Course Number: 95-755  
Information Security Risk Management I  
Units: 6

This course and its follow-on Information Security Risk Management II (95-756) examine information security as a risk management problem where the organization identifies information security risks, evaluates those risks, and makes risk mitigation and acceptance decisions given its resource constraints.

In part one of this class students will learn foundational concepts in risk management and economic valuation and will be introduced standard risk management approaches for identifying, analyzing, and responding to risk, as well as the tools and methodologies for metrics to monitor risk management activities.

Grading for this course consists of five short quizzes and a final project

Week 1 (January 14) – Risk Management Concepts – Week 1 will begin with overview of the Information Security Risk Management I class, including the syllabus, reading assignments, grading, and some basic course housekeeping. We will also cover some basic risk and risk management concepts and then start taking a broad look at the risk management as a lifecycle of activities that manage risk and preserve value for the organization.

Readings: To Be Announced (TBA)  
Assignment: None

Week 2 (January 21) – Threats, Vulnerabilities and Controls – Week 2 will be an in-depth examination of several key risk management concepts that will be foundational to understanding and practicing Information Risk Management. Each concept will augmented by practical.

Readings: TBA  
Assignment: Multiple choice quiz on required readings

Week 3 (January 28) – Risk Identification – In Week 3 we will examine the first phase of the risk management lifecycle, Risk Identification. This will begin with a broad look at the complexity of information security risk in the environment today. From this broad perspective, we will identify the values and assets at risk in the organization to create focus and priority on risks most important for each organization. Risk identification results in an informed risk profile of the organization and the inherent risks it faces.

Readings: TBA  
Assignment: Multiple choice quiz on required readings

Week 4 and 5 (February 4 and 11) – Risk Assessment Frameworks and Methods I and II – Weeks 4 and 5 will encompass the core activity of risk assessment, including the conceptual overview, tools and methods, and practical exercise of assessing risk in a variety information security and risk contexts. Information risk assessment requires a combination of process discipline, critical thinking and business context in order to consistently arrive on assessment results which are objective and meaningful.

Readings: TBA  
Assignments: Multiple choice quiz on required readings (Week 4)

Week 6 (February 18) – Risk Response – Week 6 will focus on the available options for responding to risk and the results of risk assessments, including risk transfer, risk mitigation and risk avoidance options. Particular emphasis will be placed on risk mitigation options, and the business value proposition (cost/benefit) of risk mitigation and remediation investments.

Readings: TBA  
Assignments: Multiple choice quiz on required readings

Week 7 (February 25) – Risk Monitoring and Metrics – Week 7 will explore the methods and approaches for monitoring risk, with an emphasis on quantitative/metrics-based approaches. This last step in the risk management lifecycle informs each previous step in order to inform and calibrate risk-based decisions to consistently improve the business value of risk management and provide transparency into the results of risk management activities.

Reading: TBA
Assignments: Multiple choice quiz on required readings

Week 8 (March 3) – Final Presentation Week – Week 8 students will submit their case study reports and perform short summary presentations