IA2 **Information Assurance Associates, Inc.**

Information System Security Manager (ISSM)/Information Assurance Manager (IAM) Training (Satisfying CNSS 4012 standards)

ISSM/IAM Course Overview:

Information Assurance Associates (***IA2***) provides comprehensive certification training for Information System Security Managers (ISSMs) and Information Assurance Managers (IAMs) that is compliant with knowledge factors required by the Committee on National Security Systems (CNSS), which operates under the National Security Agency (NSA). The course curriculum was specifically designed for ISSMs and IAMs that exercise security control over Department of Defense (DOD), Combatant Command, Service or Agency (CC/S/A) and federal critical information infrastructures. The ISSM/IAM course provides one week of intense, highly concentrated, non-technical professional training necessary to achieve the fundamental knowledge, skills, and abilities needed to define, design, integrate, and manage information system security policies, processes, practices, and procedures within DoD, CC/S/A, and federally controlled information systems and networks. This course addresses knowledge factors and functional requirements established for Level I and Level II Technical and Management Information Assurance (IA) Workforce training. Specific focus is directed on identifying, implementing and integrating management and administrative solutions for securing critical information infrastructures and establishing standards necessary to help protect the confidentiality, maintain the integrity and ensure the availability of sensitive data and critical organizational computing resources. The ***IA2*** ISSM/IAM course provides comprehensive training in establishing organizational Information System Security (ISS) policies, developing internal ISS processes, outlining critical ISS procedures, and implementing specially tailored ISS protocols. The focus of this course is to ensure effective security management of DOD, CC/S/A, and federal information infrastructures that process sensitive, classified or national intelligence data.

Instructor Qualifications:

The ***IA2*** award winning instructor staff are all Certified Information System Security Professionals (CISSPs), Certified Information Security Managers (CISMs), Certified in NSA Information System Security Assessment and Evaluation Methodologies (IAM/IEM), and Master Training Specialists. Additionally, each instructor 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 SI/SCI data.

References:

- Director Central Intelligence Directive (DCID) 6/3 – Protecting Sensitive Compartmented Information Within Information Systems.
- DoD Directive 8500.1, "Information Assurance" October 24, 2002.
- DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003
- Joint DODIIS Cryptologic SCI Information System Security Standards (JDCSISSS) Rev 3, June 2003
- DoD Directive 8570.1-M (Draft), DoD IA Training, Certification and Workforce Management. December 17, 2003
- DoD Directive 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual, July 2000.
- DoDD 8320.2 Data Sharing in a Net-Centric DoD, 2 December 2004
- DODI 5200.40 DOD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997.
- DoD 5200.2-R "Personnel Security Program," January 1987
- CJCSI 6510.01b "Defensive Implementation Operations" Aug 1997
- CJCSM 6510.01 "Defense-in-Depth: Information Assurance and Computer Network Defense (CND)" December 2002
- Public Law 100-235 Computer Security Act of 1987
- OMB Circular A130
- FIPS 4012/4014
- CNSS No. 4009
- Various Combatant Command, Service and Agency Directives

ISSM/IAM Course Content

Information System Security Functions and Management Responsibilities.

This lesson focuses on the security management and administration of information systems processing sensitive, classified and cryptologic information. This lesson outlines individual roles, responsibilities, obligations, and liabilities. Special emphasis is placed in the following areas:

- 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;
  - ✓ Defining training methodologies and establishing training requirements;
  - ✓ Defining the process to develop terminal and enabling objectives, establish organizational training program focus and promote individual program goals;
  - ✓ Discussing the Instructional Systems Design program standards for curriculum development as well as establishing education, evaluation and remediation goals.
- The need to ensure and preserve individual privacy issues and concerns including;
  - ✓ Individual expectation of privacy;
  - ✓ Liability issues and concerns.
- A review of organizational obligations including the concept of due-care, best business/security practice, and reasonable and customary.

Information Assurance Program Implementation.

This lesson focuses on the unique security concerns associated with today's multi-protocol, multi-topology, multi-platform, fully distributed computing environments. Discussions center on:

- 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 including;
  - ✓ Integrating appropriate administrative controls;
  - ✓ Establishing internal Information Assurance policies, standards, baselines and guidelines;
  - ✓ Defining personnel, physical, biometric and technical controls;
  - ✓ Integrating software, firmware, COMSEC and TEMPEST controls.

Threat and Vulnerability Identification; Risk Analysis, Response and Recovery.

This lesson focuses on the identification, analysis, assessment and evaluation of individual threats and vulnerabilities and their impact on an organization's critical information infrastructures. Specific discussions focus on:

- 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.

Legal Statutes, Issues, and Intrusion Forensics.

This lesson discusses Public Laws, National Statutes, and Federal directives that address compliance requirements and individual privacy issues. Special focus is placed on:

- The concept and fundamental differences between Information System, Threat and COMSEC Monitoring including;
  - ✓ Special emphasis is placed on the control and protection of "Incidental Information";
  - ✓ The restrictions associated with e-mail content monitoring;
  - ✓ The COMSEC monitoring implications within system auditing;
  - ✓ Federal as well as CC/S/A COMSEC standards (e.g. NTISSD-600)
  - ✓ Intelligence Oversight with regards to computer applications.
- 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 including;
  - ✓ PL 100-235 (Computer Security Act);
  - ✓ PL 99-474 (Computer Fraud and Abuse Act);
  - ✓ PL 94-553 (Copyright Act);
  - ✓ PL 99-508 (ECPA);
  - ✓ PL 93-579 (Privacy Act);
  - ✓ PL 107-56 (The Patriots Act);
  - ✓ PL 107-347 (E-Government Act);
  - ✓ PL 104-231 (FOIA);
  - ✓ E.O. 12333
  - ✓ E.O. 12958
  - ✓ OMB Circular A-130;
  - ✓ NTISSD-600;
  - ✓ FIPS/NSTISSI/NIST Publications and;

- ✓ DOD, Joint and CC/S/A Directives, Instructions, Regulations and Guidelines.

Intrusion Prevention, Detection, Response, Recovery, and Reporting.

This lesson provides a comprehensive review of internal and external incident response and recovery standards, guidelines, and requirements as well as defining organizational reporting processes. This also includes;

- Establish an appropriate and timely incident response protocol.
- 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.

Physical, System and Data Access Control.

This lesson focuses on issues, concerns and requirements that determine the administration and management of physical, system and data access controls based on the sensitivity of the data processed and the corresponding authorization requirements of individual users. Discussions center on:

- Determining the best, most cost effective, least intrusive, and least disruptive types of access controls necessary to satisfy specific organizational security concerns, specifically;
  - ✓ Identifying and determining physical access control methods, requirements, and procedures;
  - ✓ Defining system access control requirements including identification and authentication methods and requisite management controls.
  - ✓ Implementing biometric controls including establishing characteristics as well as identifying complications and 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

Security Evaluation Criteria (TCSEC), the DCID Protection Level (PL) standards and the International Common Criteria (CC) Evaluation Assurance Level (EAL) framework for expressing information security;

- Establishing protective, detective and corrective access restrictions that facilitate physical, technical and administrative control measures including defining organizational requirements specific to;
  - ✓ Network Intrusion Detection Systems;
  - ✓ System and Network Auditing;
  - ✓ Network firewalls.
  - ✓ Trusted Domains and Trusted Computing Baselines.

Data Encryption (Cryptology).

This lesson provides an overview of the basic concept of data encryption including the integration and application of encryption philosophies and standards as well as the history and application of encryption methodologies including:

- The purpose, the different types and the various applications of Data Encryption Standards (DES) including the unique security concerns associated with data encryption;
  - ✓ Symmetric and asymmetric key streams
  - ✓ Public and private cryptology.
  - ✓ The RSA algorithm.
- An overview of Digital Signatures characteristics, issues, concerns and requirements including;
  - ✓ Key management;
  - ✓ Key generation;
  - ✓ Key distribution;
  - ✓ Key installation and;
  - ✓ Key storage, recover, change and disposal.
- A basic overview of the Public Key Infrastructure (PKI) concept that includes a review of critical components, digital certificates and essential processes including;
  - ✓ Certification Authority, Registration Authority and Local Registration Authority requirements and responsibilities;
  - ✓ Identification of PKI enabled system components and services;

Defending the Information Environment.

This lesson provides a comprehensive review of Information Operations (IO) including Information Assurance, Information Warfare and Special Information Operations including:

- Specific discussions that revolve around the IO role in achieving information superiority and the impact on operations including;
  - ✓ The Defense-in-Depth concept;
  - ✓ The philosophy of Network Centric Warfare and;
  - ✓ The Virtual Battle Space concept.
- Procedures and protocols associated with Information Conditions (INFOCON's) including;
  - ✓ INFOCON purpose, authority, application, and scope;
  - ✓ INFOCON risk analysis and structure;
  - ✓ Information Condition - Normal, Alpha, Bravo, Charlie and Delta.
- Information Assurance Vulnerability Management (IAVM) reporting and compliance standards including;
  - ✓ Information Assurance Vulnerability Alert (IAVA) reporting methods and compliance requirements;
  - ✓ Information Assurance Vulnerability Bulletin (IAVB) reporting and compliance requirements and;
  - ✓ Information Assurance Vulnerability Technical Advisories and Task Orders (IAV-TA/TO) reporting and compliance requirements.
  - ✓ Operations Security (OPSEC) involving the control and protection of open-source information that an adversary could use to achieve an intelligence goal. This includes;
- Establishing an organizational OPSEC policy, evaluating effectiveness and defining management goals this includes:
  - ✓ Identifying organizational OPSEC Essential Elements of Friendly Information (EEFI).
  - ✓ Defining the threats associated with solicitation and elicitation.
  - ✓ Establishing e-mail vulnerabilities as well as unique concerns and requisite security controls associated with publicly accessible and open-source web sites.

Malicious Logic/MALWARE - Prevention, Detection, Reaction, Recovery and Reporting

This lesson addresses the threat posed by malicious software as well as the proper methods for downgrading, declassifying and/or destroying hardware, software and memory components used to process sensitive, classified or cryptologic data. Specifically, this lesson focuses on:

- The technical and non-technical impact malicious logic has on an organization and internal measures necessary to;
  - ✓ Identify instances of malicious logic;
  - ✓ Establish methods necessary to prevent infection or introduction of malicious software;
  - ✓ Define actions required to prevent recurrence and;
  - ✓ Establish organizational reporting requirements and responsibilities.
- Methods and control procedures required to ensure the secure and proper disposition of hardware, software, memory components and recordable information storage media. This includes discussions on;
  - ✓ Overwriting processes and procedures;
  - ✓ Sanitizing processes and procedures;
  - ✓ Degaussing processes and procedures;
  - ✓ Destruction processes and procedures;
  - ✓ Clearing processes and procedures;
  - ✓ Declassification processes and procedures.

Configuration Management, Continuity of Operations Planning (COOP), and Disaster Recovery.

This lesson topic focuses on controlling changes to "trusted" computing baselines as well as the management of security features and assurances through control of changes made to a systems hardware, software, firmware, and documentation throughout the development and operational life of the system including:

- The business need to establish a plan of action for contingency situations. Including the requirement to;
  - ✓ Implement emergency response procedures including emergency destruction and emergency action planning.
  - ✓ Establish backup procedures and system restoration and recovery processes for critical information infrastructures.
  - ✓ Define Contingency Planning, preparatory and execution activities and;
  - ✓ Develop appropriate and functional emergency response protocols.

- Defining and developing a comprehensive Consequence Management Plan, Disaster Recovery Plan and Continuity of Operations Plan (COOP).

An Introduction to Penetration Testing (PENTEST).

This lesson topic focuses on the means and methods for conducting system and network penetration testing in support of an Information System Security posture assessment and certification program. This includes:

- 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.

Information System and Network Security Certification and Accreditation (C&A).

This lesson offers comprehensive discussions that center on the DOD Information Technology Security Certification and Accreditation Process (DITSCAP), the Defense Central Intelligence Directive (DCID) 6/3 C&A process, and the NSA Information Security Certification and Accreditation Process (NISCAP). This lesson also provides a contrast and comparison review between DITSCAP, NISCAP, DIACAP and NIACAP.

- Special emphasis is placed on the DITSCAP, DCID and NISCAP concept of certification and accreditation including:
  - ✓ The various phases and activities associated with the DITSCAP, DCID and NISCAP C&A process;
  - ✓ The characteristics of DITSCAP, DCID and NISCAP;
  - ✓ The different types of accreditation.
- The format and content of the DITSCAP System Security Authorization Agreement (SSAA) including a comprehensive overview of the SSAA structure including;
  - ✓ Consolidating and formulating information for the six major sections of the DITSCAP.
  - ✓ Establishing content requirements for all applicable appendices.

- ✓ Evaluating sensitivity concerns for the completed SSAA.
- ✓ Defining the scope, content, process and construction of a Security Test and Evaluation (ST&E) and the direct relationship it must have to the Security Requirements Traceability Matrix (SRTM).

- The format, structure and content of the DCID and NISCAP System Security Plan (SSP) including;
  - ✓ Baseline document requirements and developing appropriate appendices (e.g. Trusted Facility Manual (TFM), Security Feature User Guide (SFUG) and SRTM.
  - ✓ Specific classification guidelines.

Student Progress Checks:

As required by the customer, student comprehension may be measured by administering two progress checks that are strategically placed within the course curriculum. One progress check would occur at the beginning of the third day of training and a final cumulative progress check would be administered at the end of the last day of training. Satisfactory completion and remedial requirements will be consistent with each customer training standards.