



CYB-301: Information Security Management

Description:

3 credits/126 hours

Prerequisite: None

This course is designed to give students a managerially focused overview of information security and how to effectively administer it. Students will be prepared to become information security management practitioners able to secure systems and networks and to meet the challenges in a world where continuously emerging threats, ever-present attacks, and the success of criminals illustrate weaknesses in current information technologies.

Textbook: Management of Information Security, 5th ed., Whitman & Mattord– ISBN: 978-1-305-50125-6

Course objectives:

Throughout the course, you will meet the following goals:

- Understand the importance of the manager’s role in information security
- Describe key characteristics of information security and the dominant categories of threats to information security
- Differentiate between laws and ethics in information security
- Define information security policy and understand the role it plays
- Understand risk management and how it impacts an organization
- Explain the dominant security blueprints, frameworks, and management models
- Understand personnel management and the protection mechanisms used in information security

Contents:

Chapter 1: Introduction to the Management of Information Security

Chapter 2: Compliance: Law and Ethics

Chapter 3: Governance and Strategic Planning for Security

Chapter 4: Information Security Policy

Chapter 5: Developing the Security Program

Chapter 6: Risk Management: Identifying and Assessing Risk

Chapter 7: Risk Management: Controlling Risk

Chapter 8: Security Management Models

Chapter 9: Security Management Practices

Chapter 10: Planning for Contingencies

Chapter 11: Personnel and Security

Chapter 12: Protection Mechanisms

Grading Scale

A = 95-100%

B = 88-94.9%

C = 80-87.9%

Grade Weighting

Chapter Quizzes..... 50%

Activities 20%

Final Exam 30%

D = 70-79.9%
F = Below 70%

100%