CSIT988/CSIT488 – "Security, Ethics and Professionalism"

Autumn 2025

Workshop 3

I. Quick Quiz

1. In the bull's-eye model, the outer layer in the diagram represents _____.
   A. networks
   B. applications
   C. policies
   D. systems
   E. computers

2. True or False: Policy must be able to stand up in court if challenged.

3. Which of the following statements is false?
   A. Policies are sanctioned by management
   B. Standards are built on policy and carry the weight of the policy
   C. Practices, procedures and guidelines provide detailed steps to meet standards
   D. Policies drive standards
   E. Policies explain how employees will comply with practices

4. What is one of the three types of an information security policy?
   A. Enterprise information security policy
   B. Network information security policy
   C. Threat assessment information security policy
   D. Privacy information security policy
   E. Physical information security policy

5. What type of security policy provides detailed, targeted guidance to instruct all members of the organization in the use of a process, technology or system?

6. True or False: An ISSP should not require frequent updates.

7. True or False: For policies to be effective, they must be properly developed using industry-accepted practices.

8. What documents should be gathered or produced during the analysis phase of developing an information security policy?

9. What are some methods of policy distribution?

10. True or False: SysSPs can be separated into management guidance and technical specifications or combined in a single policy document.

11. Which of the following statements are false?
    Choose one or more:
    A. The policy development project can be guided by the SecSDLC process
    B. Policy documents must be written with numerous technical jargons and management terminologies
    C. Policy enforcement must be uniform and impartial
    D. One typical ISSP topic is the use of personal equipment on company networks
    E. EISP must not support the vision statement of the organization

12. What is the most influential variable affecting the structure of an information security program?
    A. Organizational size
    B. Organizational culture
    C. Security personnel budget
    D. Security capital budget (physical resources such as offices, computer labs)
    E. Security equipment

13. Which of the following are titles used by organizations for the equivalent role to the CISO (Chief Information Security Officer) position?
    A. Manager of Security
    B. Director of Security
    C. Security Analyst
    D. Security Technician
    E. Security Guard

14. True or False: Security technicians are the technically qualified individuals who configure firewalls and IDPSs (Intrusion Detection and Prevention Systems), implement security software, diagnose and troubleshoot problems, and coordinate with systems and networks administrators to ensure that security technology is properly implemented.

15. True or False: Security consultants are the “guards, gates and guns” aspect of security.

16. What are the three major benefits of a SETA program?

17. Wood suggested many options for positioning the InfoSec program within an organization. Which of the following options involve only one middle manager between the Information Security Department Manager and the Chief Executive Office?

A. Option 3: Administrative Services
B. Option 1: Information Technology
C. Option 5: Strategy and Planning
D. None of the other listed options
E. Option 2: Security

18. What are the advantages and disadvantages of the computer-based training (CBT) method?

19. What are the five ways to divide employees into groups for training?

20. True or False: Security awareness program is the most ineffective security methods.

II. Short-Answer Questions and Case Studies

1. Describe the bull's-eye model. What does it say about policy in the InfoSec program?

2. Is policy considered static or dynamic? Which factors might determine this status?

3. List and describe the three types of InfoSec policy as described by NIST SP 800-14. In your opinion, which is best suited for use by a smaller organization and why? If the target organization were very much larger, which approach would be more suitable and why?

4. List and describe four elements that should be present in the EISP.

5. List and describe three functions that the ISSP serves in the organization.

6. What is an InfoSec program? What functions constitute a complete InfoSec program?

7. List the options for reporting relationships of InfoSec within an organization, as described by Charles Wood.

8. What are the various delivery methods for training programs?

9. When developing an awareness program, what priorities should you keep in mind?

10. Study the materials provided at UOW's Cyber Training & Resources site: https://www.uow.edu.au/cyber-safety/training-resources/

    a. What are the IT security recommendations for personal devices?
    b. What are the common cyber threats, as identified by UOW, and how to avoid them?
    c. Describe and discuss Multi-Factor Authentication at UOW.