Syllabus for ITM 725 Enterprise Security

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

Prerequisites

ITM 700: Communications for IT Professionals

Course Description

The enterprise security management course explores various technical, administrative, and physical aspects of IT security. The course seeks to investigate various security threats and apply various concepts to the design of information, network and physical security. Students are exposed to the evaluation of business processes associated with managing risks, business continuity, audit, and security challenges in software development.

Course Alignment with Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Information Technology Management:

Competency D: Manage security and compliance accounting for governance and ethical implications

- Program Outcome 10: Apply ethical frameworks to analyze problems and evaluate alternative solutions
- Program Outcome 11: Create and manage technology policies and procedures for an organization with an understanding of the regulatory environment
- Program Outcome 12: Interpret and manage IT governance policies.

Competency F: Engineer, develop and deploy strategies for enterprise systems

- Program Outcome 17: Develop appropriate data management technologies
- Program Outcome 18: Create and deploy enterprise solutions in support of organizational goals

Course Learning Objectives

At the end of this course, you will be able to:

1. Apply ethical frameworks to analyze problems and evaluate alternative solutions
2. Create and manage technology policies and procedures for an organization with an understanding of the regulatory environment
3. Interpret and manage IT governance policies
4. Design appropriate security architecture with an understanding of the technology
5. Create and deploy enterprise solutions in support of organizational goals
6. Plan and implement projects related to infrastructure, security, software development or data analysis

Course Activities and Assessments

This course will include a variety of activities and assessments including discussions, lab exercises, individual assignments, group projects, and an individual project.

Course Outline

The course is organized into the following modules. (Check the course calendar for due dates.)

Module	Topic	Key Topics	Activities & Evaluation
1	Intro to Information Security	CIA triad: Confidentiality, Integrity, Availability RMIAS model Information Security knowledge areas Cyber Security industry, certifications, and careers Cryptography	**Discussion**: Welcome/Student Introduction Quiz 1 **Individual Assignment 1:** Interview**/**Research paper on the state of Security in your Organization
2	Introduction to Computer Networks	Introduction to Networking Security protocols Threats Authentication and Authorization Access Controls Security Vulnerabilities Security Tools — Penetration testing, etc.	Quiz 2 **Lab Exercise 1:** Introduction to Kali Linux and MetaSpoilt **Video Check-in**
3	IT Security Governance and Risk Management	Four types of policies Develop and manage security policies Perform risk management for IT security Threat identification and classification Incident Management	Quiz 3 **Individual Assignment 2:** Case Study for Quantitative Risk Analysis & Risk Management plan
4	Business Continuity Planning and Disaster Recovery Planning	IT security business continuity planning IT security disaster recovery planning	Quiz 4 **Group Assignment 1:** Case Study for Cloud Hosting: Build a BC/DR plan
5	Laws, Investigations and Ethics	Types of computer crime Privacy and the law Computer forensics Information security professional's code of ethics Intellectual property law	Quiz 5 **Individual Assignment 3:** Case Study for Cyber Crime **Lab Exercise 2:** Network Forensics, Investigating Logs and Investigating Network Traffic – WireShark **Video Check-in**

	Mid-Semester	**Final Project Checkup**	**Final Individual Project:** Security Plan - Part A
6	Physical Security	Physical security domain Physical safeguards	Quiz 6 **Individual Assignment 4:** Case Study for Physical Security -- analyze and recommend remediation
7	Software Development Security	Software development lifecycle Security design reviews Best practices in software engineering	Quiz 7 **Individual Assignment 5:** Case Study for Software Development -- analyze and recommend remediation **Lab Exercise 3:** SQL Injection test
8	IT Security Enterprise Solutions	Network security in context Protecting TCP/IP networks Virtual Private Networks IPSec Overview of Cloud Security	Quiz 8 **Group Assignment 2:** Case Study for Azure Cloud security - analyze and recommend remediation **Lab Exercise 4:** Port Scanning - pre-configured VirtualBox VM to find vulnerabilities **Video Check-in**
9	Network Security architecture and design	Defining the trusted computing base System security assurance concepts Confidentiality and Integrity models	Quiz 9 **Individual Assignment 6:** Security Architecture Design
	End of Semester	**Final Project Presentation**	**Final Individual Project:** Security Plan - Part B

Grading

Course Grading: Grades will be assessed using a variety of methods including discussions, lab exercises, individual assignments, group projects, and an individual project.

GRADE WEIGHTS:

Activity	**Weight**
Discussion participation/Check-ins/Quizzes (9)	15%
Lab Exercises (4 – *Lessons 2, 5, 7 & 8*)	15%
Individual Assignments (6 – *Lessons 1, 3, 5, 6, 7 & 9*)	30%
Group Project Reports (2 – *Lessons 4 & 8*)	10%
Final Individual Project	30%

GRADE SCALE:

Grade	**Percentage**
A	90 - 100%
A-	<90 - 85%
B+	<85 - 80%
B	<80 - 75%
B-	<75 - 70%
C+	<70 - 65%
C	<65 - 60%
C-	<60 - 55%
F	<55 – 50%