Master of Science in Cybersecurity

Syllabus for CYB 707 Cybersecurity Program Design and Implementation

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

Course Description

Instruction on the process used to develop and maintain appropriate security levels for an organization with a focus on implementing a comprehensive security program, a documented set of security policies, procedures, guidelines, and standards. Topics include security planning, strategies, controls, and metrics for measuring the effectiveness.

Extended Course Description

The course considers security from the high-level down, and considers technical, administrative, and physical aspects of IT security in an organization. Specific topics covered in class include fraud, risk, information protection, business continuity, network security, auditing, physical security and governance. The course material is taken mainly from the three professional certificates: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and the Certified Information Systems Security Professional (CISSP).

Prerequisite(s)

CYB 700: Fundamentals of Cybersecurity

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 frameworks
- Program Outcome 9: Evaluate and create security policies and processes for an organization and apply appropriate security frameworks
- Program Outcome 9: Implement identity and access management controls
- Program Outcome 9: Develop and implement an incident response strategy

Course Outcomes

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

- Develop an action plan to combat security fraud
- Analyze business impact of disaster recovery and plan for business continuity
- Select technologies to implement security controls and monitor security incidents
- Define and discuss the concepts for network security controls and secure network services
- Analyze and select technical and policy solutions for physical and personnel security
- Assess security risks and conduct financial analysis for business risk

- Develop an incident response plan and apply concepts of incidence response
- Describe business-driven and technology-driven metrics for security
- Conduct a security audit and prepare/present the audit report
- Document security policies, standards, procedures, and guidelines

Course Requirements/Components

Quizzes

Every topic will include a terminology/basic concept quiz. These quizzes may be taken as many times as possible to achieve full marks.

Workbook Assignments and Small-Group Discussions

Most lecture topics will include a workbook assignment. These assignments will provide you with the base material to be used in the project assignment. You will be asked to submit your work for peer review and enhancement via small-group discussions.

Topical Discussions

Most real learning comes not from mere reading or listening to a lecture but from a true exchange of ideas and questions. In a traditional classroom, discussions are easy and natural. In the online environment, we will attempt to simulate these discussions through prompting questions and a space for responses. While there is a longer description of discussion expectations elsewhere in the course material, fundamentally, you are expected to participate in those discussions fully—not only for your education but for the expanded education of your classmates.

Major Project: Security Plan

Throughout the semester, you will be working on an implementable security plan for an organization of your choice. Since this plan is designed to be implementable, you will need access to people in the organization who can answer questions about organizational processes, technology, and policy.

There will be two submissions for this assignment. A submission approximately halfway through the course will consist of the first part of the security plan document and a session with the instructor to discuss progress and issues. The second submission will include the entire security plan document and a session with the instructor where a formal presentation of the plan will be presented. Both the first and second sessions with the instructor will take place through Collaborate Ultra in Canvas.

Grading

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

Grade	Percentage Range
A	94% - 100%
A-	90% - < 94%
B+	87% - < 90%
B	84% - < 87%
B-	80% - < 84%
C+	77% - < 80%
C	74% - < 77%
C-	70% - < 74%
F	0 - < 70%

Assignments	Percentage
Major Project	40%
Topical Discussions	30%
Workbook Assignments and Small-Group Discussions	20%
Quizzes	10%
Total	**100%**