Course number and name: **CS 03506: Cybersecurity Management, Policy, and Risk**

Credits and contact hours: 3 credits / 3 contact hours

Course Coordinator: Hope Bronson

Instructional Materials: The Cybersecurity Guide to Governance, Risk, and Compliance, First Edition, 2024, Edwards & Weaver

Specific course information

Catalog description: This course introduces students to the management and governance of cybersecurity programs, with an emphasis on policy, risk, and compliance. Students examine cybersecurity planning, security risk analysis, legal and ethical considerations, regulatory obligations, and security program management from a technical and operational perspective.

Prerequisites: None

Type of Course: ☒ Required ☐ Elective ☐ Selected Elective

Educational objectives for the course:

- Examine the placement of security functions in a system and describe the strengths and weaknesses.
- Develop contingency plans for various-sized organizations to include business continuity, disaster recovery, and incident response.
- Develop system-specific plans for a) the protection of intellectual property, b) the implementation of access controls, and c) patch and change management
- Outline and explain the roles of personnel in planning and managing security, including a) board of directors, b) senior management, c) chief information security officer (CISO), d) IT management (CIO, IT Director, etc.), e) functional area management, f) information security personnel, and g) end users
- List the applicable laws and policies related to cyber defense and describe the major components of the storage and transmission of data.
- Describe their responsibilities related to the handling of data as it pertains to legal, ethical, and/or agency auditing issues.
- Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.
- Apply knowledge to develop a security program and identify goals, objectives, and metrics.
- Apply knowledge to effectively manage a security program.
- Assess the effectiveness of a security program.

- Describe how risk relates to a system security policy.
- Describe various risk analysis methodologies.
- Evaluate and categorize risk 1) with respect to technology, 2) with respect to individuals, and 3) in the enterprise; recommend appropriate responses.
- Compare the advantages and disadvantages of various risk assessment methodologies.
- Select the optimal methodology based on needs, advantages, and disadvantages

Required list of topics to be covered:

1. Introduction to GRC (Governance, Risk, and Compliance)
2. Overview of Cybersecurity Landscape
3. Cybersecurity Leadership
4. Program & Project Management in Cybersecurity
5. Executive and Board Engagement in Cybersecurity
6. Enterprise-Wide Responsibilities in Security Planning and Management
7. Enterprise Risk Management
8. NIST Risk Management Framework (RMF)
9. Cybersecurity Metrics
10. Risk Assessments
11. Developing a security program and identifying goals, objectives, and metrics.
12. Cybersecurity Frameworks (NIST, CSF, ISO/IEC, etc.)
13. Security and Privacy Controls
14. FFIEC Examination Standards
15. U.S. Federal Cybersecurity Laws
16. U.S. State Cybersecurity Laws
17. International Cybersecurity Laws
18. Privacy Laws
19. Cybersecurity Auditing
20. Role of the Regulator
21. Ethics in Governance, Risk, and Compliance
22. U.S. Regulatory Bodies
23. Managing Regulatory Visits
24. Regulatory Penalties
25. Remediating Findings
26. Cybersecurity Architecture
27. Risk Mitigation Techniques
28. Placement of security functions within a system and describing strengths and weaknesses
29. Business Continuity & Disaster Recovery
30. Incident Response Planning
31. Cyber Insurance Considerations
32. Preparing for Emerging Technologies (AI, Quantum)
33. Security Program Evaluation and Continuous Improvement