Federal Risk Management Framework (RMF) v2022

Days: 4

Prerequisites: There are no specific prerequisites for this course. However, general computer user knowledge is assumed. Any additional experience having worked with forms and/or databases will be helpful.

Audience: It is intended to support risk management framework (RMF) assessment and accreditation.

Description: Risk Management Framework (RMF) for DoD/IC Implementation 2022 focuses on the Risk Management Framework prescribed by NIST Standards and guided by DoD Instructions. This course is current as of May 2022. It was revised due to NIST producing new and updated publications over the preceding two years, including NIST Special Publication (SP) 800-37 R2; SP-800-53 R5; SP 800-53A R5; SP 800-53B; SP 800-160, versions 1 and 2; SP 800-171 R1 (among others); and various DoD updates to Instructions and guidance documentation.

Chapter 1: RMF, cybersecurity policy regulations, and roles and responsibilities

Module A: Introduction to RMF
Module B: Cybersecurity policy regulations and framework
Module C: RMF roles and responsibilities

Chapter 2: Risk analysis

Module A: Risk management
Module B: Risk assessment and the RMF process

Chapter 3: The RMF process

Module A: Step 0—Prepare
Module B: Step 1—Categorize
Module C: Step 2—Select
Module D: Step 3—Implement
Module E: Step 4—Assess
Module F: Step 5—Authorize
Module G: Step 6—Monitor

Chapter 4: DoD RMF–specific areas

Area A: eMASS
Area B: DoD's CYBER.MIL site and resources
Area C: Continuous Monitoring and Risk Scoring (CMRS)
Area D: RMF Knowledge Service (RMFKS)
Area E: Joint SAP Implementation Guide (JSIG)

Appendices

Appendix A: RMF reference documents
Appendix B: Acronym reference
Appendix C: Steps of the RMF—Answers key
Appendix D: Lab Exercises for RMF Steps