CSIT988/CSIT488 – "Security, Ethics and Professionalism"

Autumn 2025

Workshop 2

I. Quick Quiz

1. Which statement describes what an organization wants to become?
   A. Values statement
   B. Vision statement
   C. Mission statement
   D. Aspiration statement
   E. Commitment statement

2. Which statement describes what an organization does and for whom?
   A. Values statement
   B. Vision statement
   C. Mission statement
   D. Aspiration statement
   E. Commitment statement

3. True of False: Strategic planning lays out the long-term direction to be taken by an organization.

4. Which is higher up (i.e., closer to the strategic plan) in the planning chain: the tactical plan or the operational plan?

5. What are the elements of a strategic plan?

6. Which is NOT a benefit of InfoSec Governance?
   A. Increase in shareholder value
   B. Increased predictability of business operations
   C. Optimization of limited security resources
   D. Reduction in the total amount of private data needed to keep on file
   E. Reduction of impacts on information resources

7. True or False: One aspect of an InfoSec Governance framework is an InfoSec risk management methodology.

8. What is another name for the governance framework recommended by the CGTF (Corporate Governance Task Force)?

9. Which is more likely to succeed, a top-down or bottom-up approach to InfoSec planning?

10. What are the four major components of contingency planning?

11. Which is not a stage of Business Impact Analysis?
    A. Threat attack identification and prioritization
    B. Business unit analysis
    C. Potential damage assessment
    D. Policy plan classification
    E. Attack success scenario development

12. What is NOT a stage of Incident Response Planning?
    A. Incident Detection
    B. Incident Recovery
    C. Incident Planning
    D. Plan for Disaster Recovery
    E. Incident Reaction

13. Which plan is usually activated when an incident causes minimal damage, according to criteria set in advance by the organization, with little or no disruption to business operations?

14. True or False: Incident response is a preventative measure

15. A(n) ____ is a fully configured computer facility, with all services, communications links, and physical plant operations. It duplicates computing resources, peripherals, phone systems, applications, and workstations.

16. A(n) ____ is a contract between two organizations in which each party agrees to assist the other in the event of a disaster.

17. True or False: Warm site is a shared-use option when it comes to continuity strategies.

18. True or False: An incident is generally categorized as a disaster when the level of damage or destruction is too severe that the organization is unable to quickly recover.

19. What are the three categories of incident indicators, as identified by D.L. Pipkin?

20. List some strategies used for contingency plan testing.

II. Short-Answer Questions and Case Studies

1. What is planning? How does an organization determine if planning is necessary?

2. Search for examples of vision, mission and values statements from prominent organizations.

3. What is InfoSec governance? What are the five basic outcomes that should be achieved through InfoSec governance?

4. Describe top-down strategic planning. How does it differ from bottom-up strategic planning? Which is usually more effective in implementing security in a large, diverse organization?

5. Give examples of the common technical attacks mentioned in Lecture 03.

6. List and describe the teams that perform the planning and execution of the CP plans and processes. What is the primary role of each?

7. List and describe the sets of procedures used to detect, contain, and resolve an incident.

8. Give examples of disaster classification methods.

9. What is a business continuity plan, and why is it important?

10. When analyzing phishing attacks targeting a bank's customers, incident indicator can be categorized into Possible, Probable and Definite, based on Pipkin's classification. Provide examples of these categories.