CYBR C270: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Item	Value
Curriculum Committee Approval Date	02/26/2021
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Formerly: CST C260 / CST C260B. Students will explore the eight domains of information security known as the CISSP Common Body of Knowledge (CBK). Domain topics covered include security and risk management, asset security, security architecture and engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security. Concepts covered will help students understand management level issues relevant to cybersecurity professionals, with roles such as IT Director/Manager, Security Systems Engineer, Security Analyst, Security Manager, Security Auditor, and Security Architect. Completing this course does not guarantee CISSP certification; however, the course addresses the exam objectives defined by (ISC)2 for the CISSP certification exam. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Describe the eight domains of the CISSP 'Common Body of Knowledge' (CBK) defined by the International Information Systems Security Certification Consortium (ISC)2.
2. Analyze laws, regulations, and compliance pertaining to cybersecurity incidents and business scenarios.
3. Define the key concepts and importance of business continuity and disaster recovery planning.
4. Given a business scenario, identify potential security vulnerabilities, threats, and countermeasures.

Course Objectives

- 1. Explain the OSI model and its relationship to network security.
- 2. Identify a companys assets and determine the level of security necessary to protect the assets.
- 3. Distinguish between various cryptographic systems to determine which would be most useful for a particular network.
- 4. Discuss various methods of auditing and monitoring a network and its users.
- 5. Describe the components of a comprehensive business continuity/ disaster recovery plan.
- 6. Describe various computer crimes, laws, and regulations.
- 7. Analyze plans for physical security to defend business network systems.

Lecture Content

Security Governance Through Principles and Policies Personnel Security and Risk Management Concepts Business Continuity Planning Laws, Regulations, and Compliance Protecting Security of Assets Cryptography and Symmetric Key Algorithms PKI and Cryptographic Applications Principles of Security Models, Design, and Capabilities Security Vulnerabilities, Threats, and Countermeasures Physical Security Requirements Secure Network Architecture and Securing Network Components Secure Communications and Network Attacks Managing Identity and Authentication Controlling and Monitoring Access Security Assessment and Testing Managing Security Operations Preventing and Responding to Incidents Disaster Recovery Planning Investigations and Ethics Software Development Security Malicious Code and Application Attacks

Lab Content

There will be labs that involve topics important to securing a computer network. Examples: PKI and Cryptographic Applications Security Models, Design, and Capabilities Managing Identity and Authentication

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Students are required to read the assigned chapters, supplemental material, and CISSP exam materials.

Writing Assignments

Written assignments consist of topics from class activities and forum discussions.

Out-of-class Assignments

Students will complete hands-on labs based on remote network environments. Students will also complete quizzes, exams, knowledge-based assignments, definitions, and text-based scenario questions.

Demonstration of Critical Thinking

Students will review topics regarding cybersecurity teams using best practices, processes, and procedures. Given business scenarios, students will evaluate situations to provide recommendations to modify procedures and processes following best practices.

Required Writing, Problem Solving, Skills Demonstration

Students will respond to scenario-based questions, recommend solutions to business security problems, and complete quizzes and exams to demonstrate skills.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Chapple, Mike; Stewart, James; Gibson, Darril. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 8th ed. Indianapolis, IN: John Wiley Sons, Inc., 2018 Rationale: -

Other Resources

1. Coastline Library