ISSO Boot Camp

Course Summary

Description

This training focuses on planning, identifying, implementing, enforcing and maintaining data center security as well as integrating technical and non-technical 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 ISSO Bootcamp provides five days of comprehensive, non-technical, entry level professional training necessary to achieve the fundamental knowledge, skills, and abilities necessary to facilitate and integrate requisite system level security policies, processes, practices, procedures and protocols.

Objectives

By the end of this course, students will be able to:

- Learn the security planning and administrative security procedures for systems that process sensitive, classified and national intelligence data
- Understand the implementation and enforcement of Information System Security Policies and Practices
- Know the 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
- Learn the identification, analysis, assessment and evaluation of information system threats and vulnerabilities and their impact on an organization's critical information infrastructures
- Be able to identify management, technical, personnel, operational, and physical security controls

Topics

- Develop Certification and Accreditation Posture
- Implement Site Security Policy
- Enforce and Verify System Security Policy
- Report on Site Security Status
- Support Certification and Accreditation

Audience

This course is designed for those individuals currently holding ISSO positions; those earmarked for current or planned ISSO billets; Security Managers (Corporate or Departmental Security Officer staff) responsible for IS security, Chief Informatics Office (CIO) staffs including technical support, system managers, configuration managers, etc. who have collateral IS security responsibilities.

Prerequisites

There are no prerequisites for this course.

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ISSO Boot Camp

Course Outline

I. Develop Certification And Accreditation Posture

A. Planning For Certification And Accreditation
1. Planning
2. Defense in Depth
3. Assets
4. Threats
5. Vulnerabilities
6. Criticality
7. Risk
8. Conduct Risk Assessment
9. Countermeasures
10. Organizational/Agency Systems Emergency/Incident Response Team
11. Education, Training, & Awareness (ETA)
12. Residual Risk
13. Cost/Benefit Analysis

B. Confidentiality, Integrity, And Availability (Cia) Policy
1. Contingency Plans
2. Concept of Operations (CONOP)
3. Continuity Plans
4. Legal Plan
5. Disposition of Classified Material & Emergency Destruction Policy (EDP)
6. Identification and Authentication (I&A) Policy
7. Monitoring and Auditing Policy

C. Control Systems Policies
1. Configuration Management Policy
2. Protective Technology Policy
3. Intrusion Detection Policy
4. Malicious Code Policy
5. Access Controls

D. Culture And Ethics
1. Policy
2. Organization Culture
3. Basic/Generic Management Issues
4. Agency-Specific Security Policies & Procedures

E. Incident Response
1. Concept of Operations (CONOP)
2. Criminal Activity Preparedness Planning
3. Organizational/Agency Systems Emergency/Incident Response Team
4. Malicious Code

II. Implement Site Security Policy

A. Confidentiality, Integrity, And Availability (Cia)
1. Contingency Plans
2. Emergency Destruction Procedures (EDP)
3. Continuity Plans
4. Disposition of Classified Material
5. Monitoring and Auditing
6. Audit Trail and Logging, Error/System Logs
7. Intrusion Detection
8. Investigation of Security Breaches
9. Monitoring
10. Configuration Management
11. Countermeasures

B. Ensure Facility Is Approved
1. Facility Approval
2. OPERATIONS
3. Security Policy
4. Agency/Vendor Cooperation/Coordination
5. Certification Advocacy
6. Conduct Risk Assessment
7. Contracting for Security Services
8. Ensure information system is approved
9. Life Cycle System Security Planning
10. System Security Architecture Study

C. General Principles
1. Access Control Models
2. Approval to Operate
3. Attack
4. Business Aspects of Information Security
5. Common Criteria
6. Computer Network Attack
7. Criminal Prosecution
8. Defense in Depth
9. Due Care
10. Education, Training, & Awareness
11. Industrial Security
12. Information Warfare (INFOWAR) Concepts
13. Intellectual Property Rights
14. Interim Approval to Operate (IATO)
15. Investigative Authorities
16. Knowledge of Security Laws
17. Lattice Model
18. Law Enforcement Interfaces
19. Multi-level Security
20. Need for System Certification
21. Operating Security Features
22. Risk Management
23. Security Awareness as a countermeasure
24. Security Education as a countermeasure
25. Security Training as a countermeasure
26. Software Licensing
27. Software Piracy
28. Systems Security Authorization Agreement (SSAA)
29. Systems Security Plan (SSP)
30. Standards of Conduct
31. ITSEC/Common Criteria
32. Waive Policy to Continue Operation

D. Security Management
1. Electronic Records Management
2. Records Retention
3. E-Mail
4. Non-Repudiation
5. Hardware Asset Management
6. Software Asset Management

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ISSO Boot Camp

Course Outline (cont'd)

E. Access Controls
   1. Human Access
   2. Key Management
   3. Incident Response
   4. Security Investigation Procedures

III. Enforce And Verify System Security Policy

A. Confidentiality, Integrity, And Availability/Accountability (Cia)
   1. Planning
   2. Monitoring And Auditing
   3. Environmental Controls
   4. Filtered Power
   5. Fire Prevention
   6. Grounding
   7. Safety

B. Security Management
   1. Electronic Records Management
   2. Records Retention
   3. E-Mail
   4. Non-Repudiation
   5. Hardware Asset Management
   6. Software Asset Management

C. Access Controls
   1. Human Access
   2. Key Management
   3. Configuration Management
   4. Protective Technology
   5. Media Security
   6. Network Assurance

D. Automated Security Tools
   1. Automated Security Tools
   2. Initiate Protective And/Or Corrective Measures

E. Handling Media
   1. Handling Media
   2. Labeling
   3. Marking Of Media/Information Systems Oversight Office (Isoo) Rules
   4. Marking Of Sensitive Information
   5. Physical Controls & Accounting
   6. Remanence
   7. Transportation
   8. Disposition Of Classified Material

F. Incident Response
   1. Criminal Prosecution
   2. Evidence Acceptability
   3. Evidence Collection And Preservation
   4. Legal And Liability Issues

IV. Report On Site Security Status

A. Security Continuity Reporting
   1. Contingency Plans
   2. Continuity Plans
   3. Disposition Of Classified Material & Emergency Destruction Procedures (Edp)
   4. Monitoring And Auditing
   5. Identification & Authentication
   6. Configuration Management
   7. Testing

B. Report Security Incidents
   1. Computer Organizational/Agency Systems Emergency/Incident Response Team
   2. Security Incidents
   3. Security Violations Reporting Process (Incident Response)

C. Law
   1. Investigative Authorities
   2. Law Enforcement Interfaces (Lei)
   3. Witness Interviewing/Interrogation
   4. Entrapment
   5. Disgruntled Employees

D. Report Security Status Of Information System As Required
   1. Administrative Security Policies And Procedures
   2. Agency Specific Security Policies
   3. Organizational/Agency Systems Emergency/Incident Response Team
   4. Automated Systems Security Incident Support Team (Assist)
   5. Trade Journals, Bulletin Board System (Bbs) Notices

E. Report To Ig
   1. Inspector General (Ig) (External) Audit & Assessments

V. Support Certification And Accreditation

A. Certification Function
   1. Assessments (E.G., Surveys, Inspections)
   2. Risk Assessment
   3. Technical Certification
   4. Verification And Validation Process

B. Accreditation Function
   1. Isso
   2. Managers
   3. System Administrator (Sa)

C. Respond To Requests
   1. Approval To Operate
   2. Assessment Methodology
   3. Certification Statement
   4. Certification Tools
   5. Identify Security Changes
   6. Interim Approval To Operate (Iato)
   7. Re-Certification
   8. Security Test & Evaluation (St&E)
   9. Ssaa
   10. Type Accreditation
   11. Waive Policy To Continue Operation

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically