CNSS 4015: Certification Agent

Length: 5 Day

COURSE CONTENT

1. DOCUMENTING THE MISSION NEEDS

- Coordination with Related Disciplines – This involves identifying related disciplines required for accomplishing IS certification; and discussing the relationship between mission-specific disciplines and IS requirements.
- Establishing Roles and Responsibilities: This includes outlining current roles and responsibilities of personnel assigned access to the systems being certified; and recommending changes to include additions for improving the roles and responsibilities and accountability for personnel with various levels of access to the information systems being certified.
- Methods Used to Promote Effective Oral and Written Communications: This involves the use of appropriate terms and expressions when trying to establish effective communications. Promoting the understanding that many words have multiple meanings and how to prevent misunderstanding.
- How to Effectively Negotiate and Define the Requisite A&A Processes: This includes methods used to clearly define certification requirements and accreditation boundaries; techniques that help describe more complex and time- consuming A&A requirements such as threat analysis, vulnerability assessment, the risk management process and the need to define appropriate mitigation strategies; as well as the need to effectively outline applicable Public Laws, national statutes and service directives that regulate specific critical A&A processes.
- Understanding the Mission – This involves identifying mission critical elements, to include system mission, functions, and requisite interfaces; methods used to ensure that mission critical elements are completely identified

2. CONDUCTING REGISTRATION

- System Certification Memorandum of Understanding (MOU), Memorandum of Agreement, Inter-service Support Agreement (ISSA) or Other Instruments. This includes identifying the purpose, scope and content; the parties involved, coordination challenges, responsibilities and agreement requirements; and use of these instruments within requisite A&A documents.
- Compiling and Defining Security Requirements. This includes describing the security requirement collection process; researching security requirements; and describing and defining appropriate system security requirements.
- Audit Collection, Evaluation, Retention and Reporting Requirements. This includes describing audit collection requirements relative to system certification and assisting in the identification of audit requirements.

- Coordination Requirements with Related Disciplines. This involves identifying the role of related security disciplines in the overall process of protecting information infrastructures; relating how these security disciplines apply to system certification process; and defining related security disciplines that may be needed to facilitate certification.
- Defining and Evaluating System Security Policy and Information System Security Strategy Requirements: This includes outlining the requirement for non-technical assessment of requisite security support documentation; conducting a comprehensive analysis and assessment of requisite policies, processes, procedures and protocols; evaluating compliance with relevant instructions, regulations, directives and guidelines; and defining and establishing critical resource requirements (fiscal, management, logistic, etc) to ensure effective system security administration.
- Describing the System Operating Environment: This includes conducting an evaluation of the physical environment and assessment of available security features based on the threat continuum; an evaluation of requisite administrative policies and technical procedures necessary to counter the identified risks; identification of requisite environmental, safety, training, and maintenance necessary to support operations.
- Information Security Policy Relevance to Systems Development: This involves identification of applicable security policies and procedures, and evaluating system security policies and procedures as they relate to secure system operation.
- Establishing the Requirement for Confidentiality, Integrity and Availability (CIA) within and Information Infrastructure: This includes verifying and validating the requirements for confidentiality, integrity, and availability as outlined within A&A documents. Additionally, this lesson focuses on evaluating network architectures to ensure that mechanism are available to enforce the CIA requirement and support the security policies outlined in the Security Concept of Operations.
- Evaluating Administrative Security Policies and Procedures: This includes identification and evaluation of pertinent security policies and procedures that address technical and non-technical security issues.
- Documenting and Maintaining Security Policies, Processes, Procedures and Protocols: This includes evaluating existing documents to ensure they are properly maintained, current, applicable, and appropriate to current system operations.

3. MEASURING, MANAGING AND MITIGATING INFORMATION SYSTEM THREATS, VULNERABILITIES AND ASSOCIATED RISKS.

- Threat, Vulnerability and Risk Analysis, Assessment and Management: This focuses on identifying threat and vulnerabilities inherent within an information system and methods available to analyze, assess and manage associated risks.
- Establishing a Risk Management Framework (RMF) Process: This includes defining the concept of threat and establishing the threat relationship to a vulnerability, establishing the appropriate risk analysis, assessment and management processes and defining the appropriate risk evaluation methodologies (quantitative, qualitative, active, passive, objective, subjective, ordinal, etc.). Outlining countermeasure options and specific requirements and providing measurement techniques for evaluating and expressing residual risk.
- Conducting an Environment and Threat Description Analysis: This includes a comprehensive review of the overall system operating environment and the associated threat continuum, an analysis of corresponding vulnerabilities and a clear description of the evaluated residual risks.
- Defining Threat, Vulnerability and Evaluating Risk Assessment Results: This includes establishing a process to validate threats and corresponding vulnerabilities identified by system owners; relating the resulting risks to protecting the sensitivity, veracity and accessibility of data processed; evaluating security control results to show technical and non-technical vulnerabilities that may increase the risk threshold; and analyzing threats posed by internal and external, intentional and unintentional threats.

4. LEGAL ISSUES CONCERNS, REQUIREMENTS AND RESTRICTIONS.

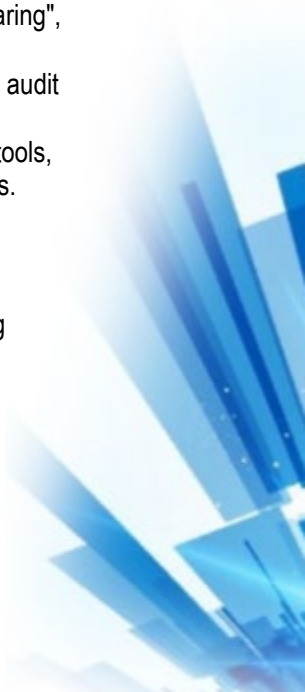
- INFOSEC Security Laws, Statutes and Legal Issues – This involves identifying, interpreting and relating relevant nation-state security laws, treaties, and/or agreements to mission needs requirements and mission accomplishment; and discussing how they can influence the certification process.
- Understanding Information System Security Laws. This includes explaining the applicability of laws, statutes, and regulations; describing how systems will operate according to legal mandates; and identifying the organizational point of contact for legal advice.

5. INTRUSION PREVENTION, DETECTION, RESPONSE, RECOVERY AND REPORTING.

- Defining Incident Prevention Processes. This includes establishing the need to facilitate incident identification methodologies and implement specific activities necessary to restore essential system services and regain control with a central focus on containing the incident, eradicating the incident, and recovering from the incident.
- Defining and Evaluating Reporting Requirements. This includes an analysis of internal and external reporting standards, guidelines, and requirements as well as defining organizational reporting processes. Additional emphasis is placed on incident analysis, evaluation, reporting, response and recovery procedures and defined reporting, requirements.

6. PHYSICAL, SYSTEM AND DATA ACCESS CONTROL.

- The Review of System Access Controls: This includes evaluating access control requirements and policies based on the classification of the data processed; the need to enforce individual access to specific data elements consistent with established need-to-know thresholds; the requirement to ensure that specific access controls are easily maintained, have a minimum impact on throughput and are transparent to users.
- Access Control Policies, Processes, Procedures and Protocols: This involves defining access controls based on the sensitivity of data processes; evaluating access controls within the trusted computing base; identify deficiencies within the information system security architecture; and identifying and recommending changes, enhancements or modifications.
- Identifying Physical, System and Data Access Control Requirements: This includes defining protection measures based on subject to object access requests and requirements. Special emphasis is placed on defining privileged access requirements, restrictions and responsibilities; identifying system access controls based on user identifiers including Identity Management methods; and data access privileges based on specific rules, individual user roles or data content based on mandatory or discretionary access control requirements. Additionally, this lesson addresses ownership responsibilities as they relate to the philosophy of “least-privilege”, “need-to-know”, “need-to-share” and “need- to-access” and "assured information sharing", as well as establishing and enforcing access control policies.
- System, Network and User Audit Control Requirements and Restrictions: This includes defining specific audit requirements; enabling specific audit events, reviewing and analyzing audit reports, and controlling and protecting audit records; determining intrusion detection methodologies including selecting appropriate tools, implementing signature updates, establishing enforcement methods and responding to specific incidents.
- Determining Audit Requirements: This includes identifying audit events, determining audit review requirements, documenting audit results, and determining reporting requirements.
- Determining Intrusion Detection System (IDS) Requirements and Restrictions: This includes identifying required IDS capabilities, defining IDS active and passive processes, documenting findings and defining reporting requirements.



7. LIFE-CYCLE SECURITY AND MANAGEMENT

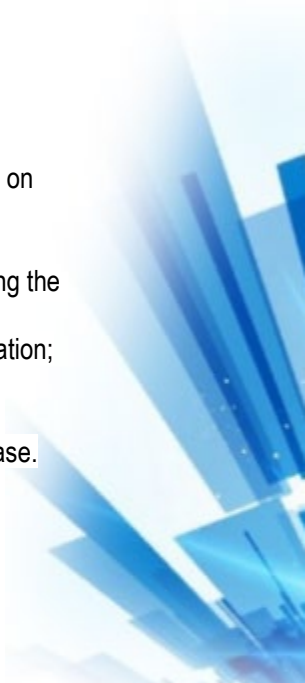
- Life-Cycle System Security Planning within System Development: This includes conducting evaluations centered on life-cycle security, life-cycle planning and managing life-cycle processes within a systems design, development and deployment.
- Life-Cycle Security and Life-Cycle Management: This includes evaluating the relationship between Life-Cycle Security and Life-Cycle Management with special focus on planning, control and implementing requirements based on established directives and guidelines; defining strategies and methodologies that help support Life-Cycle Security and life-cycle management processes; and planning and enforcement actions that help ensure security controls and management actions are implemented throughout a systems operational life- cycle.
- Life-Cycle Integration: This includes facilitating evaluation that is focused on integrating and implementing life-cycle processes and procedures within a trusted domain and how these processes and procedures help to support mission accomplishment and system predictability within an operational environment.

8. DEFENDING THE INFORMATION ENVIRONMENT (INFORMATION OPERATIONS)

- Discussions Regarding System Development, Integration, and Maintenance Environment: This includes outlining system development approach in conducting certification of systems within a deployed environment; describing access and configuration controls inherent within the system; and determining system integration, development, deployment, continuity and maintenance requirements.
- Security Engineering Principals, Practices, Requirements and Restrictions: This includes identifying security engineering requirements for developers and maintainers; establishing security-engineering principals within the A&A process; defining security-engineering practices and principals that are governed by national statute or information security policy; and engineering practices defined in the National Information Assurance Partnership (NIAP) process.
- Requirements for Applications Level Security: This includes evaluating the effectiveness of applications security mechanisms and their interactions with other systems and networks; identifying security differences between operating systems and applications; and establishing security test and evaluation plans and procedures to test security countermeasures inherent within operating systems and application software.
- Defining Maintenance Procedures that are Consistent with the Classification and Sensitivity of Data Processed: This includes determining security requirements for system maintainers and defining requirements to ensure that systems are upgraded and maintained to ensure compliance with established security technical integration requirements.
- Operating System Evaluation, Assessment and Security: This lesson focuses on methods designed to assess operating system configuration, security functionality and architecture. Additional emphasis includes response and recovery conditions; security test and evaluation processes, procedures and protocols; configuration management and control; and operating system protection analysis techniques.

9. MALICIOUS LOGIC - PREVENTION, DETECTION, REACTION, RECOVERY AND REPORTING

- Physical, System and Data Labeling: This includes verifying and validating labeling requirements based on data sensitivity levels. Additional focus is placed on controlling information storage media to determine handling requirements based on content.
- Manage, Control and Protect Against the Introduction of Malicious/ Mobile Code: This includes evaluating the use and available of tools to test the system capabilities in order to identify residual risk; verifying that appropriate capabilities are resident in the system to mitigate risk from malicious/mobile code contamination; and documenting the results of testing to support the system residual risk analysis.
- Special Security Controls Required for Mobile Code: This includes evaluation methodologies used to determine the scope and threats posed by permitting specific mobile code within a trusted computing base.



- The Technical and Non-Technical Impact of Malicious Logic: This includes evaluating internal processes, procedures and protocols on prevention, detection, correction and reporting techniques relevant to malicious software.
- Methods and Control Procedures for System Components: This includes the analysis of requisite control, disposition and disposal procedures required for specific hardware, software, memory components and recordable information storage media.

10. SECURE CONFIGURATION MANAGEMENT, COOP, CONTINGENCY AND DISASTER RECOVERY PLANNING.

- Contingency Planning – This focuses on assessing the need and requirement for contingency planning within specific operational environments; identifying and confirming critical contingency elements and IS requirements within the contingency process as they relate to mission need elements and mission accomplishment; and defines specific requirements to ensure requisite system recovery processes are clearly defined to ensure certification.
- Configuration Control Policies, Processes, Procedures and Protocols. This includes providing advice and guidance in developing and accessing system configuration control policies and reporting deficiencies and discrepancies within the configuration control policy.
- Contingency and Consequence Management (CM) Planning. This includes assessing the need for contingency and CM planning; defining contingency and CM planning activities; defining contingency and CM planning processes; assessing and reporting contingency and CM discrepancies.
- Contingency Action, Incident Response, Reporting and Recovery and Disaster Planning: This includes establishing methods necessary for contingency and consequence management; incident and disaster recovery processes; life-cycle management and security requirements; Continuity of Operations Planning (COOP); disaster recovery and reporting.
- Outlining and Defining Incident Prevention Processes and Establishing Incident Identification Methodologies: This includes evaluating specific activities necessary to restore essential system services and regain control. Special focus is on methods and requirements to contain the incident, eradicate the incident and recover from the incident; as well as a comprehensive review of internal and external reporting standards, guidelines, and requirements necessary to facilitate organizational reporting processes including incident analysis, evaluation, reporting, response and recovery procedures.
- Secure Configuration Management and Control Initiatives: This includes the evaluation of methods necessary to ensure changes, modifications or enhancements to a trusted computing base are conducted in a controlled and regulated manner. Additionally, special emphasis is placed on configuration reporting and configuration auditing as well as verification and validation (e.g. content auditing) processes used to ensure security controls have not been adversely influenced by an incorporated change.
- Identify Contingency and Continuity of Operations Planning Requirements/Testing Based on Mission Criticality: This includes determining contingency requirements and documenting restoration, recovery and reporting requirements.
- Life-Cycle Security and Configuration Control and Management: This includes documenting technical and non-technical changes to the system and documenting these changes, determining if the changes are significant enough to warrant reaccreditation as well as ensuring that configuration controls are in place to ensure proper management of system resources and proposed changes are properly staffed and tested.

11. NETWORK SECURITY AND CERTIFICATION EVALUATION.

- Processes and Procedures for Conducting a Network Security Evaluation: This includes identifying the existing network topology and connection requirements; evaluating the established security requirements for interconnecting with other systems and networks; validating network approval processes and determining if additional security controls are required; and conducting security tests to ensure secure network operations.

- Establishing Parameters and Restrictions within the Certification Process: This involves defining conditions, behaviors and standards that are critical in establishing parameters within the certification process. Special emphasis is placed on outlining precise rules of engagement that focus on ensuring mission accomplishment and accomplishing certification tasks.

12. INFORMATION SYSTEM AND NETWORK SECURITY ASSESSMENT AND AUTHORIZATION (A&A) ANALYSIS PROCESSES ASSOCIATED WITH THE NEW RISK MANAGEMENT FRAMEWORK. SPECIFIC TOPICS COVER:

- Methods, Principals and Practices of Information Security: This focuses defining and designing procedures and protocols that will aide in the assessment and authorization process. This includes identifying and defining manual and automated evaluation tools that evaluate information security within multiple environments.
- Conducting a Non-Technical Assessment of Information Security Documentation: This includes identifying and evaluating existing security documentation, determining the adequacy of existing documentation; and identifying deficiencies in system documentation.
- Assessment Team Concepts and Certification Process: This includes discussions centering around the appropriate team composition, defining special skill-sets, outlining technical and non-technical knowledge requirements, establishing individual roles and responsibilities and defining requisite professional certifications required for individual Assessment Team members. Defining the required scope for specific certification tasks, establishing boundaries and rules of engagement, and formulating plans of action and with specific milestones necessary to successfully complete the system certification process.
- The Evaluation of Security Policies, Processes and Procedures: This involves defining and evaluating specific policies and procedures that are critical to the A&A process; correlating the absence of specific policies or procedures that may increase the inherent risk associated with operating the system; establishing the need to publish specific policies and procedures that influence security or system operability and interoperability as well as the integration of policies and procedures to preserve data integrity that is critical to the security testing processes; establishing a relationship between specific policies, procedures and requirements to the A&A process and the accreditation decision.
- Review Documentation and the Origin of specific requirements applicable to the A&A Process: This involves identify documents and ensure compliance with the constructed A&A documents; determining assessment standards based on established technical and non-technical requirements; defining security requirements within a security control matrix that are unique to the system undergoing the A&A process; interpreting special security requirements based on the system composition, architecture, data processed, or mission; and designing a security assessment strategy that includes verification of technical assessment requirements, validation of requisite non-technical support documentation, and authentication of testing results to support a system authorization decision.
- Evaluation of System Architecture Including Defense-in-Depth (DiD): This includes establishing and evaluating the defined accreditation boundary; evaluating and analyzing the system architecture drawings to ensure that all components (e.g. HW/SW/FW) are properly employed to establish a DiD configuration; verifying and validating internal and external interfaces; and identifying system collateral components that are subject to the A&A process.
- Coordinating and Identifying Collateral Resources to Facilitate the A&A Process: This involves convening a team of responsible professionals with a broad experience base to work together towards system accreditation; and identifying resources and defining individual responsibilities to effectively and efficiently satisfy the A&A process.