Risk Management Framework (RMF)

Length: 2 Days

Summary: In this course, you will gain a thorough understanding of the new DoD authorization process as required by DoDI 8510.01, Risk Management Framework for DoD IT, 14 March 2014, and based on the new Committee of National Security Systems Instruction 1253 (CNSSI 1253), Security Categorization and Security Control Selection for National Security Systems (NSS), 27 March 2014, and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)

You will learn how to apply cost-effective and appropriate security controls based on risk and best practices. This highly interactive course provides actual examples of the key documents required to complete the RMF processes.

Course Objectives:

- Authorization process
- Risk management
- Risk assessment
- Roles and responsibilities
- RMF tools
- Categorize information and information systems
- Select, implement, and assess security controls
- Authorize information system
- Monitor security controls

COURSE CONTENT

1: UNDERSTAND SECURITY AUTHORIZATION

- Concept of Authorization Process
- Problem, Controls, Implement, Assess, Approve and Maintain
- Authorization Evolution
- DITSCAP, NIACAP, FISMA, NIST, DIACAP, and RMF
- Department of Defense (DoD) Risk Management Framework (RMF)
- DoD: DoDI 8500.01 and DoDI 8510.01
- CNSS: CNSSP-42, CNSSI-1253 and Appendix K Annexes, CNSSI-1253A, and CNSS 4009
- NIST: SP 800-18, SP 800-37, SP 800-39, SP 800-53, SP 800,53A, SP 800-137, and SP 800-160
- Roles and Responsibilities (NIST SP800-37 and DoD 8510.01)
- DoD and Component Chief Information Officers (CIO)
- Risk Executive (Function)
- DoD and Component Senior Information Security Officer (SISO)
- Authorizing Official (AO)
- AO Designated Representative (AODR)
- Information Owner (IO) /Steward
- Common Control Provider (CC Provider)
- Information System Security Manager (ISSM)
- Information System Owner (ISO)
- Information System Security Engineer ISSE)
- Security Control Assessor (SCA)
- User Representative (UR)

- RMF Tools - DoDI 8510.01
- eMASS and Information Assurance Support Environment (IASE)
- Security Processes and Concepts
- Adequate Security and Risk-Based Cost-Effective - OMB Circular A-130
- Security Objectives: Confidentiality, Integrity and Availability
- Risk: Low, Moderate, and High
- Privacy Rules: HIPAA and Personally Identifiable Information (PII)
- Trust Relationships: Reciprocity and Documents
- Defense-in-Depth
- Risk Management (NIST SP800-39)
- Risk Assessment (NIST SP800-30)
- Qualitative, Quantitative, and Quasi-Quantitative
- Risk Assessment Group Exercise

2: RMF STEP 1 - CATEGORIZE INFORMATION AND INFORMATION SYSTEM

- System Security Plan - SP 800-18, SP 800-37
- DoD IT Products, Services, and PIT - DoDI 8510.01
- Categorization - CNSSI-1243, FIPS 199, and SP 800-60
- Overlays- CNSSI- 1253 and SP800-53
- Risk Impact Factors - CNSSI-1253 and SP800-53
- Accreditation Boundaries - SP 800-18 and SP 800-37
- Boundary and Categorization Group Exercise
- Interconnecting Information Systems - SP 800-47
- Registration - SP 800-53
- Assigned Qualified Personnel - DoDD 8570.01 and DoDD 8140.01

3: RMF STEP 2 - SELECT SECURITY CONTROLSSPECIFIC, COMMON AND HYBRID CONTROLS - SP 800-53, CNSSI-1253, AND SAMPLE SP

- Type Control Group Exercise
- Overlays - CNSSI-1253, SP 800-53, and Sample Overlay
- Selecting Security Controls - CNSSI-1253, FIPS-200, and SP 800-53
- Tailoring Controls - CNSSI-1252 and SP 800-53
- Tailoring Controls Group Exercise
- Compensating Controls- SP800-53
- Compensating Control Group Exercise
- Trustworthiness and Assurance - SP 800-53
- Monitored Control Selection - SP 800-37
- Approval and Registration- DoDI 8510.01
- Knowledge Services and eMASS

4: RMF STEP 3 - IMPLEMENT SECURITY CONTROLS

- Security Control Implementation - SP 800-53
- Control Documentation- SP800-18 and SP800-37
- Approved Configurations, Tests and Checklists - SP 800-70, eMASS and IASE.mil
- Security Content Automation Protocol (SCAP) - SP800-115 and SP800-117

5: RMF STEP 4 - ASSESS SECURITY CONTROLS

- Assessment and Testing Methods - SP 800-53A and SP 800-115
- Vulnerability Tools and Techniques - SP 800-53A and SP 800-115
- Develop Security Assessment Plan and Report - SP 700-37 and Sample SAR
- Assessor Expertise and Independence - SP 800-37 and DoDI 8510.01
- Assess Security Control- SP800-53A and SP800-115
- Conduct Security Control Assessments - SP800-37 and SP800-53

6: RMF STEP 5 - AUTHORIZE INFORMATION SYSTEM SPECIAL DOD SYSTEMS - DODI 8510.01

- Plan of Actions and Milestones (POA&M) - OMB M-01-01 and Sample POA&M
- Security Authorization Package - SP 800-37 and DoDI 8510.01
- SSP, SAR, and POA&M
- Authorization - SP 800-37 and DoDI 8510-01
- Authority to Operate (ATO)
- Interim Authorization to Test (IATT)
- Denial of Approval to Operate (DATO)
- Special Authorizations - DoDI 8510.01
- Type Authorizations
- Platform Information Technology (PIT) Authorizations
- Contingency Strategies
- Group Contingency Deployment Group Exercises

7: RMF STEP 6 - MONITOR SECURITY CONTROLS INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) - SP 800-137 AND HBSS

- Patch and Vulnerability Management - SP 800-40
- Cloud Computing- FedRAMP, FedRAMP+, SP800-53, and SRG
- DoD RMF Schedule, Status and Issues- DoDI 8510.01
- Appendixes
- Regulations and Standards
- Authorization Evolution
- DoD RMF Processes
- Risk Management Framework Steps and Tasks
- SDLC, RMF and FIPS/SP Pub Relationship Table
- Information Security Plan (SP) Template
- Control Families
- Plan of Action and Milestones (POA&M)
- Continuous Monitoring Action Samples
- Resources Schedule of Continuous Monitoring Actions
- Security Control Overlay Template
- Security Control Monitoring Frequencies
- Patch and Vulnerability Management ROI
- DoD Cybersecurity Glossary