CSIT988/CSIT488 – "Security, Ethics and Professionalism"

Autumn 2025

Workshop 4

I. Quick Quiz

1. True or False: A security model is a concrete blueprint offered by a service organization.

2. What is a mandatory access control?

3. What are the two kinds of covert channels defined by TCSEC?

4. True or False: ISO 27002 is the successor of ISO 17799

5. True or False: ISO 27002 provides information on how to implement ISO 27001

6. What is another name for the Brewer-Nash model?

7. True or False: The Biba model ensures that no information from a subject can be passed on to an object in a higher security level.

8. What is NOT an inherent characteristic of access control?
   Choose one or more:

   A. Preventative
   B. Corrective
   C. Executive
   D. Detective
   E. Conservative

9. True or False: RBACs are tied to a particular assignment or responsibility

10. True or False: The Biba confidentiality model ensures no information from a subject can be passed on to an object in a higher security level

11. True or False: Two categories of benchmarks used in InfoSec are standard of due care and standard of due diligence.

12. True or False: The biggest barrier to benchmarking in InfoSec is the fact that many organizations often share results with other organizations.

13. True or False: Baselining is a practice related to benchmarking.

14. True or False: The document “SP 800-55 Rev. 1” provides performance measurement guide for InfoSec.

15. True or False: The InfoSec measurement development process recommended by NIST consists of 6 phases.

16. True or False: The InfoSec measurement program implementation process recommended by NIST consists of 6 phases.

17. What is NOT a step of NIST’s Risk Management Framework (RMF)?

    Select one or more:

    A. Categorize
    B. Assess
    C. Authorize
    D. Review
    E. Authenticate

18. True or False: Failure to demonstrate due care or due diligence can expose an organization to legal liability.

19. True or False: Companies with best practices are always the best in every area.

20. True or False: According to NIST SP 800-500, Rev. 1, one candidate of measurement is the percentage of users with access to shared accounts.

II. Short-Answer Questions and Case Studies

1. What is an InfoSec framework? What is an InfoSec blueprint? What is a security model?

2. What is access control? What are the essential processes of access control? What are the key principles on which access control is founded?

3. What are covert channels? Describe the two kinds of covert channels defined in TCSEC.

4. What are the common names for the following documents, what are their purposes and what resources do they provide?

    a. NIST SP 800-12, Rev. 1
    b. NIST SP 800-14
    c. NIST SP 800-18, Rev. 1
    d. NIST SP 800-30, Rev. 1

5. What is benchmarking? What is baselining and how does it differ from benchmarking?

6. What is the standard of due care? How does it relate to due diligence?

7. Provide examples in InfoSec, where:
   A. An organization has due care but not due diligence.
   B. An organization has due diligence but not due care.

8. What is a recommended security practice? When selecting recommended practices, what criteria should we use and what limitations should we keep in mind?

9. What are the 3 types of InfoSec performance measurement used in organizations? According to “SP 800-55 Rev.1”, what are the factors that must be considered during development and implementation of an InfoSec performance management program and what are the factors that are critical to the success of an InfoSec performance program?

10. Describe the cyclic six-step approach of the Risk Management Framework.