COURSE SYLLABUS

FISMA & Continuous Monitoring Fundamentals Course

An ATO is a beginning, not an ending — federal systems must be watched continuously, with weaknesses tracked and risk reported to leadership over time. This intermediate course grounds Information Security Continuous Monitoring (NIST SP 800-137) in FISMA accountability: design an ISCM strategy, work findings through POA&Ms, and build the metrics and reporting that make ongoing authorization possible.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/fisma-and-continuous-monitoring-fundamentals



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: FISMA Governance, Accountability, and Risk Oversight

Examine the statutory foundation of FISMA and the roles responsible for cybersecurity governance, accountability, and risk oversight.

Module 2: Designing an ISCM Strategy

Develop an information security continuous monitoring strategy aligned with NIST Special Publication 800-137.

Module 3: Asset, Configuration, and Vulnerability Visibility

Review the asset, configuration, and vulnerability data needed to support effective continuous monitoring.

Module 4: Control Monitoring, Assessment, and Evidence Management

Maintain current control assessments and supporting evidence throughout the system lifecycle.

Module 5: Security Metrics, Analysis, and Risk Reporting

Convert monitoring data into meaningful security metrics, analysis, and risk reporting for decision-makers.

Module 6: Findings, POA&Ms, and Risk-Based Response

Manage identified weaknesses through Plans of Action and Milestones and prioritize corrective actions based on risk.

Module 7: Ongoing Authorization and ISCM Program Evaluation

Explore how continuous monitoring supports ongoing authorization and evaluate the effectiveness of an ISCM program.

Module 8: Building a Continuous Monitoring Program Capstone

Design an end-to-end continuous monitoring program that integrates strategy, data collection, assessment, reporting, and risk response.