Information Security Continuous Monitoring (ISCM) Overview

Training Program Overview & Outline

Training Overview

This one-day core curriculum add-on training program focuses on Information Security Continuous Monitoring (ISCM), which is one of the cornerstones of RMF. Topics include:

- ISCM Roles and responsibilities
- ISCM Process – NIST SP 800-137
  - Step 1 – Define Strategy
  - Step 2 – Establish ISCM program
  - Step 3 – Implement
  - Step 4 – Analyze and Report
  - Step 5 – Respond to Findings
  - Step 6 – Review a\nd Update
- ISCM Technologies
- ISCM Challenges & Pitfalls

Practical guidance on ISCM automation and support tools is provided. Student exercises, collaboration and case studies are used to reinforce the concepts taught in the class.

The course content of Information Security Continuous Monitoring (ISCM) is geared to meet the needs of a diverse audience covering the spectrum of management, operational and technical roles.

Students will gain thorough knowledge of the theory and policy background underlying continuous monitoring as well as the practical knowledge needed for effective implementation.

Course Prerequisites

A prerequisite to this course is a strong understanding of RMF, and it is highly recommended students complete the 4-day RMF training program prior to registration.

Who should attend?

The Continuous Monitoring training program is suitable for government employees and contractors in DoD, federal “civil” agencies and the intelligence community, particularly those responsible for managing and monitoring security posture on an ongoing basis.

Information Security Continuous Monitoring (ISCM) – One-Day Course

ISCM Overview	Establish ISCM Program
ISCM Background	Implement ISCM Program
Organization Perspective	Analyze Data / Report Findings
Ongoing System Authorizations	Respond to Findings
Automation	Review and Update Monitoring Program and Strategy
ISCM Roles and Responsibilities	Implementation of ISCM
ISCM Process – NIST SP 800-137 • Step 1 – Define Strategy • Step 2 – Establish ISCM program • Step 3 – Implement • Step 4 – Analyze and Report • Step 5 – Respond to Findings • Step 6 – Review and Update	ISCM Technologies • Security Automation Domains • Security Information and Event Management (SIEM) • Continuous Monitoring and Risk Scoring (CMRS)
DHS Support of FISMA & ISCM	ISCM Challenges and Pitfalls