Enterprise Security Management  
CIS 259

Prerequisites  
CIS 175

Description  
This course is designed to cover the managerial aspects of computer security and risk management for enterprises. The student will attain knowledge for accreditation, procurement, extension and operation principles for secure computing systems. This course is one of the required courses for obtaining the NSTISSI 4011 and CNSSI 4013 certifications.

CNSSI 4013 Course Objectives

CNSSI 4013 Mapping Details

General Course Objectives

Textbook  

Other References  


Department of Defense Directive 8500.01E, October, 2002

http://en.wikiversity.org/wiki/Introduction_to_Computers


Key Management Using ANSI X9.17, U.S. Department of commerce,

OMB Circular A-130


Grading and Evaluation Criteria
30% of the grade is based on quizzes.
70% of the grade will be based on in-class and take-home labs

**Grading Scale**
A = 92 - 100
B = 83 - 91
C = 75 - 82
D = 70 - 74
F = 69 or below

**Late Work**
Late lab assignments and quizzes **will not** be accepted. Please be sure to keep up and pay very close attention to the due dates.

**Other Comments**
Dishonesty will not be tolerated. A final course grade of F will be given to any student caught cheating. See the academic honesty statement.

Jackson State will make reasonable accommodations for persons with documented physical, mental or learning disabilities. Students should notify their instructor and the Coordinator of Disabled Student Services – located in the Counseling Office, Room 12 of the Student Union Building - of any special needs. Instructors should be notified the first week of class. All discussions remain confidential.

No children allowed in the classroom.
F1A1. Define and outline organizational accountability policies, processes and programs
F1A2. Define and discuss emerging trends in the certification and accreditation policy of U.S. federal and other organization IT systems
F1A3. Describe the dominant information security blueprints, frameworks, and information security management models, including U.S. government–sanctioned models
F1A4. Select an information security management model and customize it to meet the needs of a particular organization as it relates to a system security architecture study
F1A5. Discuss and define how assessments for use during certification of information systems are prepared
F1A6. Discuss NSTISSP 11 (Common Criteria) policies
F1A7. Define and explain configuration control (management)
F1A8. Define defense in depth and give examples of defense in depth methods and policy
F1A9. Identify Department of Defense Directive 8500.1 policies appropriate civil agency guidance
F1A10. Define and describe security domains applicable to organizational policies
F1A11. Define generally accepted security principles, goals, mission and objectives of the organization
F1A12. Define and describe information assurance with regards to accreditation, planning, design, implementation and policy development
F1A13. Understand that a successful information security program is the responsibility of both an organization’s general management and IT management which includes information operations and records retention
F1A14. Using examples, demonstrate how to perform marking of sensitive information procedures and discuss policies relating to marking of classified, unclassified and sensitive information
F1A15. Define magnetic media degaussing, marking, handling, storing and destroying sensitive information and media, media management, identify information resource owner and secure data deletion for media reuse
F1A16. Identify systems security standards policies
F1A17. Identify Information Technology Security Evaluation Criteria (ITSEC) policies
F1A18. Discuss the phases of the security systems development life cycle management, which includes requirements definitions, development, demonstration and validation, implementation, operations and testing and security with regards to certification and accreditation
F1A19. Describe workstation security policies

F1B1. Describe the dominant information security blueprints, frameworks, and information security management models, including U.S. government–sanctioned models
F1B2. Explain why access control is an essential element of information security management
F1B3. Select an information security management model and customize it to meet the needs of a particular organization as it relates to a system security architecture study
F1B4. Discuss how assessments for use during certification of information systems are prepared
F1B5. Discuss NSTISSP 11 (Common Criteria) policies
(F1A) General Security Policy
  o (F1A1) Accountability: OMB Circular A-123, Management’s Responsibility for Internal Control defines organizations accountability policies and outlines accountability processes and programs. Course objective F1A1
  o (F1A2) Accreditation: Course textbook defines accreditation. Course objective F1A2
  o (F1A3) Architecture: Course textbook defines system security architectures, identifies appropriate security architectures for use in assigned IS, and address system security architecture study. Course objectives F1A3 and F1A4
  o (F1A6) Availability, Integrity, Confidentiality, Authentication and Non-Repudiation: Covered in the CIS 156 course.
  o (F1A7) Certification: The NIST Handbook Special Publication 800-12 – NIST 800-12.pdf Chapter 8 and the course textbook defines certification policies as related to organizational requirements. Course objectives F1A2
  o (F1A8) NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products: http://www.niap-ceevs.org/ web site contains detailed information about NSTISSP 11 and Common Criteria Evaluation and Validation Scheme. The course textbook also address Common Criteria. Course objective F1A6
  o (F1A9) Configuration Control: NIST Special Publication 800-53 Rev. A - Recommended Security Controls for Federal Information Systems and Organizations explains configuration control (management). Course objective F1A7
  o (F1A10) Custodian: Covered in the CIS 156 course.
  o (F1A11) Defense in Depth: CNSS Instruction No. 4009: National Information Assurance (IA) Glossary define defense in depth. Examples of defense in depth methods and policy will be presented. Course objective F1A8
  o (F1A12) Document: Department of Defense Directive 8500.01E policies are identified. Course objective F1A9
  o (F1A13) Domains: Department of Defense Directive 8500.01E defines and describes security domains applicable to organizational policies. Course objective F1A10
  o (F1A14) E-Mail: Covered in the CIS 156 course.
  o (F1A15) Wireless Security: Covered in the CIS 250 course.
  o (F1A16) EMSEC/TEMPEST (Emanations Security/Short name referring to the investigation, study, and control of compromising emanations from IS equipment): Covered in the CIS 250 course.
  o (F1A18) FAX: Covered in the CIS 156 course
  o (F1A19) Generally Accepted Security Principles: The NIST Handbook Special Publication 800-12 – NIST 800-12.pdf and the course textbook define generally accepted security principles. Course objective F1A11
  o (F1A20) Goals/Mission/Objectives: The NIST Handbook Special Publication 800-12 – NIST 800-12.pdf and the course textbook define goals, missions and objectives of the organization. Course objective F1A11
  o (F1A21) Incident Response: Covered in the CIS 156 course

(F1A23) Information Operations [DOD Organizations Only]: The NIST Handbook Special Publication 800-12, Chapter 14 defines, describes and discusses how to support information operations. Course objective F1A13.

(F1A24) Internet Security: Covered in the CIS 156 course.

(F1A25) Law Enforcement: Covered in the CIS 156 course.

(F1A26) Marking: Covered in the CIS 156 course.

(F1A27) Monitoring: Covered in the CIS 156 course.

(F1A28) Multi-Level Security: Covered in the CIS 156 course.

(F1A29) Network: Covered in the CIS 250 course.

(F1A30) Operating System: Covered in the CIS 250 course.

(F1A32) Ownership: Covered in the CIS 156 course.

(F1A33) Physical Security: Covered in the CIS 250 course.

(F1A34) Records Management: Covered in the CIS 156 course.

(F1A37) Security Tools: Covered in the CIS 156 course.

(F1A38) Sensitivity: 32 CFR Parts 2001 and 2003 Classified National Security Information defines, describes and explains information sensitivity in relation to organizational policies. Course objectives F1A14 and F1A15.

(F1A39) Separation of Duties: Covered in the CIS 156 course.


(F1A42) Testing: Covered in the CIS 156 course.

(F1A43) Validation/Verification: The NIST Handbook Special Publication 800-12 – NIST 800-12.pdf – Chapter 8 defines and identifies validation and verification process policies. Course objective F1A18.

(F1A44) Workstation: The NIST Handbook Special Publication 800-12 – NIST 800-12.pdf – Chapter 15 describes workstation security policies. Course objective F1A19.

(F1A45) Zone: Covered in the CIS 250 course.

(F1B) General Procedures

(F1B1) Network Software: CIS 175.

(F1B2) Aggregation: CIS 156.

(F1B3) Application Vulnerabilities: CIS 156.

(F1B4) Architecture: The course textbook addresses system security architecture study. Course objectives F1B1, F1B3.

Enterprise Security Management

CIS 259

General Course Objectives

1. Assess risk based on the likelihood of adverse events and the effects on information assets when events occur
2. Create a simple set of contingency plans, using business impact analysis
3. Define and describe information assurance with regards to accreditation, planning, design, implementation and policy development
4. Define and describe security domains applicable to organizational policies
5. Define and Discuss emerging trends in the certification and accreditation policy of U.S. federal and other organization IT systems
6. Define and explain configuration control (management)
7. Define and outline organizational accountability policies, processes and programs
8. Define defense in depth and give examples of defense in depth methods and policy
9. Define generally accepted security principles, goals, mission and objectives of the organization
10. Define information security policy and understand its central role in a successful information security program
11. Define magnetic media degaussing, marking, handling, storing and destroying sensitive information and media, media management, identify information resource owner and secure data deletion for media reuse
12. Define risk management and its role in the organization
13. Describe the components of a security education, training, and awareness program and explain how organizations create and manage these programs
14. Describe the dominant information security blueprints, frameworks, and information security management models, including U.S. government–sanctioned models
15. Describe the ethical foundations and approaches that underlie modern codes of ethics
16. Describe the importance of the manager’s role in securing an organization’s use of information technology and understand who is responsible for protecting an organization’s information assets
17. Describe the key components of a security metrics program
18. Describe the major components of contingency planning
19. Describe the OCTAVE Method and other approaches to managing risk
20. Describe the role of culture as it applies to ethics in information security
21. Describe the three major types of information security policy and explain what goes into each type
22. Describe the various access control approaches, including authentication, authorization, and biometric access controls
23. Describe workstation security policies
24. Determine how to plan and staff an organization’s information security program based on its size
25. Develop, implement, and maintain various types of information security policies
26. Differentiate between law and ethics
27. Differentiate between strategic organization information security planning and specialized contingency planning
28. Differentiate information security management from general management
29. Discuss and define how assessments for use during certification of information systems are prepared
30. Discuss and implement information security constraints on the general hiring processes
31. Discuss emerging trends in the certification and accreditation of U.S. federal IT systems
32. Discuss how assessments for use during certification of information systems are prepared
33. Discuss NSTISSP 11 (Common Criteria) policies
34. Discuss the phases of the security systems development life cycle management, which includes requirements definitions, development, demonstration and validation, implementation, operations and testing and security with regards to certification and accreditation
35. Document the results of risk identification
36. Enumerate and define the key characteristics of leadership and management
37. Enumerate and discuss the current issues in dial-up access and protection
38. Enumerate and explain the unique considerations and relationships that exist among the types of specialized contingency planning – IRP, DRP, and BCP
39. Evaluate risk controls and formulate a cost-benefit analysis using existing conceptual frameworks
40. Evaluate the internal and external factors that influence the activities and organization of an information security program
41. Explain cryptography and the encryption process, and compare and contrast symmetric and asymmetric encryption
42. Explain how to maintain and perpetuate risk controls
43. Explain the organizational approaches to information security
44. Explain the principal components of information security system implementation planning in the organizational planning scheme
45. Explain the role of information security in employee terminations
46. Explain the unified contingency plan approach
47. Explain why access control is an essential element of information security management
48. Identify and describe the types of intrusion detection systems and the two strategies on which they are based
49. Identify and implement basic project management practices and techniques
50. Identify current information on laws, regulations, and relevant professional organizations
51. Identify Department of Defense Directive 8500.1 policies pr appropriate civil agency guidance
52. Identify Information Technology Security Evaluation Criteria (ITSEC) polices
53. Identify major national and international laws that relate to the practice of information security
54. Identify suitable strategies for the implementation of a security metrics program
55. Identify systems security standards policies
56. Identify the roles in organizations that are active in the planning process
57. Identify the skills and requirements for information security positions
58. Identify the various types of firewalls and the common approaches to firewall implementation
59. Implement the fundamental elements of key information security management practices
60. List and describe the functional components of an information security program
61. List and describe the typical job titles and functions performed in the information security program
62. List the elements of key information security management practices
63. List the various information security professional certifications, and identify which skills are encompassed by each
64. Prepare and execute a test of contingency plans
65. Recognize and select from the risk mitigation strategy options used to control risk
66. Recognize the need for contingency planning
67. Select an information security management model and customize it to meet the needs of a particular organization as it relates to a system security architecture study
68. Understand that a successful information security program is the responsibility of both an organization’s general management and IT management which includes information operations and records retention
69. Use risk management techniques to identify and prioritize risk factors for information assets
70. Using examples, demonstrate how to perform marking of sensitive information procedures and discuss policies relating to marking of classified, unclassified and sensitive information