MIS5206 – Unit#3a Name:________________________

1. An information system (IS) auditor is reviewing a third-party agreement for a new cloud-based accounting service provider. Which of the following considerations is the MOST important with regard to the privacy of the accounting data?
    a. Data retention, backup and recovery
    [✓ b. Return or destruction of information]
    c. Network and intrusion detection
    d. A patch management process

2. During an IS risk assessment of a health care organization regarding protected health care information (PHI), an IS auditor interviews IS management. Which of the following findings from the interviews would be of MOST concern to the IS auditor?
    a. The organization does not encrypt all of its outgoing email messages
    [✓ b. Staff have to type "[PHI]" in the subject field of email messages to be encrypted]
    c. An individual's computer screen saver function is disabled
    d. Server configuration requires the user to change the password annually

3. Which of the following is the responsibility of information asset owners?
    a. Implementation of information security within applications
    [✓ b. Assignment of criticality levels to data]
    c. Implementation of access rules to data and programs
    d. Provision of physical and logical security for data

4. With the help of a security officer, granting access to data is the responsibility of:
    [✓ a. Data owners]
    b. Programmers
    c. Systems analysts
    d. Librarians

5. The FIRST step in data classification is to
    [✓ a. Establish ownership]
    b. Perform a criticality analysis
    c. Define access rules
    d. Create a data dictionary

6. Which of the following would MOST effectively reduce social engineering incidents?
    a. Security awareness training
    b. Increased physical security measures
    c. Email monitoring policy
    d. Intrusion detection system

7. Which of the following acts as a decoy to detect active Internet attacks?
    a. Honeypots
    b. Firewalls
    c. Trapdoors
    d. Traffic analysis

8. Which of the following is the BEST way for an IS auditor to determine the effectiveness of a security awareness and training program?
    a. Review the security training program
    b. Ask the security administrator
    c. Interview a sample of employees
    d. Review the security reminders to employees

9. As his company's Chief Information Security Officer (CISO), George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?
    a. threats x vulnerability X asset value = residual risk
    b. SLE x frequency = ALE, which is equal to residual risk
    c. (threats x vulnerability x asset value) x control gap = residual risk
    d. (total risk – asset value) x countermeasures = residual risk

10. Which of the following is not included in a risk assessment?
    a. Discontinuing activities that introduce risk
    b. Identifying assets
    c. Identifying threats
    d. Analyzing risk in order of cost or criticality

11. Which of the following choices BEST helps information owners to properly classify data?

    a. Understanding the technical controls that protect data
    b. Training on organizational policies and standards
    c. Use of an automated data leak prevention (DLP) tool
    d. Understanding which people need to access the data

12. Which of the following provides the MOST relevant information for proactively strengthening security settings?

    a. Bastion host
    b. Intrusion detection system (IDS)
    c. Honeypot
    d. Intrusion prevention system (IPS)

13. What is the BEST approach to mitigate the risk of a phishing attack?

    a. Implementation of an intrusion detection system (IDS)
    b. Assessment of web site security
    c. Strong authentication
    d. User education

14. The GREATEST benefit of having well-defined data classification policies and procedures is:

    a. A more accurate inventory of information assets
    b. A decreased cost of controls
    c. A reduced risk of inappropriate system access
    d. An improved regulatory compliance

15. The FIRST step in a successful attack to a system would be:

    a. Gathering information
    b. Gaining access
    c. Denying services
    d. Evading detection

16. Which of the following methods BEST mitigates the risk of disclosing confidential information through the use of social networking sites?

    a. Providing security awareness training
    b. Requiring a signed acceptable use policy
    c. Monitoring the use of social media
    d. Prohibiting the use of social media through network controls

17. The integrity of data is not related to which of the following?

    a. The modification of data without authorization
    b. Unauthorized manipulation or changes to data
    c. The intentional or accidental substitution of data
    d. The extraction of data to share with unauthorized entities

18. A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?
    a. The asset's value in the external marketplace
    b. The level of insurance required to cover the asset
    c. The initial and outgoing costs of purchasing, licensing, and supporting the asset
    d. The asset's value to the organization's production operations