IS 497B: Information Security and Assurance
Reading Preparation Assignment
Management of Information Security
Chapter 5

Read Chapter 5, Developing the Security Program, of the *Management of Information Security* textbook, pp. 161-206.

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. What is an information security program?
2. What functions constitute a complete information security program?
3. Where can an organization place the information security unit? Where should (and shouldn't) it be placed? What is the criteria that should determine where it is kept?
4. Into what four areas should the information security functions be divided?
5. What are the five roles that an information security professional can assume?
6. What are the three areas of the SETA program?
7. What can influence the effectiveness of a training program?
8. What are some of the various ways to implement an awareness program?
9. Which two documents largely determine the shape of the information security program? Which other documents can assist in this effort?
10. What are the elements of a security program, according to NIST SP 800-14?
11. Information security positions can be classified into what three areas? What are the differences among them?
12. Describe the two overriding benefits of awareness, training, and education.
13. What is the purpose of a SETA program?
14. Which of the SETA program's three elements is the organization best prepared to offer? Which should it consider outsourcing?
15. How does training differ from education? Which is provided to the broader audience with regard to information security?
16. What are the various training program delivery methods?
17. Describe a sample seven-step methodology for implementing training.
18. When developing an awareness program, what priorities should you keep in mind?