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

IS 497B: Information Security and Assurance

Reading Preparation Assignment
Chapter 3

Read Chapter 3, Planning for Contingencies, of the *Management of Information Security* textbook, pp. 73-117.

Prepare for class discussion based on the following review questions:

1. What is the name for the broad process of planning for the unexpected? What are its primary components?
2. Which two communities of interest are usually associated with contingency planning? Which community must give authority to ensure broad support for the plans?
3. List the seven-step CP process recommended by NIST.
4. List and describe the teams that perform the planning and execution of the CP plans and processes. What is the primary role of each?
5. Define the term "incident" as used in the context of IRP. How is it related to the concept of incident response?
6. Describe the criteria used to determine whether an actual incident is occurring.
7. List and describe the sets of procedures used to detect, contain, and resolve an incident.
8. List and describe the IR planning steps.
9. List and describe the actions that should be taken during an incident response.
10. Describe the containment strategies given in the text. On which tasks do they focus?
11. What is an *incident damage assessment*? What is it used for?
12. What criteria should be used when considering whether or not to involve law enforcement agencies during an incident?
13. What is a *disaster recovery plan* and why is it important to the organization?
14. Describe a *rapid-onset disaster* and give an example. Describe a *slow-onset disaster* and give an example.
15. What is a *business continuity plan* and why is it important?
16. What is a *business impact analysis* and what is it used for?
17. Why should continuity plans be tested and rehearsed?

This document created and maintained by David W. Miller, PhD.
The page was last updated on February 7, 2014.