IA2 Information Assurance Associates, Inc.

CNSS-4016 National Information Assurance Standards for Risk Analyst and the Risk Management Framework (RMF)

Risk Analyst Course Overview:

Information Assurance Associates (***IA2***) provides comprehensive CNSS-4016 Risk Analysis certification and the federal Risk Management Framework (RMF) training for Information System Security Managers (ISSM's), Certification Agents and Security Control Assessors (SCA's). The ***IA2*** Risk Analysis Certification 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 intense, 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.

Student Prerequisites:

Students should have an advanced understanding, practical knowledge and recent experience in enforcing federal or corporate requirements, applying risk methodologies and facilitating acquisition, program management or system accreditation activities. Students should also have extensive System Administrator, Information System Security Manager (ISSM) or System Certifier/Validator experience, and be very familiar with the risk relevant responsibilities associated with system Assessment and Authorization (A&A) processed. Completion of CNSS-4012 Senior System Manager and CNSS-4015 System Certifier training is highly recommended but not required.

Instructor Qualifications:

The ***IA2*** award winning instructor staff are certified as Fully Qualified Certification Agents and System Validators, Certified Information System Security Professionals (CISSPs), Certified Information Security Managers (CISMs), Certified in Risk and Information Systems Control (CRISC), and Certified in NSA Information System Security Assessment and Evaluation Methodologies (IAM/IEM). Additionally, each instructor is certified as a Master Training Specialist and has a minimum of fifteen years experience as a functional DOD, national Intelligence Community (IC) or federal Information System Security Manager. For IC applications, ***IA2*** instructor staff members have been certified as NSA Adjunct Faculty and as NSA Accreditation Action Officers (AAOs) and hold a security clearance for access to National Security System data.

References:

/ CNSS Instruction No. 4009. “National Information Assurance (IA) Glossary.” Dated 19 May 2003

/ NSTISS Directive No. 5-1. “National training Program for Information System Security (INFOSEC) Professionals.” Dated 16 November 1992

/ “The National Strategy to Secure Cyberspace, Priority III: A national Cyberspace Security Awareness and Training Program. “ dated February 2003

/ “Federal Information Security Management Act of 2002 (FISMA).” Contained under Title III of the “Electronic Government Act.” Dated December 17, 2002.

/ Risk Management Guide for DOD Acquisition, Sixth Edition, v.1.0, dated August 2006

- NSTISSI Instruction No. 4015, "National Information Assurance training Standards for Systems Certifiers," dated December 2000.
- CNSS Instruction No. 4012, "National Information Assurance Training Standards for Senior System Managers." Dated June 2004.
- CNSS Instruction No. 4016, "National Information Assurance training Standards for System Certifiers ," dated November 2005.
- NIST-800-53 Guide for Assessing the Security Controls within Federal Information Systems.
- NIST-800-39 Managing Information Security Risk
- NIST-800-30 Risk Management Guide for Information Technology Systems
- NIST-800-37 Guide for Applying RMF to Information Systems
- NIST-800-64 Security Considerations in the System Developmental Life-Cycle.
- DODI 8510.01 Risk Management Framework (RMF) for DoD Information Technology dated: March 12, 2014
- DODI 8500.01 Cybersecurity dated: March 14, 2014
- CNSSI 1253 Security Categorization and Control Selection for National Security Systems dated: October 2009

Risk Analyst Course Content

LESSON 1. Fundamentals of Threat/Vulnerability Analysis and Risk Management.

This lesson focuses on the fundamentals of threat analysis and vulnerability assessment as it relates to the Risk Management Framework (RMF) process. Special emphasis is placed on defining the characteristics of threats, the principals of Risk Management, the processes associated with Risk Analysis and Risk Assessment, and Risk Mitigation tactics and requirements. Specific topics include:

- Threat Evaluation.
- Vulnerability Analysis
- Risk Assessment Methodologies
- Risk Analysis Processes
- Risk Management
- Likelihood Determination
- Risk Mitigation Strategies

LESSON-2. Information System Controls and the System Development Life-Cycle (SDLC):

This lesson focuses on the identification of specific risk and system control categories and the determination of control strength as well as the need to ensure a cost-benefit Return-On-Investment (ROI). Additionally, this lesson focuses on Risk Management Framework (RMF) activities that are required and relevant within System Development Life-Cycle processes. Special emphasis is placed on identifying the stages of a system life-cycle and identify RMF responsibilities within each stage. Additional discussions include defining the processes necessary for assessing and mitigating risk during a system's life-cycle. Specific discussions focus on:

/ The control selection criteria, categories and strength;

/ Project and Risk Management processes including Scope Management; Time Management; Budget Management and Metrics Management;

/ Enterprise Risk Management and Enterprise Resource Planning.

/ Agency/Vendor Cooperation/Coordination in system acquisition.

/ Risk climate, risk goals and risk security requirements within a Trusted Domain

/ Risk Management Framework (RMF) issues, concerns, requirements and restrictions.

/ Defining risk goals specific to life-cycle security, life-cycle control, life-cycle management and System Development Life-Cycle.

/ Establishing risk confidences necessary to maintain an appropriate measure of CIA.

/ Risk Management roles, controls and responsibilities in Configuration Management and Configuration Control.

/ Risk Management Framework integration within System Development Life-Cycle.

LESSON-3 Risk Planning in Consequence Management and Protection Strategies:

This lesson discusses the requirements relevant to Consequence Management including Contingency Planning, Disaster Recovery and Incident Reporting. Specific focus is on assessing and mitigating risks during the design, development, implementation, operation, maintenance, and disposition phases of information systems life cycle. This lesson focuses on the following:

/ Identifying risk actions necessary to mitigate loss impact resulting from an incident or contingency action.

- Identifying, characterizing and assessing threats associated with Consequence Planning.
- Assessing the vulnerability of critical assets to specific threats relevant to Contingency Planning,
- Determining the risk (i.e. the *expected* consequences of specific types of attacks on specific assets).
- Identifying protection and preparatory measures to reduce risks associated with contingency actions.
- Prioritizing risk reduction measures based on a defined strategy in Disposition/Reutilization.
- System centric Risk Control Requirements including Administrative, Personal, Technical, Emanations and Cryptography actions to reduce risk.
- Consequence Management within the Risk Management Framework.

LESSON-4. Risk Monitoring and Countermeasure Identification, Implementation and Assessment

This lesson focuses on the principal of risk ownership, common risk and continuous risk monitoring practices, processes and procedures as well as RMF compliance reporting requirements. Specific emphasis is placed on risk assessment methodologies and the concept of Key Risk Indicators and Key Performance Indicators. Additionally, this lesson focuses on the identification, implementation and assessment of appropriate, cost-effective countermeasures within the RMF. Specific focus is placed on determining appropriate controls that are consistent with organizational RMF requirements; identifying the processes associated with analyzing and determining countermeasures; and managing, measuring and implementing countermeasures. Specific focus is placed on:

- RMF monitoring essentials, techniques and control implementation
- Risk monitoring and management including threat analysis
- Capability Maturity Modeling
- Control categories, features and requirements.
- Analyze and Determine Potential Countermeasures
- Identifying Potential Countermeasures
- Determining Cost-Benefit Analysis of Countermeasures
- Countermeasure control categories
- Access control requirements (physical, system and data)
- Access control features
- Identity Risk Management
- Role-Based/Rule-Based ACLs.

/ Reference Validation Mechanism (Reference Monitor)

/ Critical Infrastructure Protect

/ Defense–in-Depth

LESSON-5. Risk Identification Assessment and Evaluation.

This lesson focuses on risk identification, assessment and evaluation processes and protocols that help to determining the risk exposure within an organization and define a risk mitigation strategy to effectively mitigate risks to an acceptable level. Discussions will focus on risk scenario processes and determining risk factors and the concept of risk factor analysis as well as risk assessment methods and methodologies. Additionally, this lesson focuses on RMF Secure Configuration Management and the impact Configuration Control and Configuration Management has on maintaining a predictable and risk centric operational environment. Specific discussions focus on:

/ The risk process including risk identification, determination, and management strategies;

/ Risk based organizational impact analysis in consequence and configuration management;

/ The RMF climate, including internal and external risk factor analysis;

/ Risk prioritization, including establishing mission risk impact analysis strategies; and risk issues and concerns

/ Threat/Risk Assessment

/ Secure Configuration Management that includes operability, interoperability, functionality, predictability, stability and improved survivability within the Risk Management Framework.

LESSON-6. Synthesis of Risks and Analysis:

This lesson focuses on synthesizing the results of Cybersecurity efforts taken to protect an information system and secure the information processed. The central focus is to create a relevant, sufficient, and comprehensible synthesis of paired-threat/vulnerability, countermeasure, and mission impact information in a context to support decision makers. Specific topics include:

/ Synthesis of Components and Overall Risks

/ Analyzing Vulnerabilities and Attack Avenues

/ Risk Aspects of Security

/ Risk Management Framework Assessment Methodology

/ Association of Threat Probabilities to Vulnerability

/ Conducting Risk Analysis

/ Countermeasure Analysis
/ Detailed Residual Risk
/ The Effect of Countermeasures on Risk
/ Effective Risk Mitigation
/ Risk Assessment (Environment & Threat Description)
/ Risk Management Methodology

LESSON-7. Risk Assessment, Testing and Evaluation:

This lesson focuses on the identification, analysis, assessment and evaluation of risks through a structured testing and evaluation assessment process. Special focus is placed identifying potential sources of threat that may adversely impact an information system and its associated resources in terms of mission objectives and risk tolerance and appetite. Discussion topics include:

/ The Identification, Analysis Assessment and Evaluation of Risks Through a Structured Risk Management Framework Methodology
/ The Identification of Threat, Vulnerability and Associated Risk Source.
/ Determining Individual Assessment, Test and Evaluation Requirements, Roles and Responsibilities
/ Defining and Designing Assessment Policies, Plans, Procedures and Protocols
/ Determining Threats and Vulnerabilities Through a Structured Test and Evaluation Assessment Process
/ Assessment Viewpoints and Categories
/ Test and Evaluation Customization, Logistics, Resource Requirements, Execution, Coordination and Mitigation Actions
/ Post-Test Analysis, Assessment and Reporting

LESSON 8. Threat and Adversary Analysis:

This lesson focuses on the analysis and assessment of risks as well as the nature and degree of system risks. This includes methods used to assess potential threats to information systems in terms of mission adversaries, their impact on a system, their motivation, and their ability to effect harm. Specific emphasis is placed on:

/ Conducting Risk Analysis and Cost/Benefit Analysis
/ Risk Management Framework Threat Assessment Methodology
/ Threat Analysis, Treat Description and Threat/Risk Assessment
/ Vulnerability Analysis and Assessment Methodology
/ Risk Assessment Methodology
/ Computing Loss Expectancy Based on Asset Valuation

/ Incident Identification, Analysis and Assessment

/ Incident Response, Recovery and Reporting Requirements

LESSON 9. Federal Risk Management Framework (RMF):

This lesson focuses on Risk Management process that incorporates a cybersecuirity, risk centric focus on the Assessment and Authorization (A&A) to facilitate a more dynamic approach that provides the capability to more effectively mange information system-related security risks in a highly diverse environment of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. Specifically, this lesson addresses:

/ RMF processes, procedures and protocols specific to system Security Categorization, Security Control Selection, Security Control Implementation, Security Control Assessment, Security Authorization and Continuous Monitoring.

/ RMF governance including policy alignment and transformation initiatives.

/ RMF emphasis and characteristics specific to the Assessment and Authorization process.

/ RMF hierarchy and processes necessary to make cost-effective, risk-based decisions within organizational information systems.

/ RMF processes at the information system level and Risk Management processes at the organizational level through the Risk Executive function.

/ RMF transition and transformation goals and requirements

LESSON 10. Mission and Assets Risk Management:

This lesson addresses the assessment of mission assets as well as determining role and criticality of information systems to an organization overall mission. Specific focus is placed on how an information system supports a given mission and how a given information system's degradation impacts that mission. Specific discussions include:

/ Conducting RMF centric Risk Analysis

/ Cost-Benefit Analysis, ROI, Critical Thinking, Benchmarking and Deductive Reasoning

/ Organizational Risk and Asset Management

/ Requirement for continuous Risk Management and Associated Processes

/ System, Application and Technology Provided Risk Mitigation

/ Networking and Computing Environment Risk Factor Analysis

/ Risk Identification, Determination and Evaluation Techniques

/ Risk Response Planning

LESSON 11. Vulnerabilities and Attack Avenues Analysis:

This lesson focuses on evaluation processes necessary to reveal system weaknesses and associated adversary techniques. Specific focus is on identification and evaluation of information system weaknesses with respect to their cost (resource/jeopardy to themselves) to exploit, an attacker's objectives, access requirements, jeopardy incurred, and the impact on an organization's mission. Specific focus is placed on:

- Vulnerabilities, attacks, threats, and consequences
- Effect of Countermeasures on Residual Risk
- Effects of Mitigation
- Hostile Intelligence Sources
- Risk Variables
- Risk Assessment and Risk Management Framework Methodology
- Threat and Vulnerability Analysis Within an Operational Framework
- Adversaries and Avenues of Attack

LESSON 12. Risk Training, Policies and Legal Issues:

This lesson focuses on the requirement to facilitate risk centric training; education and awareness to ensure threats, vulnerabilities and the associated risks are identified, analyzed, assessed, managed and mitigated in a timely manner. Specific discussions center on:

- Access Control Policies and Associated Laws, Regulations, and Other Public Policy
- Agency-Specific IA and IT Policies and Procedures
- Assessment Methodology
- Communications Security Policy and Guidance
- Knowledge and/or Awareness of Security Laws
- Methods of Defining Security Requirements
- Risk Acceptance Process
- Risk Management Methodology
- Security Awareness
- Ethics

Student Progress Check:

Student comprehension will be measured by administering a cumulative and very comprehensive 50-question progress check that is administered at the end of the last day of training. Satisfactory completion and remedial requirements will be consistent with each customer training standards.