

COURSE OUTLINE

CMSY-264 Successful CISSP Preparation 3 Semester Hours

HOWARD COMMUNITY COLLEGE

Description

The Computer Information Systems Security Professional (CISSP) designation is particularly useful for those who are focused on managing either process or people responsible for activities related to the design, implementation and administration of an information security infrastructure. Topics will include practical aspects of law and forensics, physical and operations security, technical elements of networking and encryption and basic tenets of access control, security models and management practices. Upon completion of the course, the student will have a framework necessary to successfully complete the CISSP exam. Three to four years of related experience are needed to sit for this exam. Testing instruments similar to the CISSP examination will be used to demonstrate comprehension during midterm and noncumulative final exams. (3 hours weekly)

Overall Course Objectives

Upon completion of this course, the student will be able to:

1. Describe major elements of security planning to include risk analysis, data classification and access control.
2. Describe key elements of computer architecture to include systems and security models.
3. Describe elements of physical security to include electrical power, fire suppression and perimeter security.
4. Analyze major elements of computer networking to include the OSI layers, LAN access technologies, network topologies, firewalls and network types.
5. Compare and contrast elements of encryption to include cipher types, encryption methods, PKI, Internet security and typical attacks.
6. Describe operations issues for security to include separation of duties, need to know, least privilege, change control, and typical attacks.
7. Develop a business recovery plan to include business continuation, disaster recovery, backup models, stages of recovery planning, types of recovery sites and types of recovery testing.
8. Analyze legal and ethical issues related to security to include well known ethical standards, types of computer fraud, examples of computer crimes, forms of law, forms of evidence, elements of computer forensics and well-known government regulations.
9. Describe security aspects related to applications to include security controls, database terms and function and elements of object-oriented programming.

Major Topics

- I. Security Management Practices
- II. Law, Investigation and Business Ethics
- III. Security Models, Architecture and Access Control
- IV. Application and System Development
- V. Telecommunications and Networking Security
- VI. Cryptography
- VII. Physical and Operations Security
- VIII. Disaster Recovery and Business Continuity

Course Requirements

Grading/exams: Grading procedures will be determined by the individual faculty member. Quizzes, exams, and in-class participation will be included.

Other Course Information

Parallel discussion and guide sessions will be available.

Students should plan to take the CISSP exam within four weeks of completing the course.