**IT409 Final Review**

1. Which of the following is NOT an access control method?
   1. MAC
   2. RBAC
   3. DAC
   4. PAC.
2. This access control method is characterized by the information owner being responsible for assigning privileges to appropriate users:
   1. MAC
   2. RBAC
   3. DAC
   4. PAC.
3. This access control method is characterized by the position, not the person, being assigned an access level to data:
   1. MAC
   2. RBAC
   3. DAC
   4. PAC.
4. This access control method is used by the Federal Government in the USA:
   1. MAC
   2. RBAC
   3. DAC
   4. PAC.
5. Which of the following is NOT a direct risk from un-secure code?
   1. Denial of Service attack
   2. Social engineering attack
   3. Running commands on the web server that hosts the application
   4. Attack on data confidentiality
6. System maintenance is required because
   1. Code needs maintenance when it is used a lot
   2. Code needs more maintenance if more employees use it
   3. Actually, it is not needed. Once code is written and is secure, it should not be touched anymore.
   4. No code should remain static over the years
7. When is the best time to think about security when a new piece of code is written?
   1. At the end, once all the modules have been written
   2. After the users have had a chance to review the application
   3. At the beginning of the project
   4. After the application has been approved and authorized by the ISO
8. Retroactively injecting security into existing code at the end of a development project usually results in which of the following?
   1. A perfectly secure application
   2. Creating new vulnerabilities
   3. It cannot be done
   4. A complete and secure review of the code
9. What is the number one goal of a Disaster Recovery and Business Continuity plan?
   1. Litigation against the parties responsible for the loss of uptime
   2. Protecting the confidentiality of the data
   3. Reassuring the public that the situation is being handled
   4. The physical safety of all employees, visitors and clients
10. Which of the following components of a BCP is that one that addresses what should be done IMMEDIATELY after a disaster struck?
    1. Disaster Preparation
    2. Disaster Response
    3. Business Contingency
    4. First Response
11. Who is in charge of managing a disaster?
    1. The ISO
    2. The BC Team
    3. The CEO/President
    4. The Board of Directors or equivalent body
12. What is GLBA also known as?
    1. The Glass-Steagal act
    2. The Bank Holding Company Act
    3. The Bank and Insurance Act
    4. The Financial Modernization Act
13. Which title of the GLBA specifically addresses protecting both the privacy and security of financial information?
    1. Title 3
    2. Title 4
    3. Title 5
    4. Title 6
14. As it pertains to GLBA, what does NPI stand for?
    1. Non-public information
    2. Non-public personal information
    3. Non-private information
    4. Non-private personal information
15. As it pertains to GLBA, automotive dealers, check-cashing businesses and courier services, among many others, are referred to as:
    1. Companies that provide non-traditional services
    2. Companies that provide traditional services
    3. Fiduciary institutions
    4. Traditional lenders
16. Who enforces the GLBA?
    1. 8 different federal agencies and states
    2. The FDIC
    3. The FFIEC
    4. The Secretary of the Treasury
17. Which organization, according to the provisions of HIPAA, is mandated to develop and publish rules to implement the HIPAA administrative simplification requirements?
    1. The FDIC
    2. The Department of Health and Human Services
    3. The Office of the Attorney General
    4. The OCS
18. How many rule sets did the HHS publish?
    1. 2
    2. 3
    3. 4
    4. 5
19. When it comes to HIPAA, what does PHI stand for?
    1. Public Health Information
    2. Public Health Institution
    3. Protected Health Information
    4. Protected Health Institution
20. As it pertains to HIPAA, what is a covered entity?
    1. A medical patient protected by HIPAA
    2. A health care provider who must be compliant with HIPAA
    3. A health care provider who does NOT have to be compliant with HIPAA
    4. A medical patient NOT protected by HIPAA
21. As it pertains to HIPAA, what is the CIA triad?
    1. Confidentiality, Integrity, Availability
    2. Confidentiality, Integrity, Authentication
    3. Confidentiality, Integrity, Authorization
    4. Confidentiality, Integrity, Accountability
22. What is the first requirement set forth by the security management process part of HIPAA’s administrative safeguards?
    1. A penetration test
    2. A vulnerability assessment
    3. A risk assessment
    4. A disaster recovery assessment
23. Which of the following concerns educational institutions?
    1. FISMA
    2. FERPA
    3. SOX
    4. GLBA
24. Which of the following concerns publicly traded companies?
    1. FISMA
    2. FERPA
    3. SOX
    4. GLBA
25. Which of the following concerns federal agencies?
    1. FISMA
    2. FERPA
    3. SOX
    4. GLBA
26. Which of the following is not a focus of FISMA?
    1. Confidentiality
    2. Availability
    3. Assurance
    4. Authentication
27. According to FISMA, who is the focal point for information security?
    1. The CEO of each federal agency
    2. The CIO of Homeland Security
    3. The CIO of each federal agency
    4. The CIO of the NSA
28. NIST stands for
    1. National Institute of Standards and Technology
    2. National Institute of Security and Technology
    3. National Institute of Standards and Threats
    4. National Institute of Safeguards and Technology
29. FERPA is a federal law that protects which of the following?
    1. Private banking records
    2. Private health-related information
    3. Confidential information stored by publicly-traded companies
    4. Student records
30. Which of the following should employees be allowed to install on their company-owned computer?
    1. hardware
    2. software
    3. nothing
    4. anything
31. Which of the following is correct when it comes to monitoring employees’ use of the Internet?
    1. It is never acceptable to monitor employees’ use of the Internet
    2. Monitoring employees’ use of the Internet is a serious privacy laws violation
    3. It is acceptable to monitor employees’ use of the Internet if it is part of the acceptable use policy
    4. It is always acceptable to monitor employees’ use of the Internet