Control Assessments

Task 6-3: Ongoing Remediation Actions

Task 6-4: Key Updates

Task 6-5: Security Status Reporting

Task 6-6: Ongoing Risk Determination and Acceptance

Task 6-7: Information System Removal and Decommissioning

Continuous Monitoring

Security Automation Domains

Lab Step 6: Monitoring Security Controls

#### Chapter 11: RMF for DoD and the Intelligence Community

eMASS

RMF Knowledge Service

DoD 8510.01

DFAR 252.204-7012

ICD 503

CNSSI-1253

FedRAMP

RMF within DoD and IC process review

#### Reference

Acronym reference

RMF process checklists by step

Review question answer key

Lab question answer key