CNSS 4012: Information System Security Manager

Length: 5 Days

COURSE CONTENT

1. **INFORMATION SYSTEM SECURITY FUNCTIONS AND MANAGEMENT RESPONSIBILITIES.**

- The unique responsibilities and special obligations associated with Information System Security (ISS) management;
- The concept of centralized authority to facilitate daily information system controls and decentralized management to ensure a high state of organizational information security awareness, sensitivity and readiness.
- The need to establish an Information System Security Awareness Training and Education (SATE) program by;
- The need to ensure and preserve individual privacy issues and concerns including;
- A review of organizational obligations including the concept of due- care, best business/security practice, and reasonable and customary.

2. **INFORMATION ASSURANCE PROGRAM IMPLEMENTATION.**

- Establishing an Information Assurance Policy, creating a positive ISS climate, defining and establishing ISS goals, controlling and securing network interoperability and system interdependencies;
- Defining the Information Assurance Technical Framework (IATF) and Information Assurance Program elements and requirements;
- Evaluating protection requirements and determining information Mission Assurance Categories (MAC), Security Levels of Concern (LOC) and robustness
- Understanding the unique challenges and security requirements for sharing operationally critical data and protecting essential information infrastructures in a Network-Centric environment;
- Defining and establishing Information Assurance Protection Measures

3. **THREAT AND VULNERABILITY IDENTIFICATION; RISK ANALYSIS, RESPONSE AND RECOVERY.**

- The concept of threat analysis as well as the potential impact of common technical and non-technical (administrative) vulnerabilities and their corresponding relationship with identified threats;
- Countermeasure analysis that outlines ways to integrate reasonable, cost-effective controls necessary to mitigate the threat/vulnerability risk potential to an acceptable level;
- Risk assessment discussions that center on the resulting impact or harm to an organizations efficiency, functionality, reputation and mission;
- Special risk analysis, risk assessment, and risk management techniques as well as risk calculation and measurement methods;
- Individual actions and activities that facilitate the identification control, measurement and mitigation of individual risk factors to satisfy Information System Security certification and accreditation.

4. LEGAL STATUTES, ISSUES, AND INTRUSION FORENSICS.

- The concept and fundamental differences between Information System, Threat and COMSEC Monitoring including;
- The science of Intrusion Forensics including discussions that center on the process of investigating incidents, retrieving data, and then protecting the information (rules of evidence) in a manner that will make it admissible in a legal proceeding;
- Incident analysis, initial response, regaining control and restoring essential information services;
- Information Assurance and Information System Security laws and statutes as well as national and federal information protect standards, regulations, guidelines and directives

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

- Identify specific recovery activities necessary to restore essential system services.
- Establishing incident analysis, evaluation, reporting, response and recovery procedures.
- Defining reporting, requirements, structure and levels;
- Identifying the differences between incidents, events, and violations;
- Creating reporting guidelines, methods, categories and timelines;
- Formulating organizational specific incident report format, follow-up actions and procedures.

6. PHYSICAL, SYSTEM AND DATA ACCESS CONTROL

- Determining the best, most cost effective, least intrusive, and least disruptive types of access controls necessary to satisfy specific organizational security concerns
- Establishing rule based, role based or content based access controls that facilitate data access requirements and accommodate data access controls that are consistent with the established Trusted Computer
- Establishing protective, detective and corrective access restrictions that facilitate physical, technical and administrative control measures including defining organizational requirements

7. DATA ENCRYPTION (CRYPTOLOGY).

- The purpose, the different types and the various applications of Data Encryption Standards (DES) including the unique security concerns associated with data encryption
- An overview of Digital Signatures characteristics, issues, concerns and requirements
- A basic overview of the Public Key Infrastructure (PKI) concept that includes a review of critical components, digital certificates and essential processes

8. DEFENDING THE INFORMATION ENVIRONMENT.

- Specific discussions that revolve around the IO role in achieving information superiority and the impact on operations
- Procedures and protocols associated with Information Conditions (INFOCON's)
- Information Assurance Vulnerability Management (IAVM) reporting and compliance standards
- Establishing an organizational OPSEC policy, evaluating effectiveness and defining management goals

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

- The technical and non-technical impact malicious logic has on an organization and internal measures necessary
- Methods and control procedures required to ensure the secure and proper disposition of hardware, software, memory components and recordable information storage media.

10. CONFIGURATION MANAGEMENT, CONTINUITY OF OPERATIONS PLANNING (COOP), AND DISASTER RECOVERY.

- The business need to establish a plan of action for contingency situations.
- Defining and developing a comprehensive Consequence Management Plan, Disaster Recovery Plan and Continuity of Operations Plan (COOP).

11. AN INTRODUCTION TO PENETRATION TESTING (PENTEST).

- Establishing information gathering techniques including outlining critical planning, discovery, attack and reporting methodologies
- Defining goals and establishing requisite "Rules of Engagement"
- Implementing the "Red Team" – "Blue Team" concept of PENTESTING
- Defining specific limitations, discussing precise protocols and establishing and defining individual responsibilities and restrictions.

12. INFORMATION SYSTEM AND NETWORK SECURITY CERTIFICATION AND ACCREDITATION (C&A).

- Special emphasis is placed on the DITSCAP, DCID and NISCAP concept of certification and accreditation including:
- The format and content of the DITSCAP System Security Authorization Agreement (SSAA) including a comprehensive overview of the SSAA structure
- The format, structure and content of the DCID and NISCAP System Security Plan (SSP)