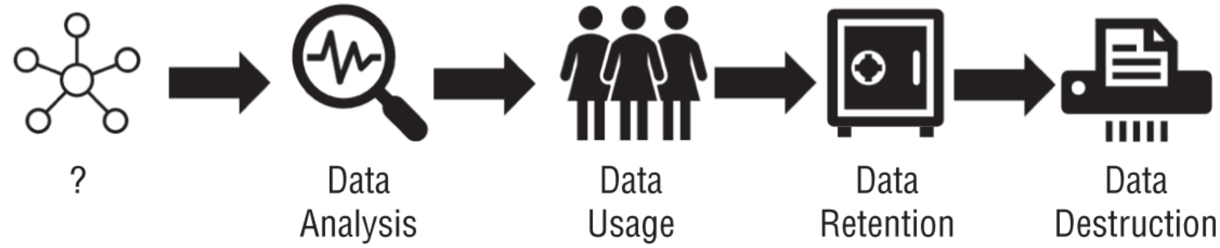
# Chapter 2
# Asset Security (Domain 2)

**SUBDOMAINS:**

- 2.1 Identify and classify information and assets
- 2.2 Establish information and asset handling requirements
- 2.3 Provision resources securely
- 2.4 Manage data lifecycle
- 2.5 Ensure appropriate asset retention (e.g. End-of-Life (EOL), End-of-Support (EOS))
- 2.6 Determine data security controls and compliance requirements

1. Angela is an information security architect at a bank and has been assigned to ensure that transactions are secure as they traverse the network. She recommends that all transactions use TLS. What threat is she most likely attempting to stop, and what method is she most likely using to protect against it?
    1. Man-in-the-middle, VPN
    2. Packet injection, encryption
    3. Sniffing, encryption
    4. Sniffing, TEMPEST
2. Control Objectives for Information and Related Technology (COBIT) is a framework for information technology (IT) management and governance. Which data management role is most likely to select and apply COBIT to balance the need for security controls against business requirements?
    1. Business owners
    2. Data processors
    3. Data owners
    4. Data stewards
3. Nadia's company is operating a hybrid cloud environment with some on-site systems and some cloud-based systems. She has satisfactory monitoring on-site, but needs to apply security policies to both the activities her users engage in and to report on exceptions with her growing number of cloud services. What type of tool is best suited to this purpose?
    1. A NGFW
    2. A CASB
    3. An IDS
    4. A SOAR
4. When media is labeled based on the classification of the data it contains, what rule is typically applied regarding labels?
    1. The data is labeled based on its integrity requirements.
    2. The media is labeled based on the highest classification level of the data it contains.
    3. The media is labeled with all levels of classification of the data it contains.
    4. The media is labeled with the lowest level of classification of the data it contains.

5. Which one of the following administrative processes assists organizations in assigning appropriate levels of security control to sensitive information?
    1. Data classification
    2. Remanence
    3. Transmitting data
    4. Clearing
6. How can a data retention policy help to reduce liabilities?
    1. By ensuring that unneeded data isn't retained
    2. By ensuring that incriminating data is destroyed
    3. By ensuring that data is securely wiped so it cannot be restored for legal discovery
    4. By reducing the cost of data storage required by law
7. Staff in an information technology (IT) department who are delegated responsibility for day-to-day tasks hold what data role?
    1. Business owner
    2. User
    3. Data processor
    4. Custodian
8. Helen's company uses a simple data lifecycle as shown in the figure here. What stage should come first in their data lifecycle?



    1. Data policy creation
    2. Data labeling
    3. Data collection
    4. Data analysis
9. Ben has been tasked with identifying security controls for systems covered by his organization's information classification system. Why might Ben choose to use a security baseline?
    1. It applies in all circumstances, allowing consistent security controls.
    2. They are approved by industry standards bodies, preventing liability.
    3. They provide a good starting point that can be tailored to organizational needs.
    4. They ensure that systems are always in a secure state.
10. Megan wants to prepare media to allow for its reuse in an environment operating at the same sensitivity level. Which of the following is the best option to meet her needs?
    1. Clearing
    2. Erasing
    3. Purging
    4. Sanitization
11. Mikayla wants to identify data that should be classified that already exists in her environment. What type of tool is best suited to identifying data like Social Security numbers, credit card numbers, and similar well-understood data formats?
    1. Manual searching

2. A sensitive data scanning tool
3. An asset metadata search tool
4. A data loss prevention system (DLP)

12. What issue is common to spare sectors and bad sectors on hard drives as well as overprovisioned space on modern SSDs?
    1. They can be used to hide data.
    2. They can only be degaussed.
    3. They are not addressable, resulting in data remanence.
    4. They may not be cleared, resulting in data remanence.
13. Naomi knows that commercial data is typically classified based on different criteria than government data. Which of the following is not a common criterion for commercial data classification?
    1. Useful lifespan
    2. Data value
    3. Impact to national security
    4. Regulatory or legal requirements

For questions 14–16, please refer to the following scenario:

Your organization regularly handles three types of data: information that it shares with customers, information that it uses internally to conduct business, and trade secret information that offers the organization significant competitive advantages. Information shared with customers is used and stored on web servers, while both the internal business data and the trade secret information are stored on internal file servers and employee workstations.

14. What term best describes data that is resident in system memory?
    1. Data at rest
    2. Buffered data
    3. Data in use
    4. Data in motion
15. What technique could you use to mark your trade secret information in case it was released or stolen and you need to identify it?
    1. Classification
    2. Symmetric encryption
    3. Watermarks
    4. Metadata
16. What type of encryption is best suited for use on the file servers for the proprietary data, and how might you secure the data when it is in motion?
    1. TLS at rest and AES in motion
    2. AES at rest and TLS in motion
    3. VPN at rest and TLS in motion
    4. DES at rest and AES in motion
17. What does labeling data allow a DLP system to do?
    1. The DLP system can detect labels and apply appropriate protections based on rules.

2. The DLP system can adjust labels based on changes in the classification scheme.
3. The DLP system can modify labels to permit requested actions.
4. The DLP system can delete unlabeled data.

18. Why is it cost effective to purchase high-quality media to contain sensitive data?
    1. Expensive media is less likely to fail.
    2. The value of the data often far exceeds the cost of the media.
    3. Expensive media is easier to encrypt.
    4. More expensive media typically improves data integrity.
19. Chris is responsible for workstations throughout his company and knows that some of the company's workstations are used to handle both proprietary information and highly sensitive trade secrets. Which option best describes what should happen at the end of their life (EOL) for workstations he is responsible for?
    1. Erasing
    2. Clearing
    3. Sanitization
    4. Destruction
20. Fred wants to classify his organization's data using common labels: private, sensitive, public, and proprietary. Which of the following should he apply to his highest classification level based on common industry practices?
    1. Private
    2. Sensitive
    3. Public
    4. Proprietary
21. What scenario describes data at rest?
    1. Data in an IPsec tunnel
    2. Data in an e-commerce transaction
    3. Data stored on a hard drive
    4. Data stored in RAM
22. If you are selecting a security standard for a Windows 10 system that processes credit cards, what security standard is your best choice?
    1. Microsoft's Windows 10 security baseline
    2. The CIS Windows 10 baseline
    3. PCI DSS
    4. The NSA Windows 10 Secure Host Baseline

For questions 23–25, please refer to the following scenario:

The Center for Internet Security (CIS) works with subject matter experts from a variety of industries to create lists of security controls for operating systems, mobile devices, server software, and network devices. Your organization has decided to use the CIS benchmarks for your systems. Answer the following questions based on this decision.

23. The CIS benchmarks are an example of what practice?
    1. Conducting a risk assessment
    2. Implementing data labeling
    3. Proper system ownership

    4. Using security baselines
24. Adjusting the CIS benchmarks to your organization's mission and your specific IT systems would involve what two processes?
    1. Scoping and selection
    2. Scoping and tailoring
    3. Baselining and tailoring
    4. Tailoring and selection
25. How should you determine which controls from the baseline should be applied to a given system or software package?
    1. Consult the custodians of the data.
    2. Select based on the data classification of the data it stores or handles.
    3. Apply the same controls to all systems.
    4. Consult the business owner of the process the system or data supports.
26. The company that Henry works for operates in the EU and collects data about their customers. They send that data to a third party to analyze and provide reports to help the company make better business decisions. What term best describes the third-party analysis company?
    1. The data controller
    2. The data owner
    3. The data subject
    4. The data processor
27. The government defense contractor that Selah works for has recently shut down a major research project and is planning on reusing the hundreds of thousands of dollars of systems and data storage tapes used for the project for other purposes. When Selah reviews the company's internal processes, she finds that she can't reuse the tapes and that the manual says they should be destroyed. Why isn't Selah allowed to degauss and then reuse the tapes to save her employer money?
    1. Data permanence may be an issue.
    2. Data remanence is a concern.
    3. The tapes may suffer from bitrot.
    4. Data from tapes can't be erased by degaussing.
28. Information maintained about an individual that can be used to distinguish or trace their identity is known as what type of information?
    1. Personally identifiable information (PII)
    2. Personal health information (PHI)
    3. Social Security number (SSN)
    4. Secure identity information (SII)
29. Which of the following information security risks to data at rest would result in the greatest reputational impact on an organization?
    1. Improper classification
    2. Data breach
    3. Decryption
    4. An intentional insider threat
30. Full disk encryption like Microsoft's BitLocker is used to protect data in what state?
    1. Data in transit
    2. Data at rest

3. Unlabeled data
4. Labeled data

31. The company that Katie works for provides its staff with mobile phones for employee use, with new phones issued every two years. What scenario best describes this type of practice when the phones themselves are still usable and receiving operating system updates?
    1. EOL
    2. Planned obsolescence
    3. EOS
    4. Device risk management
32. What is the primary purpose of data classification?
    1. It quantifies the cost of a data breach.
    2. It prioritizes IT expenditures.
    3. It allows compliance with breach notification laws.
    4. It identifies the value of the data to the organization.
33. Fred's organization allows downgrading of systems for reuse after projects have been finished and the systems have been purged. What concern should Fred raise about the reuse of the systems from his Top Secret classified project for a future project classified as Secret?
    1. The Top Secret data may be commingled with the Secret data, resulting in a need to relabel the system.
    2. The cost of the sanitization process may exceed the cost of new equipment.
    3. The data may be exposed as part of the sanitization process.
    4. The organization's DLP system may flag the new system due to the difference in data labels.
34. Which of the following concerns should not be part of the decision when classifying data?
    1. The cost to classify the data
    2. The sensitivity of the data
    3. The amount of harm that exposure of the data could cause
    4. The value of the data to the organization
35. Which of the following is the least effective method of removing data from media?
    1. Degaussing
    2. Purging
    3. Erasing
    4. Clearing

For questions 36–38, please refer to the following scenario:

The healthcare company that Amanda works for handles HIPAA data as well as internal business data, protected health information, and day-to-day business communications. Its internal policy uses the following requirements for securing HIPAA data at rest and in transit.

| Classification | Handling Requirements |
|---|---|
| Confidential (HIPAA) | Encrypt at rest and in transit. |

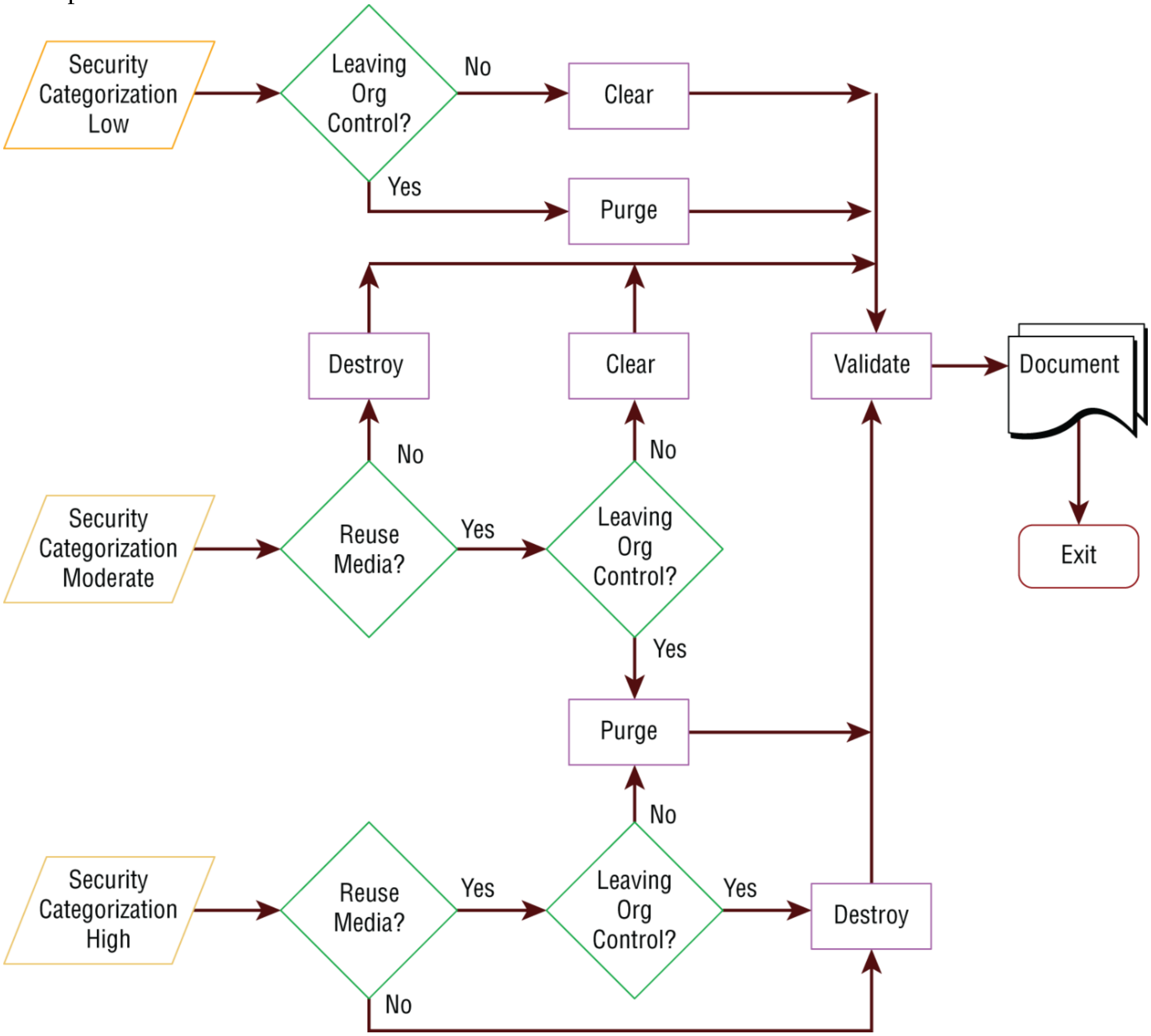
| Classification | Handling Requirements |
|---|---|
| | Full disk encryption is required for all workstations. |
| | Files can only be sent in encrypted form, and passwords must be transferred under separate cover. |
| | Printed documents must be labeled with “HIPAA handling required.” |
| Private (PHI) | Encrypt at rest and in transit. |
| | PHI must be stored on secure servers, and copies should not be kept on local workstations. |
| | Printed documents must be labeled with “Private.” |
| Sensitive (business confidential) | Encryption is recommended but not required. |
| Public | Information can be sent unencrypted. |

36. What encryption technology would be appropriate for HIPAA documents in transit?
    1. BitLocker
    2. DES
    3. TLS
    4. SSL
37. Amanda's employer asks Amanda to classify patient X-ray data that has an internal patient identifier associated with it but does not have any way to directly identify a patient. The company's data owner believes that exposure of the data could cause damage (but not exceptional damage) to the organization. How should Amanda classify the data?
    1. Public
    2. Sensitive
    3. Private
    4. Confidential
38. What technology could Amanda's employer implement to help prevent confidential data from being emailed out of the organization?
    1. DLP
    2. IDS
    3. A firewall
    4. UDP
39. Jacob's organization uses the US government's data classification system, which includes Top Secret, Secret, Confidential, and Unclassified ratings (from most sensitive to least). Jacob encounters a system that contains Secret, Confidential, and Top Secret data. How should it be classified?
    1. Top Secret
    2. Confidential
    3. Secret
    4. Mixed classification

40. Elle is planning her organization's asset retention efforts and wants to establish when the company will remove assets from use. Which of the following is typically the last event in a manufacturer or software provider's lifecycle?
    1. End of life
    2. End of support
    3. End of sales
    4. General availability
41. Amanda has been asked to ensure that her organization's controls assessment procedures match the specific systems that the company uses. What activity best matches this task?
    1. Asset management
    2. Compliance
    3. Scoping
    4. Tailoring
42. Chris is responsible for his organization's security standards and has guided the selection and implementation of a security baseline for Windows PCs in his organization. How can Chris most effectively make sure that the workstations he is responsible for are being checked for compliance and that settings are being applied as necessary?
    1. Assign users to spot-check baseline compliance.
    2. Use Microsoft Group Policy.
    3. Create startup scripts to apply policy at system start.
    4. Periodically review the baselines with the data owner and system owners.
43. Frank is reviewing his company's data lifecycle and wants to place appropriate controls around the data collection phase. Which of the following ensures that data subjects agree to the processing of their data?
    1. Retention
    2. Consent
    3. Certification
    4. Remanence
44. As a DBA, Amy's data role in her organization includes technical implementations of the data policies and standards, as well as managing the data structures that the data is stored in. What data role best fits what Amy does?
    1. Data custodian
    2. Data owner
    3. Data processor
    4. Data user
45. The company Jim works for suffered from a major data breach in the past year and now wants to ensure that it knows where data is located and if it is being transferred, is being copied to a thumb drive, or is in a network file share where it should not be. Which of the following solutions is best suited to tagging, monitoring, and limiting where files are transferred to?
    1. DRM
    2. DLP
    3. A network IPS
    4. Antivirus
46. What security measure can provide an additional security control in the event that backup tapes are stolen or lost?

    1. Keep multiple copies of the tapes.
    2. Replace tape media with hard drives.
    3. Use appropriate security labels.
    4. Use AES-256 encryption.
47. Joe works at a major pharmaceutical research and development company and has been tasked with writing his organization's data retention policy. As part of its legal requirements, the organization must comply with the US Food and Drug Administration's Code of Federal Regulations Title 21. To do so, it is required to retain records with electronic signatures. Why would a signature be part of a retention requirement?
    1. It ensures that someone has reviewed the data.
    2. It provides confidentiality.
    3. It ensures that the data has been changed.
    4. It validates who approved the data.
48. Susan wants to manage her data's lifecycle based on retention rules. What technique can she use to ensure that data that has reached the end of its lifecycle can be identified and disposed of based on her organization's disposal processes?
    1. Rotation
    2. DRM
    3. DLP
    4. Tagging
49. Ben has been asked to scrub data to remove data that is no longer needed by his organization. What phase of the data lifecycle is Ben most likely operating in?
    1. Data retention
    2. Data maintenance
    3. Data remanence
    4. Data collection
50. Steve is concerned about the fact that employees leaving his organization were often privy to proprietary information. Which one of the following controls is most effective against this threat?
    1. Sanitization
    2. NDAs
    3. Clearing
    4. Encryption
51. Alex works for a government agency that is required to meet US federal government requirements for data security. To meet these requirements, Alex has been tasked with making sure data is identifiable by its classification level when it is created. What should Alex do to the data?
    1. Classify the data.
    2. Encrypt the data.
    3. Label the data.
    4. Apply DRM to the data.
52. Ben is following the National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines for sanitization and disposition as shown here. He is handling information that his organization classified as sensitive, which is a moderate security categorization in the NIST model. If the media is going to be sold as surplus,

what process does Ben need to follow?



Source: NIST SP 800-88.

1. Destroy, validate, document
2. Clear, purge, document
3. Purge, document, validate
4. Purge, validate, document

53. What methods are often used to protect data in transit?
    1. Telnet, ISDN, UDP
    2. BitLocker, FileVault
    3. AES, Serpent, IDEA
    4. TLS, VPN, IPsec

54. Which one of the following data roles bears ultimate organizational responsibility for data?
    1. System owners

2. Business owners
3. Data owners
4. Mission owners

55. Shandra wants to secure an encryption key. Which location would be the most difficult to protect, if the key was kept and used in that location?
    1. On a local network
    2. On disk
    3. In memory
    4. On a public network

For questions 56–58, please refer to the following scenario:

Chris has recently been hired into a new organization. The organization that Chris belongs to uses the following classification process:

5. Criteria are set for classifying data.
6. Data owners are established for each type of data.
7. Data is classified.
8. Required controls are selected for each classification.
9. Baseline security standards are selected for the organization.
10. Controls are scoped and tailored.
11. Controls are applied and enforced.
12. Access is granted and managed.

56. If Chris is one of the data owners for the organization, what steps in this process is he most likely responsible for?
    1. He is responsible for steps 3, 4, and 5.
    2. He is responsible for steps 1, 2, and 3.
    3. He is responsible for steps 5, 6, and 7.
    4. All of the steps are his direct responsibility.
57. Chris manages a team of system administrators. What data role are they fulfilling if they conduct steps 6, 7, and 8 of the classification process?
    1. They are system owners and administrators.
    2. They are administrators and custodians.
    3. They are data owners and administrators.
    4. They are custodians and users.
58. If Chris's company operates in the European Union and has been contracted to handle the data for a third party, what role is his company operating in when it uses this process to classify and handle data?
    1. Business owners
    2. Mission owners
    3. Data processors
    4. Data administrators

For questions 59–62, please refer to the following scenario:

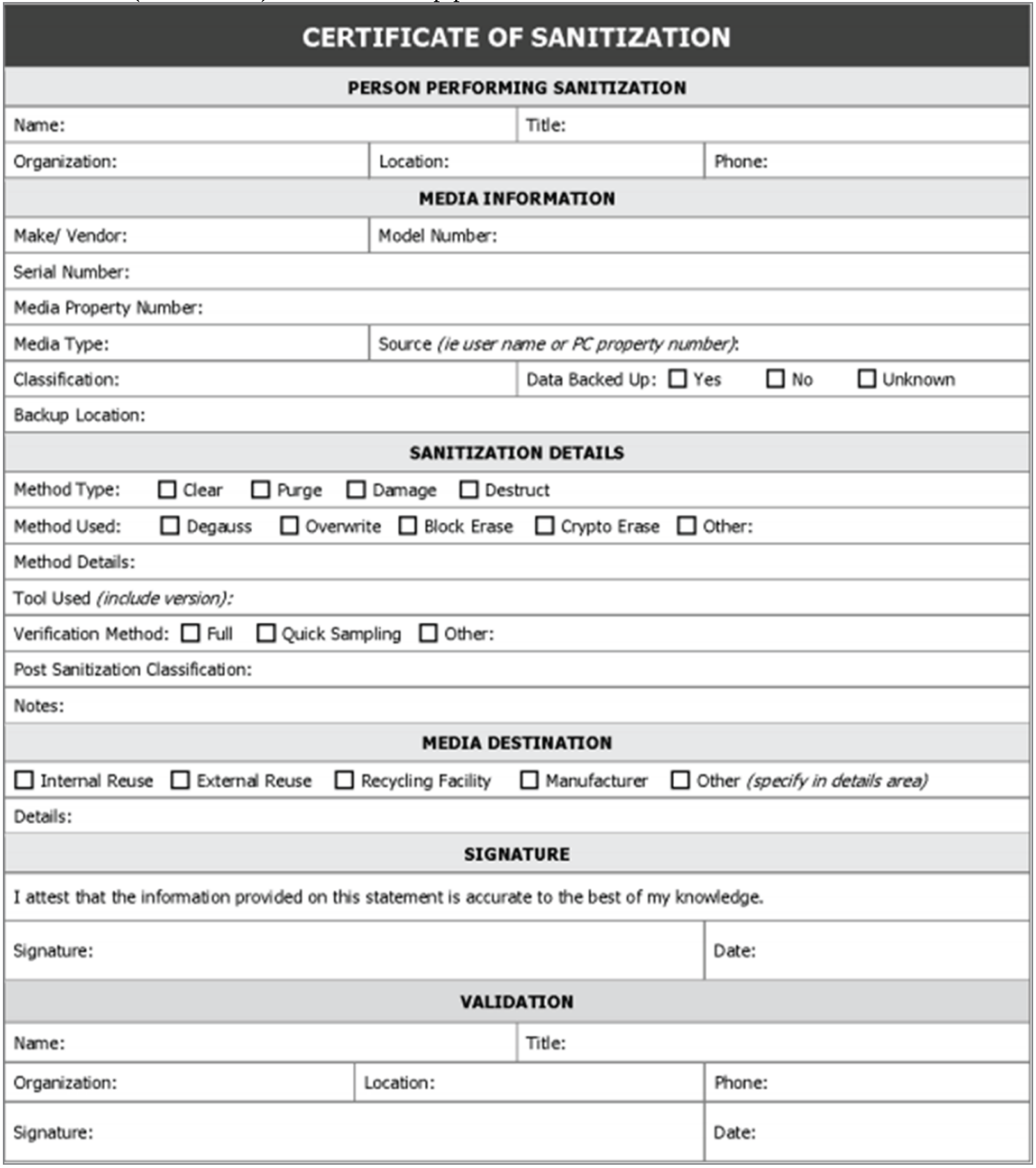
Chris has been put in charge of his organization's IT service management effort, and part of that effort includes creating an inventory of both tangible and intangible assets. As a security professional, you have been asked to provide Chris with security-related guidance on each of the following topics. Your goal is to provide Chris with the best answer from each of the options, knowing that in some cases more than one of the answers could be acceptable.

59. Chris needs to identify all of the active systems and devices on the network. Which of the following techniques will give him the most complete list of connected devices?
    1. Query Active Directory for a list of all computer objects.
    2. Perform a port scan of all systems on the network.
    3. Ask all staff members to fill out a form listing all of their systems and devices.
    4. Use network logs to identify all connected devices and track them down from there.
60. Chris knows that his inventory is only accurate at the moment it was completed. How can he best ensure that it remains up-to-date?
    1. Perform a point-in-time query of network connected devices and update the list based on what is found.
    2. Ensure that procurement and acquisition processes add new devices to the inventory before they are deployed.
    3. Require every employee to provide an updated inventory of devices they are responsible for on a quarterly basis.
    4. Manually verify every device in service at each organizational location on a yearly basis.
61. Chris knows that his organization has more than just physical assets. In fact, his organization's business involves significant intellectual property assets, including designs and formulas. Chris needs to track and inventory those assets as well. How can he most effectively ensure that he can identify and manage data throughout his organization based on its classification or type?
    1. Track file extensions for common data types.
    2. Ensure that data is collected in specific network share locations based on the data type and group that works with it.
    3. Use metadata tagging based on data type or security level.
    4. Automatically tag data by file extension type.
62. Chris has been tasked with identifying intangible assets but needs to provide his team with a list of the assets they will be inventorying. Which of the following is not an example of an intangible asset?
    1. Patents
    2. Databases
    3. Formulas
    4. Employees
63. Which of the following is not a common requirement for the collection of data under data privacy laws and statutes?
    1. Only data that is needed is collected.
    2. Data should be obtained lawfully and via fair methods.

3. Data should only be collected with the consent of the individual whose data is being collected.
4. Data should be collected from all individuals equally.

64. Susan works in an organization that labels all removable media with the classification level of the data it contains, including public data. Why would Susan's employer label all media instead of labeling only the media that contains data that could cause harm if it was exposed?
    1. It is cheaper to order all prelabeled media.
    2. It prevents sensitive media from not being marked by mistake.
    3. It prevents reuse of public media for sensitive data.
    4. Labeling all media is required by HIPAA.
65. Data stored in RAM is best characterized as what type of data?
    1. Data at rest
    2. Data in use
    3. Data in transit
    4. Data at large

66. What issue is the validation portion of the NIST SP 800-88 sample certificate of sanitization (shown here) intended to help prevent?



**CERTIFICATE OF SANITIZATION**

**PERSON PERFORMING SANITIZATION**

Name: Title:

Organization: Location: Phone:

**MEDIA INFORMATION**

Make/ Vendor: Model Number:

Serial Number:

Media Property Number:

Media Type: Source *(ie user name or PC property number)*:

Classification: Data Backed Up: □ Yes □ No □ Unknown

Backup Location:

**SANITIZATION DETAILS**

Method Type: □ Clear □ Purge □ Damage □ Destruct

Method Used: □ Degauss □ Overwrite □ Block Erase □ Crypto Erase □ Other:

Method Details:

Tool Used *(include version):*

Verification Method: □ Full □ Quick Sampling □ Other:

Post Sanitization Classification:

Notes:

**MEDIA DESTINATION**

□ Internal Reuse □ External Reuse □ Recycling Facility □ Manufacturer □ Other *(specify in details area)*

Details:

**SIGNATURE**

I attest that the information provided on this statement is accurate to the best of my knowledge.

Signature: Date:

**VALIDATION**

Name: Title:

Organization: Location: Phone:

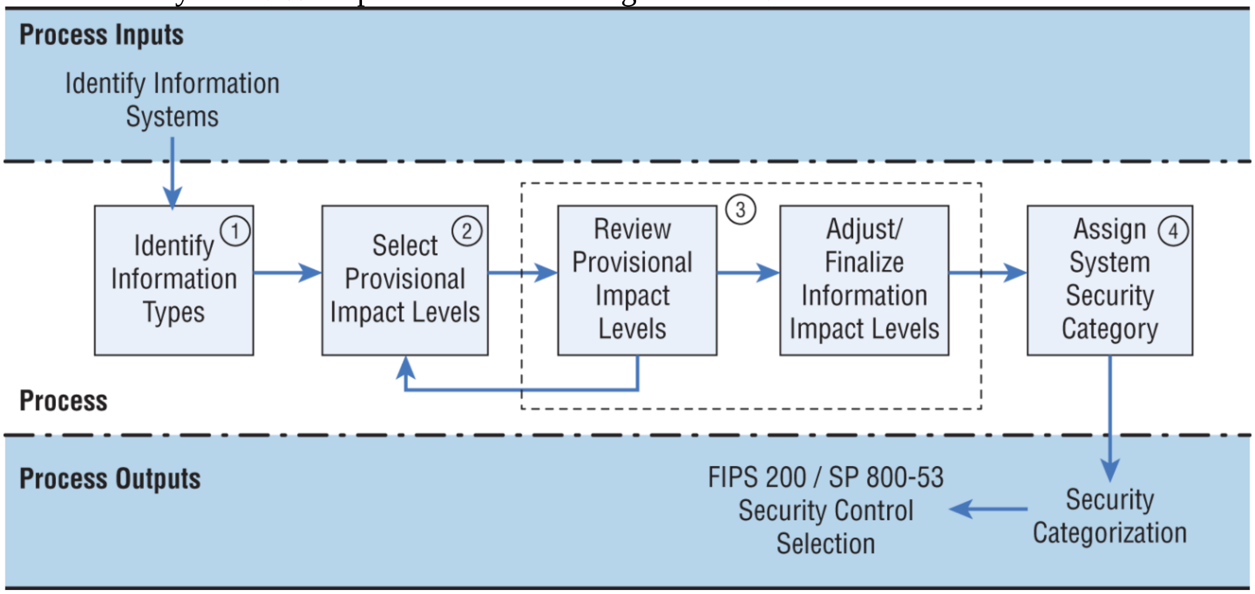
Signature: Date:

Source: Certificate of Sanitization.

1. Destruction
2. Reuse
3. Data remanence

    4. Attribution
67. Why is declassification rarely chosen as an option for media reuse?
    1. Purging is sufficient for sensitive data.
    2. Sanitization is the preferred method of data removal.
    3. It is more expensive than new media and may still fail.
    4. Clearing is required first.
68. Incineration, crushing, shredding, and disintegration all describe what stage in the lifecycle of media?
    1. Sanitization
    2. Degaussing
    3. Purging
    4. Destruction
69. What term is used to describe information like prescriptions and X-rays?
    1. PHI
    2. Proprietary data
    3. PID
    4. PII
70. Why might an organization use unique screen backgrounds or designs on workstations that deal with data of different classification levels?
    1. To indicate the software version in use
    2. To promote a corporate message
    3. To promote availability
    4. To indicate the classification level of the data or system
71. Charles has been asked to downgrade the media used for storage of private data for his organization. What process should Charles follow?
    1. Degauss the drives, and then relabel them with a lower classification level.
    2. Pulverize the drives, and then reclassify them based on the data they contain.
    3. Follow the organization's purging process, and then downgrade and replace labels.
    4. Relabel the media, and then follow the organization's purging process to ensure that the media matches the label.
72. Which of the following tasks is not performed by a system owner per NIST SP 800-18?
    1. Develops a system security plan
    2. Establishes rules for appropriate use and protection of data
    3. Identifies and implements security controls
    4. Ensures that system users receive appropriate security training

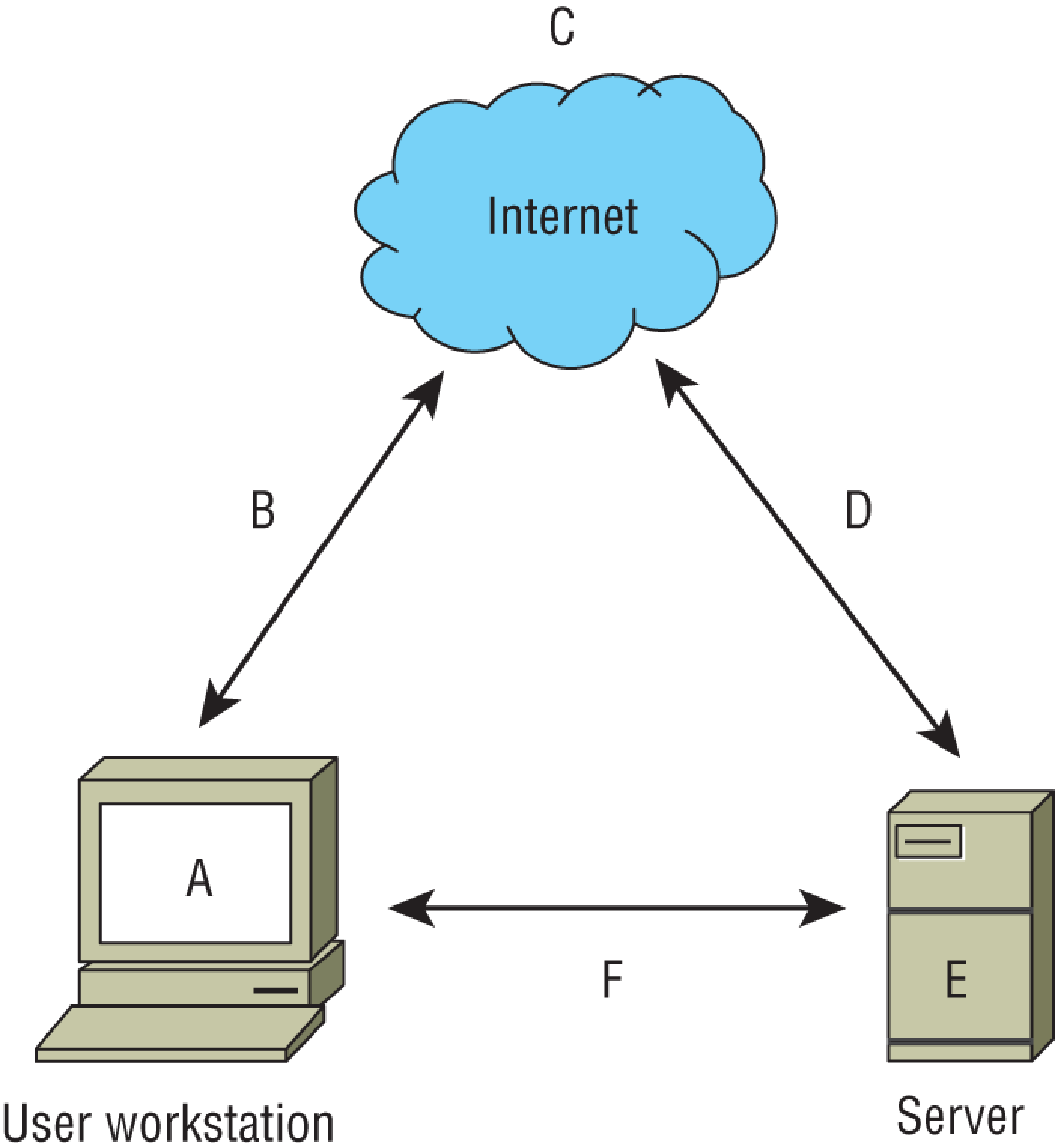
73. NIST SP 800-60 provides a process shown in the following diagram to assess information systems. What process does this diagram show?


Process Inputs
Identify Information Systems
Identify Information Types 1
Select Provisional Impact Levels 2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category 4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Source: NIST SP 800-60.

1. Selecting a standard and implementing it
2. Categorizing and selecting controls
3. Baselining and selecting controls
4. Categorizing and sanitizing

The following diagram shows a typical workstation and server and their connections to each other and the internet. For questions 74–76, please refer to this diagram.



74. Which letters on this diagram are locations where you might find data at rest?
    1. A, B, and C
    2. C and E
    3. A and E
    4. B, D, and F

75. What would be the best way to secure data at points B, D, and F?
    1. AES-256
    2. SSL

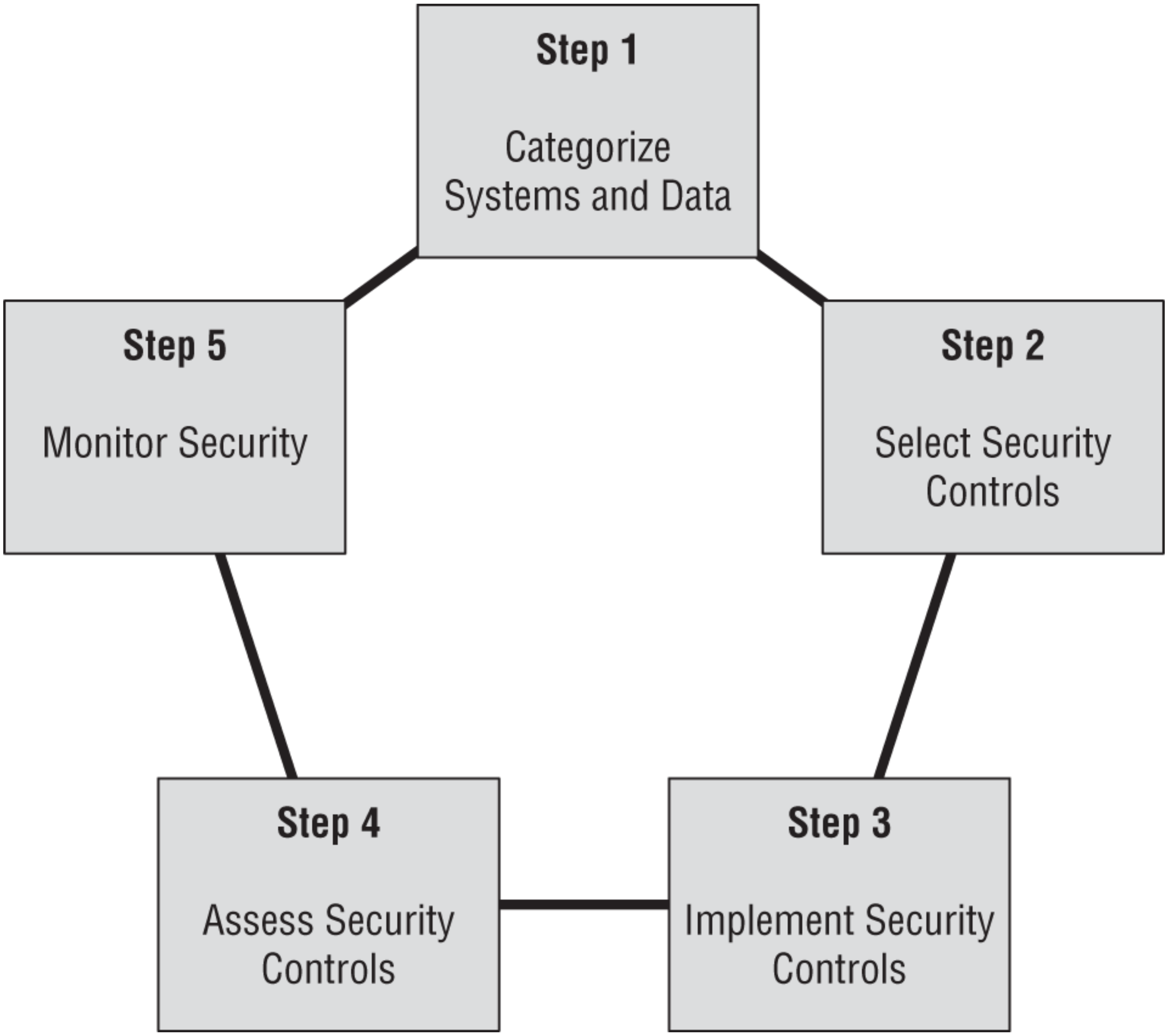
    3. TLS
    4. 3DES
76. What is the best way to secure files that are sent from workstation A via the internet service (C) to remote server E?
    1. Use AES at rest at point A, and use TLS in transit via B and D.
    2. Encrypt the data files and send them.
    3. Use 3DES and TLS to provide double security.
    4. Use full disk encryption at A and E, and use SSL at B and D.
77. Susan needs to provide a set of minimum security requirements for email. What steps should she recommend for her organization to ensure that the email remains secure?
    1. All email should be encrypted.
    2. All email should be encrypted and labeled.
    3. Sensitive email should be encrypted and labeled.
    4. Only highly sensitive email should be encrypted.
78. How can a data retention policy reduce liabilities?
    1. By reducing the amount of storage in use
    2. By limiting the number of data classifications
    3. By reducing the amount of data that may need to be produced for lawsuits
    4. By reducing the legal penalties for noncompliance
79. What data role does a system that is used to process data have?
    1. Mission owner
    2. Data owner
    3. Data processor
    4. Custodian
80. Which one of the following is not considered PII under US federal government regulations?
    1. Name
    2. Social Security number
    3. Student ID number
    4. ZIP code
81. What type of health information is the Health Insurance Portability and Accountability Act required to protect?
    1. PII
    2. PHI
    3. SHI
    4. HPHI
82. The system that Ian has built replaces data in a database field with a randomized string of characters that remains the same for each instance of that data. What technique has he used?
    1. Data masking
    2. Tokenization
    3. Anonymization
    4. DES
83. Juanita's company processes credit cards and wants to select appropriate data security standards. What data security standard is she most likely to need to use and comply with?
    1. CC-Comply

   2. PCI-DSS
   3. GLBA
   4. GDPR

84. What is the best method to sanitize a solid-state drive (SSD)?
    1. Clearing
    2. Zero fill
    3. Disintegration
    4. Degaussing

For questions 85–87, please refer to the following scenario:

As shown in the following security lifecycle diagram (loosely based on the NIST reference architecture), NIST uses a five-step process for risk management. Using your knowledge of data roles and practices, answer the following questions based on the NIST framework process.



85. What data role will own responsibility for step 1, the categorization of information systems; to whom will they delegate step 2; and what data role will be responsible for step 3?
    1. Data owners, system owners, custodians
    2. Data processors, custodians, users
    3. Business owners, administrators, custodians
    4. System owners, business owners, administrators
86. If the systems that are being assessed all handle credit card information (and no other sensitive data), at what step would the PCI DSS first play an important role?
    1. Step 1
    2. Step 2
    3. Step 3
    4. Step 4
87. What data security role is primarily responsible for step 5?
    1. Data owners
    2. Data processors
    3. Custodians
    4. Users
88. Susan’s organization performs a secure disk wipe process on hard drives before they are sent to a third-party organization to be shredded. What issue is her organization attempting to avoid?
    1. Data retention that is longer than defined in policy
    2. Mishandling of drives by the third party
    3. Classification mistakes
    4. Data permanence
89. Mike wants to track hardware assets as devices and equipment are moved throughout his organization. What type of system can help do this without requiring staff to individually check bar codes or serial numbers?
    1. A visual inventory
    2. WiFi MAC address tracking
    3. RFID tags
    4. Steganography
90. Retaining and maintaining information for as long as it is needed is known as what?
    1. Data storage policy
    2. Data storage
    3. Asset maintenance
    4. Record retention
91. Which of the following activities is not a consideration during data classification?
    1. Who can access the data
    2. What the impact would be if the data was lost or breached
    3. How much the data cost to create
    4. What protection regulations may be required for the data
92. What type of encryption is typically used for data at rest?
    1. Asymmetric encryption
    2. Symmetric encryption
    3. DES

    4. OTP

93. Which data role is tasked with apply rights that provide appropriate access to staff members?
    1. Data processors
    2. Business owners
    3. Custodians
    4. Administrators
94. What element of asset security is often determined by identifying an asset's owner?
    1. It identifies the individual(s) responsible for protecting the asset.
    2. It provides a law enforcement contact in case of theft.
    3. It helps establish the value of the asset.
    4. It determines the security classification of the asset.
95. Fred is preparing to send backup tapes off-site to a secure third-party storage facility. What steps should Fred take before sending the tapes to that facility?
    1. Ensure that the tapes are handled the same way the original media would be handled based on their classification.
    2. Increase the classification level of the tapes because they are leaving the possession of the company.
    3. Purge the tapes to ensure that classified data is not lost.
    4. Decrypt the tapes in case they are lost in transit.
96. Which of the following does not describe data in motion?
    1. Data on a backup tape that is being shipped to a storage facility
    2. Data in a TCP packet
    3. Data in an e-commerce transaction
    4. Data in files being copied between locations
97. A new law is passed that would result in significant financial harm to your company if the data that it covers was stolen or inadvertently released. What should your organization do about this?
    1. Select a new security baseline.
    2. Relabel the data.
    3. Encrypt all of the data at rest and in transit.
    4. Review its data classifications and classify the data appropriately.
98. Which of the following data roles are typically found inside of a company instead of as a third-party contracting relationship? (Select all that apply.)
    1. Data owners
    2. Data controllers
    3. Data custodians
    4. Data processors
99. What commercial data classification is most appropriate for data contained on corporate websites?
    1. Private
    2. Sensitive
    3. Public
    4. Proprietary

100. Match each of the numbered data elements shown here with one of the lettered categories. You may use the categories once, more than once, or not at all. If a data element matches more than one category, choose the one that is most specific.

**Data elements**

1. Medical records
2. Trade secrets
3. Social Security numbers
4. Driver's license numbers

**Categories**

5. Proprietary data
6. Protected health information
7. Personally identifiable information