TIM-7030: Managing Risk, Security, & Privacy in Information Systems

(3 credits)

## Course Description:

With more application, systems and data processed and managed in mobile, cloud, and virtual environments, privacy, and security issues are on the rise. Privacy and integrity issues are also a growing threat to the normal and secure state of internal operations. Record tampering and accidental or intentional exposure are also among the internal risks every enterprise faces. During this course, you will learn how to assess, mitigate, and manage risks, threats, and vulnerabilities. You will also study theories and techniques to effectively design protection mechanisms, practices, and procedures to implement and manage operations and information systems and applications.

## Number of Activities: 11

## Learning Outcomes:

1. Assess emerging technologies and techniques for their utility in managing risk in information systems.
2. Examine current and emerging theories of risk mitigation and risk management in traditional and cloud infrastructure landscapes.
3. Evaluate the gaps between theory and practice in the management of risk, security, and privacy.
4. Devise risk reduction strategies to improve the current theory and practice of the management of risk, security, and privacy.

## Course Concepts:

1. Security Risk Analysis
2. Risk Management
3. Security Information and Event Management
4. Logs Collection and Analysis
5. Information Security Policies and Procedures
6. Risks, Security, and Privacy Research

## Primary Resource/textbook:

None

# Course Overview

**Section 1: Managing Risk in Information Security**

**Week 1: Risk Assessment and Information Discovery**

Week 1 Assignment: Analyze Potential Cybersecurity Risks (10 Points)

**Week 2: Risk Reduction Techniques for Perimeter Protection**

Week 2 Assignment 1: Describe the Importance of Risk Mitigation Strategies (5 Points)

Week 2 Assignment 2: Compare Popular Risk Management Frameworks (5 Points)

**Week 3: Information Security Governance**

Week 3 Assignment 1: Critique Advanced Persistent Threats (5 Points)

Week 3 Assignment 2: Develop a Model for Security Policies, Standards, and Procedures (5 Points)

**Section 2: Risk Reduction Strategies for Solutions Architecture**

**Week 4: Control Structure for Secure Database and Software Development**

Week 4 Assignment: Design a Control Model for Secure Development (10 Points)

**Week 5: Ethics and Cyber-Espionage Prevention and Management**

Week 5 Assignment 1: Analyze Threat Prevention and Response Solutions (5 Points)

Week 5 Assignment 2: Propose Strategies and Tools for Cloud Security (5 Points)

**Week 6: Vulnerability Assessments for Perimeter Protection**

Week 6 Assignment: Research Vulnerability Assessment Models and Frameworks (15 Points)

**Section 3: Managing Privacy in Information Security**

**Week 7: Mobile Computing and Master Data Management**

Week 7 Assignment: Benchmark MDM Software for BYOD Data Loss Prevention (10 Points)

**Week 8: Strategic Development of a Corporate Risk Management Strategy**

Week 8 Signature Assignment: Design a Corporate Risk Management Plan (25 Points)