Domain 1 Questions

1. An information security policy does NOT usually include:

- [ ] a. authority for information security department
- [ ] b. guidelines for how to implement policy
- [ ] c. basis for data classification
- [ ] d. recognition of information as an asset of the organization

2. Which of the following is a realistic goal of every loss prevention program?

- [ ] a. Be 100% effective in preventing loss.
- [ ] b. Permit losses that aren't very important.
- [ ] c. Reduce losses to a pre-defined level that management can tolerate.
- [ ] d. Reduce losses to within 10% of a pre-defined level

3. When is it acceptable for management not to take action on an identified risk?

- [ ] a. When responsibility for the conditions that cause the risk to arise is outside their department
- [ ] b. When the cost of taking action outweighs the potential cost of the risk being realized.
- [ ] c. When risk reduction measures may affect the productivity of the business.
- [ ] d. Never - action should always be taken to reduce or eliminate an identified risk.

4. Which of the following MOST clearly indicates whether specific risk reduction controls should be implemented?

- [ ] a. Threat and vulnerability analysis
- [ ] b. Risk evaluation
- [ ] c. ALE calculation
- [ ] d. Countermeasure cost/benefit analysis

5. A newly assigned Risk Manager requests access to a file share containing corporate financial records. The access request is reviewed by the Chief Financial Officer who determines that access will be granted to only three files for one month. This principle is referred to as:

- [ ] a. Job rotation
- [ ] b. Least privilege
- [ ] c. Special privilege
- [ ] d. Separation of duties

6. One purpose of a security awareness program is to modify

- [ ] a. Employee's attitude and behaviors
- [ ] b. Management's approach
- [ ] c. Attitudes of employees with sensitive data
- [ ] d. Corporate attitudes about safeguarding data

7. Which of the following assures alignment of security functions and the organization's goals, missions and objectives?

- [ ] a. Governance oversight
- [ ] b. System security oversight
- [ ] c. Human resource oversight
- [ ] d. Business service oversight

8. The concept of "least privilege" involves:

- [ ] a. Individual accountability
- [ ] b. Access authentication
- [ ] c. Authorization levels
- [ ] d. Identification of users

9. Which is the FIRST step that should be considered in a penetration test?

- [ ] a. The approval of the change management control team
- [ ] b. The development of a detailed test plan
- [ ] c. The formulation of specific management objectives
- [ ] d. The communication process among team members

10. Under the principle of negligence, executives can be held liable for losses that result from system breaches if

- [ ] a. The company is a multi-national company
- [ ] b. They have not exercised due care protecting computing resources
- [ ] c. They have failed to properly insure computer resources against loss
- [ ] d. The company does not prosecute the hacker that caused the breach

11. If a company has no written policy notifying employees of its right to monitor network activity, what must it do to be in compliance with certain privacy laws or principles?

- [ ] a. Monitor only during off hours
- [ ] b. Obtain a search warrant prior to any monitoring
- [ ] c. Not capture any network traffic related to monitoring employee's activity
- [ ] d. Apply for a waiver from Interpol before monitoring

12. What are the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information related to?

- [ ] a. Privacy
- [ ] b. Secrecy
- [ ] c. Availability
- [ ] d. Reliability

13. Under which one of the following situations would a trash can fire be considered a disaster?

- [ ] a. The fire caused critical business systems to be disabled for longer than the Recovery Time Objective.
- [ ] b. The fire alarms went off and the building had to be evacuated.
- [ ] c. The trash can contained company sensitive documents.
- [ ] d. The fire spread beyond the trash can and the fire department had to be called.

14. Which of the following is LEAST likely to be required to quantify the impact associated with a potential disaster to a commercial enterprise?

- [ ] a. Identify the organization's key business functions
- [ ] b. Identify the computer systems critical to the survival of the organization.
- [ ] c. Estimate the financial impact a loss would have on the business based on how long an outage would last.
- [ ] d. Acquire information from government agencies about the likelihood of a natural disaster occurring.

15. Which of the following would BEST help an organization to gain a common understanding of functions that are critical to survival?

- [ ] a. Risk assessment
- [ ] b. Emergency response plan
- [ ] c. Disaster recovery plan
- [ ] d. Business impact analysis

16. Which of the following best defines a Business Impact Analysis (BIA)?

- [ ] a. It is the process of analyzing all business functions to determine the impact of an outage.
- [ ] b. It is the process of analyzing corporate functions, such as accounting, personnel, and legal to determine which functions must operate immediately following an outage.
- [ ] c. It is the process of documenting procedures and capabilities to sustain organizational essential functions at an alternate site.
- [ ] d. It is the process of documenting viable recovery options for each business unit in the event of an outage.

17. When conducting the business impact assessment, business processes are examined relative to all EXCEPT:

- [ ] a. Customer interruption impacts
- [ ] b. Embarassment of loss of confidence impacts
- [ ] c. Executive management disruption impacts
- [ ] d. Revenue loss potential impact

18. Which of the following defines the intent of a system security policy?

- [ ] a. A description of the settings that will provide the highest level of security
- [ ] b. A brief high-level statement defining what is and is not permitted in the operation of a system
- [ ] c. A definition of those items that must be denied on the system
- [ ] d. A listing of tools and applications that will be used to protect the system

19. An organizational information security strategy is incomplete without

- [ ] a. Recommendations for salary improvement of security professionals
- [ ] b. Addressing privacy and health care requirements of employees
- [ ] c. Alignment with organizational audit and marketing plans
- [ ] d. Incorporating input from organizational privacy and safety professionals

20. The organizational information security plan can

- [ ] a. Assure protection of organizational data and information
- [ ] b. Select the technology solutions to enhance organizational security effectiveness
- [ ] c. Identify potential risks to organizational employee behavior
- [ ] d. Align organizational data protection schemes to business goals

21. Which of these terms is MOST closely related to confidentiality?

- [ ] a. Reliability
- [ ] b. Need-to-know
- [ ] c. Auditability
- [ ] d. Trustworthiness

22. Which of these is the MOST important factor when considering the alignment between release a product and making it secure?

- [ ] a. Service level agreements
- [ ] b. Customer satisfaction
- [ ] c. Policy
- [ ] d. Profit

23. Which statement is MOST accurate in the majority of organizational structures?

- [ ] a. The Security Officer is responsible for ensuring that recommendations to executive management are full, accurate, and complete.
- [ ] b. The Security Officer accepts the risk of system failures
- [ ] c. The Security Officer reports to the Privacy Officer.
- [ ] d. The Security Officer is responsible for protection of business information assets.

24. Governance involves _____

- [ ] a. the regulations that affect a company within a state or country
- [ ] b. the risk management processes and procedures within a company
- [ ] c. the organizational structure that includes standards, procedures and policies
- [ ] d. the organizational chart that describes who reports to whom as defined for a company

25. Which of these Intellectual Property Law concepts is NOT a part of Contract Law?

- [ ] a. Commercial software
- [ ] b. Shareware
- [ ] c. Public domain
- [ ] d. Freeware

26. In order to determine whether encrypted messages can be sent between any two particular countries, which resource should be consulted?

- [ ] a. World Intellectual Property Office (WIPO)
- [ ] b. International Traffic in Arms Reductions (ITAR) Agreements
- [ ] c. Organization for Economic Cooperation and Development (OECD)
- [ ] d. Wassenaar Arrangement

27. Which of these is one of the Organization for Economic Cooperation and Development (OECD) guidelines on privacy?

- [ ] a. Personal data should be relevant to the purpose for which they are to be used
- [ ] b. Personal data might need to be protected by reasonable security safeguards as necessary
- [ ] c. The use of personal data does not need to be disclosed at any time
- [ ] d. There are no limits on the amount of personal data or the type of personal data that is collected.

28. Which of the following definitions is correct?

- [ ] a. RTO (Recovery Time Objective) is the amount of time it will take to recover all critical systems at an alternate site
- [ ] b. RPO (Recovery Point Objective) is a measure of tolerable data loss
- [ ] c. End of disaster is when all systems are recovered at the alternate site
- [ ] d. End of disaster declaration occurs when the Security Manager determines that the activation was false alarm

29. What is essential to get from an employee or contractor when they leave an organization?

- [ ] a. A non-disclosure agreement
- [ ] b. Their passwords
- [ ] c. His or her badge
- [ ] d. Any clothing items with the company logo

30. In risk analysis calculations, which of these statements is correct?

- [ ] a. When exposure factor (EF) is unknown it should be assumed to be zero
- [ ] b. Annual Rate of Occurrence (ARO) increases whenever Single Loss Expectancy (SLE) is greater than zero
- [ ] c. ALE (Annual Loss Expectancy) equals Asset Value (AV) times EF times ARO
- [ ] d. ALE equals AV times EF times SLE

31. Which of these is NOT an example of social engineering?

- [ ] a. Session hijacking
- [ ] b. Shoulder surfing
- [ ] c. Tailgating
- [ ] d. Baiting

32. Which of these statements is MOST likely to trigger a change in policy?

- [ ] a. Lack of compliance by staff
- [ ] b. Large number of approved exceptions
- [ ] c. Policy is short
- [ ] d. Policy contains metrics

33. A laptop with a medical database contains records of device sales, such as canes, walkers, braces and many sales are done during in-home visits. Recognizing that these items are covered under HIPAA, PIPEDA and other international equivalents what should be done to protect the company?

- [ ] a. All data must be encrypted
- [ ] b. Encryption is not required and due to the overhead of key management, is not warranted
- [ ] c. Encryption of Patient Identification Information (PII) alone is required, and each sales person must have a unique key
- [ ] d. Whole disk encryption is not required, but it is the easiest and safest solution

34. Which of these deals with international copyright agreements?

- [ ] a. ISO 27000
- [ ] b. The Wassenaar Arrangement
- [ ] c. The Montreal Protocol
- [ ] d. WIPO

35. Closed-circuit camera feeds and recordings are commonly used as all of these EXCEPT for which of the following?

- [ ] a. A deterrent control
- [ ] b. A detective control
- [ ] c. A corrective control
- [ ] d. A preventive control

36. A compensating control is _____

- [ ] a. a control put in place when another control is suspended or disabled
- [ ] b. a control put in place to overcome the shortcomings of another control
- [ ] c. a control put in place that automatically continues to protect the system when the primary control fails
- [ ] d. a control that compensates for law enforcement or management's lack of technical skills

37. Copyright protects _____

- [ ] a. a symbol that represents an idea
- [ ] b. a proprietary process or procedure
- [ ] c. the expression of an idea
- [ ] d. the idea itself

38. As an employee of an investment bank, you have just completed programming on a highly profitable automated stock trading program. You decide to copy it onto a writable CD and then use the program at home for your friends and family, but do not charge anyone fees. Which of the following statements apply?

- [ ] a. The employer owns the copyright since it is work for hire, but you may use it if you don't charge anyone for it, under fair use principles
- [ ] b. The employer owns the copyright since it is work for hire so you many not use it under any circumstances without permission
- [ ] c. As author you own the copyright and may use it any way you wish
- [ ] d. You and the employer share the copyright and you may use it if you don't charge anyone for it