California State University, Northridge
College of Business & Economics
Department of Accounting & Information Systems

IS 497B: Information Security and Assurance
Reading Preparation Assignment
Management of Information Security
Chapter 9

Read Chapter 9, Risk Management: Controlling Risk, of the *Management of Information Security* textbook, pp. 313-337.

The following review questions will be used to lead class discussion. Note, while I feel that it is a good idea to write out the answers to these questions, please know that I will not be collecting them as homework.

1. List and define the five risk control strategies discussed in the book.
2. Describe residual risk.
3. What four types of controls or applications can be used to avoid risk?
4. Describe how outsourcing can be used for risk transference.
5. What conditions must be met to ensure that risk acceptance has been used properly?
6. What is risk appetite? Explain why risk appetite varies from organization to organization.
7. What is a cost-benefit analysis?
8. What is the difference between intrinsic value and acquired value? Why is the distinction important in risk management?
9. What is single loss expectancy? What is annual loss expectancy?
10. What is the difference between benchmarking and baselining?
11. What is the difference between organizational feasibility and operational feasibility?
12. What is the difference between qualitative measurement and quantitative measurement?
13. What is the OCTAVE Method? What does it provide to those who adopt it?
14. How does Microsoft define "risk management"? What phases are used in its approach?