# Risk Management Framework (RMF) (SEC-RMF)

**Modality: Virtual Classroom**

**Duration: 4 Days**

## About this course:

The Department of Defense is replacing the old security management program legacy Certification of Accreditation (C&A) processes with the Risk Management Framework (RMF) as a unified security Framework. Federal Risk Management Framework is now used in the departments and agencies of federal government including the Department of Defense (DOD) and intelligence Community (IC). RMF is fundamental for the implementation of the Federal Information Security Management Act

Transition from DIACAP to RMF in the department of defense has made the course Federal Risk Management Framework (RMF) specifically beneficial for the employees and contractors of Department of Defense. The courseware for the Risk Management Framework (RMF) incorporates the publications and recommendations of National Institute of Standard and Technology (NIST) and the Committee on National Security System (CNSS).

## Course Outline:

### Module 1

- Define the important concepts: assurance, assessment, authorization
- List the three key characteristics of security
- List the reasons for the widespread change to the Risk Management Framework (RMF)
- Define security controls and list examples of the three classes of controls

### Module 2

- Describe the evolution and interaction of security laws, policy, and regulations in information security
- List the DoD IA policy drivers
- Access the correct documents for information assurance guidance
- Describe Assessment and Authorization transformation goals

### Module 3

- Understand and assign the correct roles in the RMF process for your organization
- Perform the responsibilities associated with your RMF role
- Identify the RMF roles of your colleagues

### Module 4

- Support and follow the four-step risk management process within your agency
- Understand the factors that produce the impact level (high, medium, low) of your information

system
- Accurately quantify the level of risk to your information system
- Decide on the effective risk management options for your system

**Module 5**

- Identify the six steps in the RMF process
- Produce or support the production of the key documents in the RMF process
- Categorize the security characteristics of confidentiality, integrity and availability for an information system as high, medium, or low
- Describe the information processed, stored and transmitted by your information system
- Register an information system

**Module 6**

- Identify your information system's common controls
- Select the appropriate baseline controls for your information system
- Tailor security controls for your information system
- Supplement the baseline and tailored controls for your information system
- Develop and/or support a continuous monitoring strategy for your information system

**Module 7**

- Allocate the appropriate security controls for your information system
- Implement the security controls for your information system
- Describe your information system in a functional manner appropriate for documentation in the security plan

**Module 8**

- Use one or more of the three methods of assessment to assess your information system's security controls
- Prepare or support the preparation of the security assessment report documenting the issues, findings, and recommendations from the security control assessment

**Module 9**

- Support the creation and completion of the plan of action and milestones (POAM) in accordance with your RMF role
- Describe the contents of the security authorization package
- Authorize or support the authorization of the information system
- State the level of acceptable risk for your information system
- Adhere to the correct procedures when a system is authorized to operate, given interim authorization, or not authorized to operate

**Module 10**

- Manage, control and document changes to your information system and its environment of

operation
- Implement the correct forms of patches when the situation calls for a patch
- Select or support the selection of the appropriate assessments
- State the characteristics of good performance measures and choose accordingly
- Report or react to the reporting of vulnerabilities and mitigation
- Decommission an information system in the most efficient of the four methods based on the type of information captured, process or stored by the information system

**Module 11**

- Utilize information assurance tools such as eMass to improve the A&A process
- Access the DIACAP Knowledge Service for up-to-date information on the risk management framework
- Understand the purpose and use of CyberScope