Domain 2 Questions

1. Who is ultimately responsible to ensure that information is categorized and that specific protective measures are taken?

- [ ] a. Security Officer
- [ ] b. Senior Management
- [ ] c. Data Owner
- [ ] d. Custodian

2. Data classification may assist an organization in:

- [ ] a. Eliminating regulatory mandates
- [ ] b. Lowering of accountability of data classifiers
- [ ] c. Reducing costs for protecting data
- [ ] d. Normalization of databases

3. Which one of the following could be a challenge when attempting to classify data?

- [ ] a. Making users aware that the organization is committed to protecting information from unauthorized access.
- [ ] b. Providing the identification of information that is considered to be critical for the business success.
- [ ] c. If integrity is a concern, classification can identify data that must only be modified in authorized ways.
- [ ] d. Accurate classification depends on the ability and knowledge of the classifier.

4. What is the first step in information protection?

- [ ] a. Information classification
- [ ] b. Information identification
- [ ] c. Information backup
- [ ] d. Information flow diagrams

5. What is the characteristic of a trusted process where users are granted restricted access to sensitive data?

- [ ] a. Confined domain
- [ ] b. Need-to-know
- [ ] c. Restricted resource
- [ ] d. Validated execution

6. The greater risk to most organizations through portable computing is:

- [ ] a. Loss of expensive hardware
- [ ] b. Vulnerability of remote access
- [ ] c. Loss of confidential data
- [ ] d. Tracking and inventory of equipment

7. An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media of other magnetic media is called

- [ ] a. A magnetic field
- [ ] b. A degausser
- [ ] c. Magnetic remanence
- [ ] d. Magnetic saturation

8. Fault-tolerance requirements are based on

- [ ] a. Mean Time Between Failures (MTBF)
- [ ] b. Memorandum of Understanding (MOU)
- [ ] c. Maximum Tolerable Downtime (MDT)
- [ ] d. Mandatory Access Control (MAC)

9. All of the following methods ensure that data is unreadable EXCEPT

- [ ] a. Writing random data over the old file
- [ ] b. Physical alteration of media
- [ ] c. Degaussing the disk or tape
- [ ] d. Removing the volume header information

10. In Mandatory Access Control the need-to-know element is provided by the:

- [ ] a. Operating system
- [ ] b. Information Owner
- [ ] c. Security Administrator
- [ ] d. System Administrator

11. The purpose of an information classification system is to _____

- [ ] a. comply with governmental regulation
- [ ] b. give data the appropriate level of protection
- [ ] c. enforce the need-to-know concept
- [ ] d. ensure that only those people with proper clearance can gain access to data

12. Which of the following is the MOST accurate statement with respect to categorization?

- [ ] a. A system with higher categorization than it needs is an acceptable error.
- [ ] b. A system with lower categorization than it needs is an acceptable error.
- [ ] c. Categorization is part of a company's overall risk management strategy
- [ ] d. Categorization is simply another word for classification.

13. Which of the following is most often missing from classification policies, standards and procedures?

- [ ] a. Penalties for unauthorized disclosure
- [ ] b. Methods for keeping data secure
- [ ] c. Ways to determine which level (eg. Secret, confidential) to apply to a data item
- [ ] d. Declassification of information procedures

14. What is the difference between the information owner and the data custodian?

- [ ] a. There is no difference, the terms are used interchangeably
- [ ] b. The information owner classifies the data, the data custodian creates, uses and eventually destroys it
- [ ] c. The data custodian classifies the data, the information owner creates, uses and eventually destroys it
- [ ] d. The information owner creates, classifies, uses and eventually destroys the data. The data custodian stores it, backs it up, restores it on demand and otherwise protects its availability.

15. Data storage in the cloud is increasingly popular. What is the BEST way to deal with data remanence for the data?

- [ ] a. Encrypt with and destroy the key
- [ ] b. Create a strong Service Level Agreement (SLA)
- [ ] c. Audit the cloud provider
- [ ] d. Overwrite the data with nonsense bytes

16. What is the BEST way to delete data on a solid state drive?

- [ ] a. Use the manufacturer's crypto-erase function
- [ ] b. Use the manufacturer's built-in sanitization commands
- [ ] c. Use multiple overwrite passes that contain enough data to fill the disk
- [ ] d. Physically destroy the disk

17. If there is no law or regulation dictating the answer, how long should a company retain data?

- [ ] a. Management may set its own policy
- [ ] b. Management should refer to the ISO standards on record retention and treat them as a maximum
- [ ] c. Management should refer to the ISO standards on record retention and treat them as a minimum
- [ ] d. Management should follow industry standard practices

18. The MOST important reason to adopt a cyber-security framework is _____

- [ ] a. it is required by law.
- [ ] b. it will help identify the gap between current state and desired state.
- [ ] c. it will assess progress as a company moves toward the desired state.
- [ ] d. it will help lower the overall risk profile of the organization.

19. Loss of a thumb drive can disclose confidential data. Which of the following is the BEST way to protect against that loss?

- [ ] a. File encryption software
- [ ] b. Media encryption software
- [ ] c. Self encrypting drives
- [ ] d. In transit encrypting technologies

20. The EU courts support "the right to be forgotten". The court's jurisdiction applies unless which of these conditions are met?

- [ ] a. The data is stored outside the EU, the person is an EU citizen or resident, but the data are available inside the EU
- [ ] b. The data are stored outside the EU, the person is an EU citizen or resident, but the data are unavailable inside the EU
- [ ] c. The data is stored outside the EU, the person is not an EU citizen or resident, and the data are unavailable inside the EU
- [ ] d. The data is stored inside the EU, the person is not an EU citizen or resident, and the data are unavailable inside the EU

21. Who or what defines the classifications of corporate data?

- [ ] a. the security administrator
- [ ] b. the system administrator
- [ ] c. the data/information owner
- [ ] d. the security policy

22. In a discretionary access control environment, need-to-know is part of _____

- [ ] a. classification
- [ ] b. clearance
- [ ] c. categorization
- [ ] d. certification

23. The BEST definition of data remanence is

- [ ] a. deleted data on disks that have not yet been overwritten
- [ ] b. data remaining after erasure
- [ ] c. data on cloud provider's storage systems after deletion by data owner
- [ ] d. data that have been declared obsolete but have not yet been destroyed

24. Which of the following statements MOST accurately describes what a data classification policy should include?

- [ ] a. Who has access to the data, how the data will be secured, where the data originated
- [ ] b. Who has access to the data, how the data will be secured, whether the data should be encrypted
- [ ] c. How to dispose of the data, whether the data should be encrypted, whether the data are of foreign origin
- [ ] d. How to secure the data, who can use the data, and what are the fines for misuse of the data

25. Of the choices below, which are the three BEST mechanisms for maintaining confidentiality?

- [ ] a. data classification, encryption, and destruction
- [ ] b. Clustering, server backups, and purging
- [ ] c. Data classification, quality assurance, and degaussing
- [ ] d. Server backups, encryption, and training

26. Which of the following is NOT a primary enabler of data management success?

- [ ] a. Ensuring that the data owner and the data custodian share the same duties
- [ ] b. Organizational alignment and defined data handling processes
- [ ] c. Scalable technologies and infrastructure
- [ ] d. A single centralized and relational repository

27. Which statement below is MOST correct?

- [ ] a. The data custodian creates the data and makes it available to users when they need it
- [ ] b. The data owner classifies the data and sets rules for user privileges, then delegates the day-to-day maintenance to the data custodian
- [ ] c. The data owner provides permissions to the data based on users' need-to-know, and the data custodian implements the classifications
- [ ] d. The data custodian provides user permissions and access to the data after the data owner has secured the data

28. Which of the following is considered Payment Card Industry (PCI) data?

- [ ] a. Job title
- [ ] b. Marital status
- [ ] c. Educational background
- [ ] d. Primary Account Number

29. Which is NOT a common activity undertaken during the data life cycle?

- [ ] a. Sanitizing the data upon receiving it
- [ ] b. Acquiring the data and putting it to use
- [ ] c. Decommissioning and disposing of the data
- [ ] d. Defining data requirements

30. Which of the following would BEST improve the quality of data?

- [ ] a. Anonymizing all incoming data to avoid data leakage
- [ ] b. Using data quality, validation, and verification techniques
- [ ] c. Doing a yearly audit of all financial data
- [ ] d. Metadata, improving data quality by making the data more accurate.

31. Of the techniques listed below, which of the following is the BEST method for erasing information on a hard disk drive (HDD)?

- [ ] a. Deleting files and then emptying the recycle bin.
- [ ] b. High level Operating System re-formatting.
- [ ] c. Multiple rounds of zero-one bit overwriting.
- [ ] d. Low level re-formatting.

32. Which statement below about the use of baselines in Asset Management is LEAST accurate?

- [ ] a. A common organizational practice is to combine many baseline ideas into one large overarching baseline.
- [ ] b. To create an effective baseline, you need to know what parts of the organization can be protected with the same baseline.
- [ ] c. Baselines help establish a minimum set of controls with which to protect some or all IT systems in the enterprise.
- [ ] d. Sets of baseline safeguards can be found in international, national, or industry standards.

33. Which statement below about implementing controls is LEAST accurate?

- [ ] a. Supplementation involves adding details to adequately meet the risk management needs of an organization.
- [ ] b. Scoping provides an organization with general ideas about implementing controls.
- [ ] c. Scoping provides an organization with specific terms and conditions about implementing controls.
- [ ] d. Tailoring helps an organization fine-tune their chosen controls so that they better fit their intended situations.

34. Which of the following answers is NOT one of the Center for Strategic and International Studies (CSIS) five critical security tenets?

- [ ] a. Prioritization - invest first in the controls that will give you the greatest benefit
- [ ] b. Metrics - allow required adjustments to be more quickly known and fixes implemented
- [ ] c. Continuous Monitoring - test and validate the effectiveness of your controls
- [ ] d. Accuracy - keep an accurate, up-to-date count of current threats.