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 11

Read Chapter 11, Personnel and Security, of the *Management of Information Security* textbook, pp. 399-439.

The following review questions will be used to lead class discussion.

1. When an organization undertakes an InfoSec-driven review of job descriptions, which job descriptions must be reviewed? Which IT jobs not directly associated with information security should be reviewed?
2. List and describe the criteria for selecting InfoSec personnel.
3. What are some of the factors that influence an organization's hiring decisions?
4. What attributes do organizations seek in a candidate when hiring InfoSec professionals? Prioritize this list of attributes and justify your ranking.
5. What are the critical actions that management must consider taking when dismissing an employee? Do these issues change based on whether the departure is friendly or hostile?
6. How do the security considerations for temporary or contract workers differ from those for regular employees?
7. Which two career paths are the most commonly encountered as entrees into the InfoSec discipline? Are there other paths? If so, describe them.
8. Why is it important to have a body of standard job descriptions for hiring InfoSec professionals?
9. What functions does the CISO perform, and what are the key qualifications and requirements for the position?
10. What functions does the security manager perform, and what are the key qualifications and requirements for the position?
11. What functions does the security technician perform, and what are the key qualifications and requirements for the position?
12. What functions does the internal security consultant perform, and what are the key qualifications and requirements for the position?
13. What is the rationale for acquiring professional credentials?
14. List and describe the certification credentials available to InfoSec professionals.
15. In your opinion, who should pay for the expenses of certification? Under what circumstances would your answer be different? Why?
16. List and describe the standard personnel practices that are part of the InfoSec function. What happens to these practices when they are integrated with InfoSec concepts?
17. Why shouldn't you show a job candidate secure areas during interviews?
18. List and describe the types of nonemployee workers often used by organizations. What special security considerations apply to such workers, and why are they significant?
19. What is separation of duties? How can this method be used to improve an organization's InfoSec practices?
20. What is least privilege? Why is implementing least privilege important?

This document created and maintained by David W. Miller. ©2005-2014
The page was last updated on April 27, 2014.