Master of Science in Cybersecurity

Syllabus for CYB765 Cybersecurity Management

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

Covers management of cybersecurity policies and strategies at the organizational, national, and transnational levels. Examines the implications of key domestic and international regulations and changes in information technology and communications on security operations. Includes development of organizational security preparation, processes, and responses, and developing a disaster recovery program.

Prerequisite(s)

CYB 700, 703, 705, 707, 715, 720

Program Outcomes

This course addresses the following competencies and program outcomes of the Master of Science in Cybersecurity:

- Program Outcome 3: Design, evaluate, and test systems including networks, computers, and hardware for security requirements
- Program Outcome 7: Conduct security risk management assessments
- Program Outcome 8: Develop and implement threat management framework
- Program Outcome 9: Evaluate and create security policies and processes for an organization and apply appropriate security frameworks
- Program outcome 10: Implement identity and access management controls
- Program Outcome 11: Assess trends in computer criminology and social behaviors related to technology use including physical security
- Program Outcome 12: Engage in ethical decision-making and apply ethical principles to cybersecurity
- Program Outcome 13: Engage in professional collaboration and communication with technical and nontechnical stakeholders on issues related to security

Course Outcomes

Upon completing this course, you will be able to do the following:

1. Formulate a management strategy for cybersecurity
2. Assess cybersecurity risks for organizations
3. Assess the application of a security framework to an organization
4. Implement security policies using procedures and guidelines
5. Plan and manage cybersecurity operations

Course Components

Quizzes

Every topic will include a quiz that covers foundational terminology and concepts.

Discussions

The purpose of lesson discussions is to engage in critical reflection and dialogue with classmates regarding course content.

Assignment

You'll encounter a variety of assignments covering cybersecurity planning, conducting a risk analysis of a fictitious organization, using the COSO framework to evaluate SaaS providers, evaluating baseline controls implemented by an organization and suggesting improvements, developing an incident response plan for a fictitious organization, evaluating the results of an audit and planning methods for remediation.

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	>94%
A-	>90%
B+	>87.5%
B	>85%
B-	>80%
C+	>77.5%
C	>70%
C-	>65%
F	<65%

Assignment	Percentage
Quizzes	25%
Discussions	30%
Assignments	45%
Total Percentage	**100%**