CNSSI – 4016: Risk Analyst

Length: 4 Days

Summary: CNSS-4016 The Risk Analysis and Risk Management Framework (RMF) curriculum was specifically designed for cybersecurity practitioners that exercise security or Assessment and Authorization (A&A) as well as Program or Acquisition Management control over critical information infrastructures.

This course provides four days of highly concentrated, non-technical professional training necessary to achieve the fundamental knowledge, skills, and abilities needed to analyze, assess, control, determine, mitigate and manage risks within computer systems that store, process, display or transmit classified or sensitive information. This course provides training in knowledge factors and functional requirements established for Entry and Intermediate Level Risk Analysts and addresses professional processes and policy requirements established within the federal Risk Management Framework (RMF). Specific focus is directed on identifying, implementing and integrating management, acquisition and administrative risk methodologies for securing critical information infrastructures and establishing standards necessary to help protect the confidentiality, maintain the integrity and ensure the availability of critical organizational computing resources within a risk managed framework. Topical areas include those actions and activities necessary to facilitate risk centric analysis and assessment requirements as well as RMF actions and activities necessary to ensure that Authorizing Officials (AO's) have the information necessary to make informed, risk-based decisions. Special attention is directed on analyzing, evaluating, and assessing information system security risks and the procedures necessary to assess the impact and consequence of a realized risk on critical information infrastructures.

COURSE CONTENT

1. FUNDAMENTALS OF THREAT/VULNERABILITY ANALYSIS & RISK MGMT
2. INFORMATION SYSTEM CONTROLS & THE SYSTEM DEVELOPMENT LIFE-CYCLE (SDLC)
3. RISK PLANNING IN CONSEQUENCE MANAGEMENT & PROTECTION STRATEGIES
4. RISK MONITORING & COUNTERMEASURE IDENTIFICATION, IMPLEMENTATION, AND ASSESSMENT
5. RISK IDENTIFICATION ASSESSMENT & EVALUATION
6. SYNTHESIS OF RISKS & ANALYSIS
7. RISK ASSESSMENT, TESTING, AND EVALUATION
8. THREAT AND ADVERSARY ANALYSIS
9. FEDERAL RISK MANAGEMENT FRAMEWORK (RMF)
10. MISSION & ASSETS RISK MANAGEMENT
11. VULNERABILITIES AND ATTACK AVENUES ANALYSIS
12. RISK TRAINING, POLICIES AND LEGAL ISSUES