CISSP Official (ISC)2 Practice Tests, 2nd Edition by Mike Chapple; David Seidl Published by Sybex, 2018

Chapter 1
Security and Risk Management (Domain 1)

1. What is the final step of a quantitative risk analysis?
    1. Determine asset value.
    2. Assess the annualized rate of occurrence.
    3. Derive the annualized loss expectancy.
    4. Conduct a cost/benefit analysis.
2. Match the following numbered wireless attack terms with their appropriate lettered descriptions:

    Wireless attack terms

    1. Rogue access point
    2. Replay
    3. Evil twin
    4. War driving

    Descriptions

    5. An attack that relies on an access point to spoof a legitimate access point's SSID and Mandatory Access Control (MAC) address
    6. An access point intended to attract new connections by using an apparently legitimate SSID
    7. An attack that retransmits captured communication to attempt to gain access to a targeted system
    8. The process of using detection tools to find wireless networks
3. Under the Digital Millennium Copyright Act (DMCA), what type of offenses do not require prompt action by an internet service provider after it receives a notification of infringement claim from a copyright holder?
    1. Storage of information by a customer on a provider's server
    2. Caching of information by the provider
    3. Transmission of information over the provider's network by a customer
    4. Caching of information in a provider search engine
4. FlyAway Travel has offices in both the European Union (EU) and the United States and transfers personal information between those offices regularly. They have recently received a request from an EU customer requesting that their account be terminated. Under the General Data Protection Regulation (GDPR), which requirement for processing personal information states that individuals may request that their data no longer be disseminated or processed?
    1. The right to access
    2. Privacy by design

3. The right to be forgotten
4. The right of data portability

5. Which one of the following is not one of the three common threat modeling techniques?
    1. Focused on assets
    2. Focused on attackers
    3. Focused on software
    4. Focused on social engineering
6. Which one of the following elements of information is not considered personally identifiable information that would trigger most United States (U.S.) state data breach laws?
    1. Student identification number
    2. Social Security number
    3. Driver's license number
    4. Credit card number
7. In 1991, the Federal Sentencing Guidelines formalized a rule that requires senior executives to take personal responsibility for information security matters. What is the name of this rule?
    1. Due diligence rule
    2. Personal liability rule
    3. Prudent man rule
    4. Due process rule
8. Which one of the following provides an authentication mechanism that would be appropriate for pairing with a password to achieve multifactor authentication?
    1. Username
    2. Personal identification number (PIN)
    3. Security question
    4. Fingerprint scan
9. What United States government agency is responsible for administering the terms of privacy shield agreements between the European Union and the United States under the EU GDPR?
    1. Department of Defense
    2. Department of the Treasury
    3. State Department
    4. Department of Commerce
10. Yolanda is the chief privacy officer for a financial institution and is researching privacy issues related to customer checking accounts. Which one of the following laws is most likely to apply to this situation?
    1. GLBA
    2. SOX
    3. HIPAA
    4. FERPA
11. Tim's organization recently received a contract to conduct sponsored research as a government contractor. What law now likely applies to the information systems involved in this contract?
    1. FISMA
    2. PCI DSS

3. HIPAA
4. GISRA

12. Chris is advising travelers from his organization who will be visiting many different countries overseas. He is concerned about compliance with export control laws. Which of the following technologies is most likely to trigger these regulations?
    1. Memory chips
    2. Office productivity applications
    3. Hard drives
    4. Encryption software
13. Bobbi is investigating a security incident and discovers that an attacker began with a normal user account but managed to exploit a system vulnerability to provide that account with administrative rights. What type of attack took place under the STRIDE threat model?
    1. Spoofing
    2. Repudiation
    3. Tampering
    4. Elevation of privilege
14. You are completing your business continuity planning effort and have decided that you wish to accept one of the risks. What should you do next?
    1. Implement new security controls to reduce the risk level.
    2. Design a disaster recovery plan.
    3. Repeat the business impact assessment.
    4. Document your decision-making process.
15. Which one of the following control categories does not accurately describe a fence around a facility?
    1. Physical
    2. Detective
    3. Deterrent
    4. Preventive
16. Tony is developing a business continuity plan and is having difficulty prioritizing resources because of the difficulty of combining information about tangible and intangible assets. What would be the most effective risk assessment approach for him to use?
    1. Quantitative risk assessment
    2. Qualitative risk assessment
    3. Neither quantitative nor qualitative risk assessment
    4. Combination of quantitative and qualitative risk assessment
17. What law provides intellectual property protection to the holders of trade secrets?
    1. Copyright Law
    2. Lanham Act
    3. Glass-Steagall Act
    4. Economic Espionage Act
18. Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances?
    1. Due diligence

2. Separation of duties
3. Due care
4. Least privilege

19. Darcy is designing a fault tolerant system and wants to implement RAID level 5 for her system. What is the minimum number of physical hard disks she can use to build this system?
    1. One
    2. Two
    3. Three
    4. Five
20. Which one of the following is an example of an administrative control?
    1. Intrusion detection system
    2. Security awareness training
    3. Firewalls
    4. Security guards
21. Keenan Systems recently developed a new manufacturing process for microprocessors. The company wants to license the technology to other companies for use but wishes to prevent unauthorized use of the technology. What type of intellectual property protection is best suited for this situation?
    1. Patent
    2. Trade secret
    3. Copyright
    4. Trademark
22. Which one of the following actions might be taken as part of a business continuity plan?
    1. Restoring from backup tapes
    2. Implementing RAID
    3. Relocating to a cold site
    4. Restarting business operations
23. When developing a business impact analysis, the team should first create a list of assets. What should happen next?
    1. Identify vulnerabilities in each asset.
    2. Determine the risks facing the asset.
    3. Develop a value for each asset.
    4. Identify threats facing each asset.
24. Mike recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. What type of risk management strategy is Mike pursuing?
    1. Risk acceptance
    2. Risk avoidance
    3. Risk mitigation
    4. Risk transference
25. Which one of the following is an example of physical infrastructure hardening?
    1. Antivirus software
    2. Hardware-based network firewall
    3. Two-factor authentication
    4. Fire suppression system

26. Which one of the following is normally used as an authorization tool?
    1. ACL
    2. Token
    3. Username
    4. Password
27. The International Information Systems Security Certification Consortium uses the logo shown here to represent itself online and in a variety of forums. What type of intellectual property protection may it use to protect its rights in this logo?

    1. Copyright
    2. Patent
    3. Trade secret
    4. Trademark
28. Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?

1. Availability
2. Confidentiality
3. Disclosure
4. Distributed

29. Which one of the following organizations would not be automatically subject to the terms of HIPAA if they engage in electronic transactions?
    1. Healthcare provider
    2. Health and fitness application developer
    3. Health information clearinghouse
    4. Health insurance plan
30. John's network begins to experience symptoms of slowness. Upon investigation, he realizes that the network is being bombarded with TCP SYN packets and believes that his organization is the victim of a denial of service attack. What principle of information security is being violated?
    1. Availability
    2. Integrity
    3. Confidentiality
    4. Denial

31. Renee is designing the long-term security plan for her organization and has a three- to five-year planning horizon. What type of plan is she developing?
    1. Operational
    2. Tactical
    3. Summary
    4. Strategic
32. What government agency is responsible for the evaluation and registration of trademarks?
    1. USPTO
    2. Library of Congress
    3. TVA
    4. NIST
33. The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?
    1. Mandatory vacation
    2. Separation of duties
    3. Defense in depth
    4. Job rotation
34. Which one of the following categories of organizations is most likely to be covered by the provisions of FISMA?
    1. Banks
    2. Defense contractors
    3. School districts
    4. Hospitals
35. Robert is responsible for securing systems used to process credit card information. What standard should guide his actions?
    1. HIPAA
    2. PCI DSS
    3. SOX
    4. GLBA
36. Which one of the following individuals is normally responsible for fulfilling the operational data protection responsibilities delegated by senior management, such as validating data integrity, testing backups, and managing security policies?
    1. Data custodian
    2. Data owner
    3. User
    4. Auditor
37. Alan works for an e-commerce company that recently had some content stolen by another website and republished without permission. What type of intellectual property protection would best preserve Alan's company's rights?
    1. Trade secret
    2. Copyright
    3. Trademark
    4. Patent

38. Florian receives a flyer from a federal agency announcing that a new administrative law will affect his business operations. Where should he go to find the text of the law?
    1. United States Code
    2. Supreme Court rulings
    3. Code of Federal Regulations
    4. Compendium of Laws
39. Tom enables an application firewall provided by his cloud infrastructure as a service provider that is designed to block many types of application attacks. When viewed from a risk management perspective, what metric is Tom attempting to lower?
    1. Impact
    2. RPO
    3. MTO
    4. Likelihood
40. Which one of the following individuals would be the most effective organizational owner for an information security program?
    1. CISSP-certified analyst
    2. Chief information officer (CIO)
    3. Manager of network security
    4. President and CEO
41. What important function do senior managers normally fill on a business continuity planning team?
    1. Arbitrating disputes about criticality
    2. Evaluating the legal environment
    3. Training staff
    4. Designing failure controls
42. You are the CISO for a major hospital system and are preparing to sign a contract with a software as a service (SaaS) email vendor and want to ensure that its business continuity planning measures are reasonable. What type of audit might you request to meet this goal?
    1. SOC 1
    2. FISMA
    3. PCI DSS
    4. SOC 2
43. Gary is analyzing a security incident and, during his investigation, encounters a user who denies having performed an action that Gary believes he did perform. What type of threat has taken place under the STRIDE model?
    1. Repudiation
    2. Information disclosure
    3. Tampering
    4. Elevation of privilege
44. Beth is the security administrator for a public school district. She is implementing a new student information system and is testing the code to ensure that students are not able to alter their own grades. What principle of information security is Beth enforcing?
    1. Integrity
    2. Availability
    3. Confidentiality

4. Denial

45. Which one of the following issues is not normally addressed in a service-level agreement (SLA)?
    1. Confidentiality of customer information
    2. Failover time
    3. Uptime
    4. Maximum consecutive downtime
46. Joan is seeking to protect a piece of computer software that she developed under intellectual property law. Which one of the following avenues of protection would not apply to a piece of software?
    1. Trademark
    2. Copyright
    3. Patent
    4. Trade secret

For questions 47–49, please refer to the following scenario:

Juniper Content is a web content development company with 40 employees located in two offices: one in New York and a smaller office in the San Francisco Bay Area. Each office has a local area network protected by a perimeter firewall. The local area network (LAN) contains modern switch equipment connected to both wired and wireless networks.

Each office has its own file server, and the information technology (IT) team runs software every hour to synchronize files between the two servers, distributing content between the offices. These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS-based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Juniper Content, and you are working to augment existing security controls to improve the organization's security.

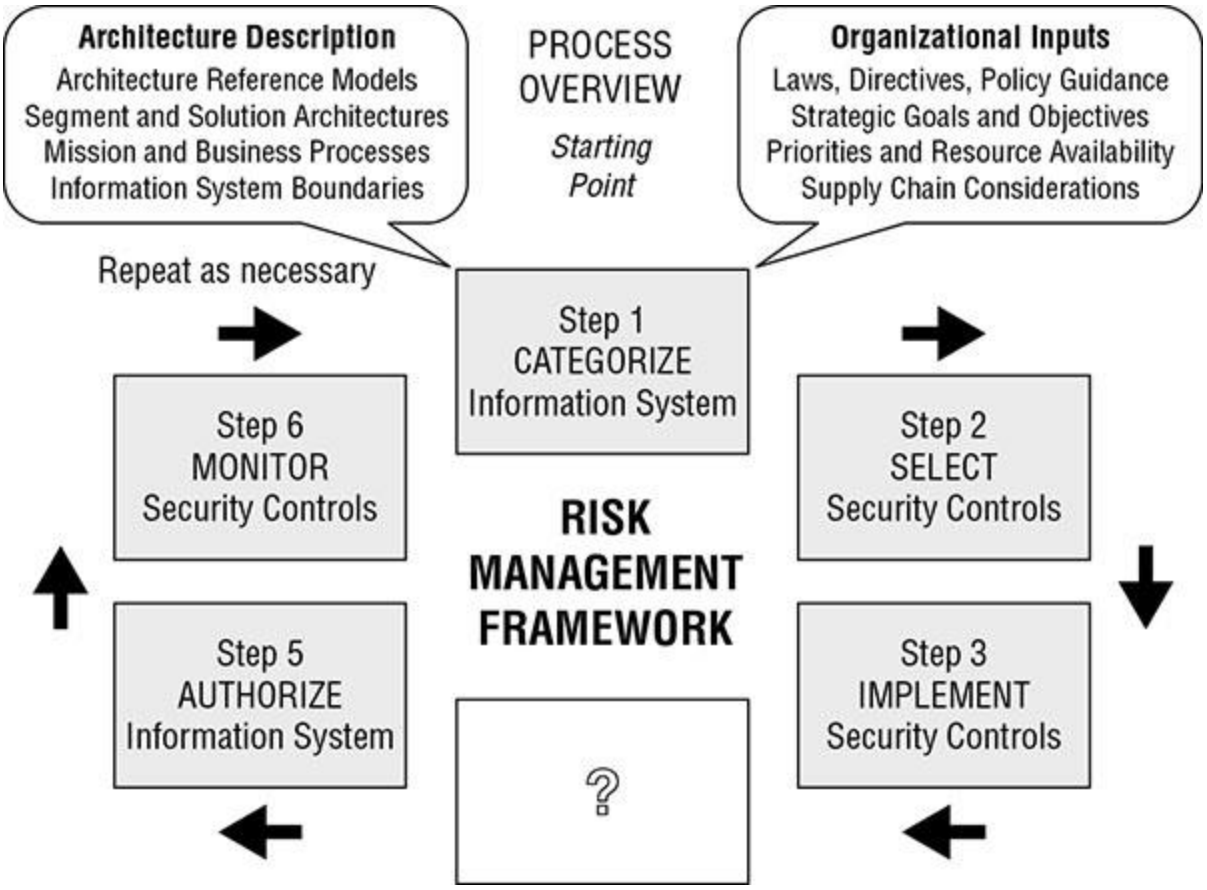
47. Users in the two offices would like to access each other's file servers over the internet. What control would provide confidentiality for those communications?
    1. Digital signatures
    2. Virtual private network
    3. Virtual LAN
    4. Digital content management
48. You are also concerned about the availability of data stored on each office's server. You would like to add technology that would enable continued access to files located on the server even if a hard drive in a server fails. What integrity control allows you to add robustness without adding additional servers?
    1. Server clustering
    2. Load balancing
    3. RAID

4. Scheduled backups

49. Finally, there are historical records stored on the server that are extremely important to the business and should never be modified. You would like to add an integrity control that allows you to verify on a periodic basis that the files were not modified. What control can you add?
    1. Hashing
    2. ACLs
    3. Read-only attributes
    4. Firewalls
50. What law serves as the basis for privacy rights in the United States?
    1. Privacy Act of 1974
    2. Fourth Amendment
    3. First Amendment
    4. Electronic Communications Privacy Act of 1986
51. Which one of the following is not normally included in business continuity plan documentation?
    1. Statement of accounts
    2. Statement of importance
    3. Statement of priorities
    4. Statement of organizational responsibility
52. An accounting employee at Doolittle Industries was recently arrested for participation in an embezzlement scheme. The employee transferred money to a personal account and then shifted funds around between other accounts every day to disguise the fraud for months. Which one of the following controls might have best allowed the earlier detection of this fraud?
    1. Separation of duties
    2. Least privilege
    3. Defense in depth
    4. Mandatory vacation
53. Which one of the following is not normally considered a business continuity task?
    1. Business impact assessment
    2. Emergency response guidelines
    3. Electronic vaulting
    4. Vital records program
54. Which information security goal is impacted when an organization experiences a DoS or DDoS attack?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Denial
55. Yolanda is writing a document that will provide configuration information regarding the minimum level of security that every system in the organization must meet. What type of document is she preparing?
    1. Policy
    2. Baseline
    3. Guideline

4. Procedure

56. Who should receive initial business continuity plan training in an organization?
    1. Senior executives
    2. Those with specific business continuity roles
    3. Everyone in the organization
    4. First responders
57. James is conducting a risk assessment for his organization and is attempting to assign an asset value to the servers in his data center. The organization's primary concern is ensuring that it has sufficient funds available to rebuild the data center in the event it is damaged or destroyed. Which one of the following asset valuation methods would be most appropriate in this situation?
    1. Purchase cost
    2. Depreciated cost
    3. Replacement cost
    4. Opportunity cost
58. The Computer Security Act of 1987 gave a federal agency responsibility for developing computer security standards and guidelines for federal computer systems. What agency did the act give this responsibility to?
    1. National Security Agency
    2. Federal Communications Commission
    3. Department of Defense
    4. National Institute of Standards and Technology
59. Which one of the following is not a requirement for an invention to be patentable?
    1. It must be new.
    2. It must be invented by an American citizen.
    3. It must be nonobvious.
    4. It must be useful.
60. Frank discovers a keylogger hidden on the laptop of his company's chief executive officer. What information security principle is the keylogger most likely designed to disrupt?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Denial
61. What is the formula used to determine risk?
    1. Risk = Threat * Vulnerability
    2. Risk = Threat / Vulnerability
    3. Risk = Asset * Threat
    4. Risk = Asset / Threat
62. The following graphic shows the NIST risk management framework with step 4 missing. What is the missing step?



1. Assess security controls.
2. Determine control gaps.
3. Remediate control gaps.
4. Evaluate user activity.

63. HAL Systems recently decided to stop offering public NTP services because of a fear that its NTP servers would be used in amplification DDoS attacks. What type of risk management strategy did HAL pursue with respect to its NTP services?
    1. Risk mitigation
    2. Risk acceptance
    3. Risk transference
    4. Risk avoidance
64. Susan is working with the management team in her company to classify data in an attempt to apply extra security controls that will limit the likelihood of a data breach. What principle of information security is Susan trying to enforce?
    1. Availability
    2. Denial
    3. Confidentiality
    4. Integrity
65. Which one of the following components should be included in an organization's emergency response guidelines?
    1. List of individuals who should be notified of an emergency incident
    2. Long-term business continuity protocols

3. Activation procedures for the organization's cold sites
4. Contact information for ordering equipment

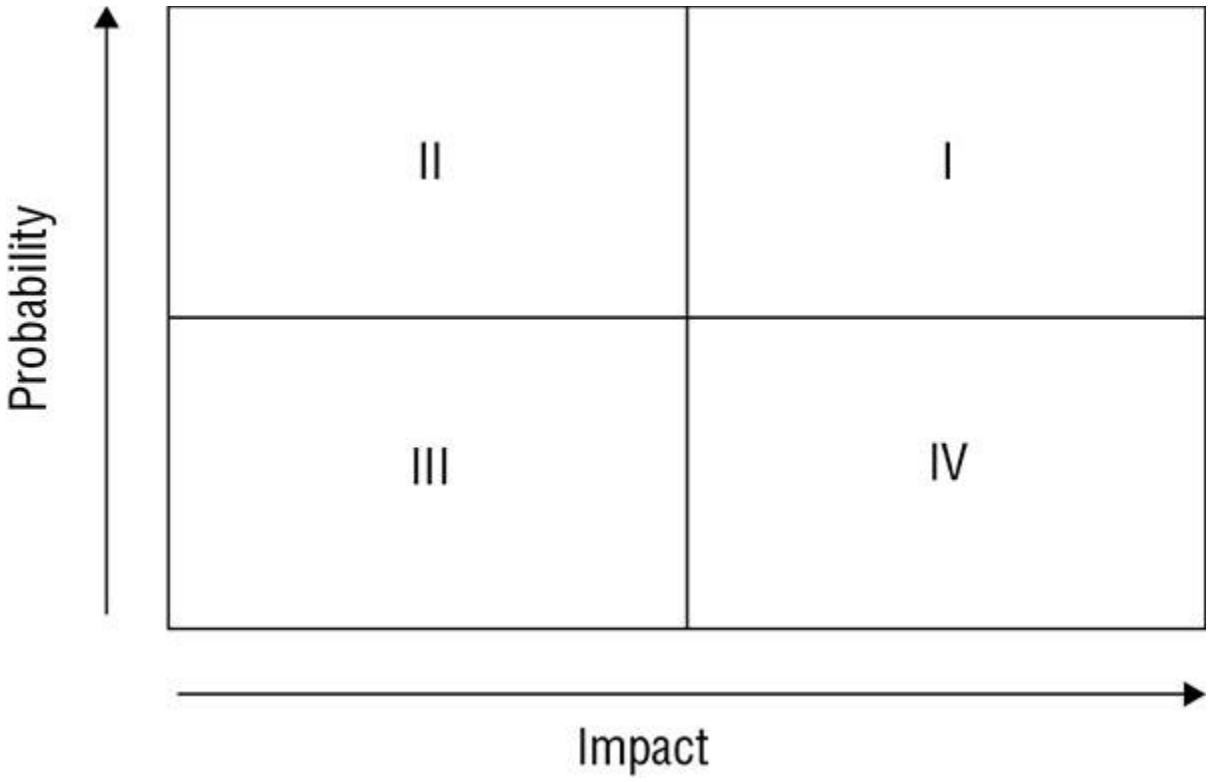
66. Who is the ideal person to approve an organization's business continuity plan?
    1. Chief information officer
    2. Chief executive officer
    3. Chief information security officer
    4. Chief operating officer
67. Which one of the following actions is not normally part of the project scope and planning phase of business continuity planning?
    1. Structured analysis of the organization
    2. Review of the legal and regulatory landscape
    3. Creation of a BCP team
    4. Documentation of the plan
68. Gary is implementing a new website architecture that uses multiple small web servers behind a load balancer. What principle of information security is Gary seeking to enforce?
    1. Denial
    2. Confidentiality
    3. Integrity
    4. Availability
69. Becka recently signed a contract with an alternate data processing facility that will provide her company with space in the event of a disaster. The facility includes HVAC, power, and communications circuits but no hardware. What type of facility is Becka using?
    1. Cold site
    2. Warm site
    3. Hot site
    4. Mobile site
70. What is the threshold for malicious damage to a federal computer system that triggers the Computer Fraud and Abuse Act?
    1. $500
    2. $2,500
    3. $5,000
    4. $10,000
71. Ben is seeking a control objective framework that is widely accepted around the world and focuses specifically on information security controls. Which one of the following frameworks would best meet his needs?
    1. ITIL
    2. ISO 27002
    3. CMM
    4. PMBOK Guide
72. Which one of the following laws requires that communications service providers cooperate with law enforcement requests?
    1. ECPA
    2. CALEA
    3. Privacy Act

4. HITECH Act

73. Every year, Gary receives privacy notices in the mail from financial institutions where he has accounts. What law requires the institutions to send Gary these notices?
    1. FERPA
    2. GLBA
    3. HIPAA
    4. HITECH
74. Which one of the following agreements typically requires that a vendor not disclose confidential information learned during the scope of an engagement?
    1. NCA
    2. SLA
    3. NDA
    4. RTO
75. Which one of the following is not an example of a technical control?
    1. Router ACL
    2. Firewall rule
    3. Encryption
    4. Data classification
76. Which one of the following stakeholders is not typically included on a business continuity planning team?
    1. Core business function leaders
    2. Information technology staff
    3. CEO
    4. Support departments
77. Ben is designing a messaging system for a bank and would like to include a feature that allows the recipient of a message to prove to a third party that the message did indeed come from the purported originator. What goal is Ben trying to achieve?
    1. Authentication
    2. Authorization
    3. Integrity
    4. Nonrepudiation
78. What principle of information security states that an organization should implement overlapping security controls whenever possible?
    1. Least privilege
    2. Separation of duties
    3. Defense in depth
    4. Security through obscurity
79. Which one of the following is not a goal of a formal change management program?
    1. Implement change in an orderly fashion.
    2. Test changes prior to implementation.
    3. Provide rollback plans for changes.
    4. Inform stakeholders of changes after they occur.
80. Ben is responsible for the security of payment card information stored in a database. Policy directs that he remove the information from the database, but he cannot do this for operational reasons. He obtained an exception to policy and is seeking an appropriate compensating control to mitigate the risk. What would be his best option?

1. Purchasing insurance
2. Encrypting the database contents
3. Removing the data
4. Objecting to the exception

81. The Domer Industries risk assessment team recently conducted a qualitative risk assessment and developed a matrix similar to the one shown here. Which quadrant contains the risks that require the most immediate attention?



1. I
2. II
3. III
4. IV

82. Tom is planning to terminate an employee this afternoon for fraud and expects that the meeting will be somewhat hostile. He is coordinating the meeting with Human Resources and wants to protect the company against damage. Which one of the following steps is most important to coordinate in time with the termination meeting?
    1. Informing other employees of the termination
    2. Retrieving the employee's photo ID
    3. Calculating the final paycheck
    4. Revoking electronic access rights
83. Rolando is a risk manager with a large-scale enterprise. The firm recently evaluated the risk of California mudslides on its operations in the region and determined that the cost of responding outweighed the benefits of any controls it could implement. The company

chose to take no action at this time. What risk management strategy did Rolando's organization pursue?

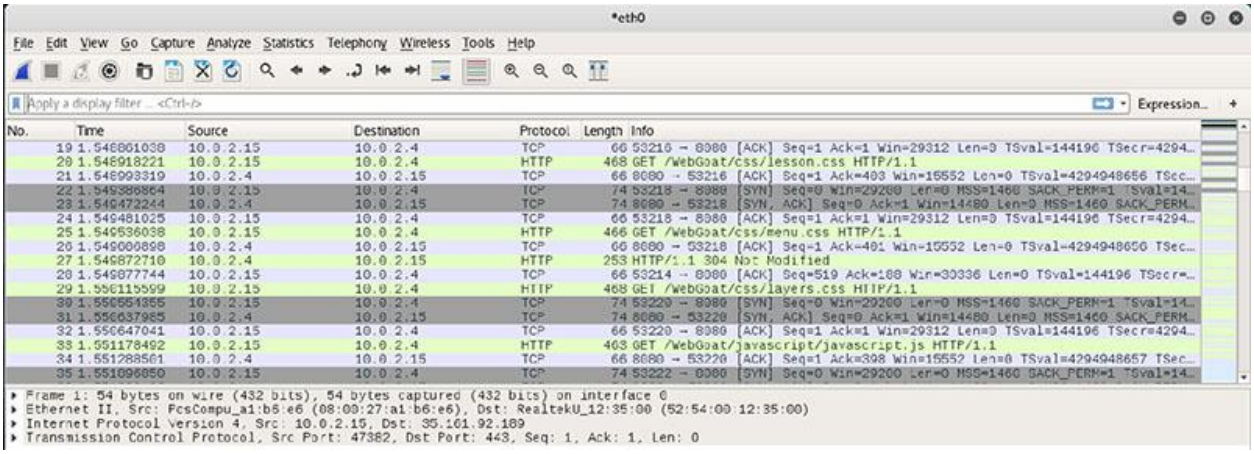
1. Risk avoidance
2. Risk mitigation
3. Risk transference
4. Risk acceptance

84. Helen is the owner of a website that provides information for middle and high school students preparing for exams. She is concerned that the activities of her site may fall under the jurisdiction of the Children's Online Privacy Protection Act (COPPA). What is the cutoff age below which parents must give consent in advance of the collection of personal information from their children under COPPA?
    1. 13
    2. 15
    3. 17
    4. 18
85. Tom is considering locating a business in the downtown area of Miami, Florida. He consults the FEMA flood plain map for the region, shown here, and determines that the area he is considering lies within a 100-year flood plain.

What is the ARO of a flood in this area?

1. 100
2. 1
3. 0.1
4. 0.01

86. You discover that a user on your network has been using the Wireshark tool, as shown here. Further investigation revealed that he was using it for illicit purposes. What pillar of information security has most likely been violated?



1. Integrity
2. Denial
3. Availability
4. Confidentiality

87. Alan is performing threat modeling and decides that it would be useful to decompose the system into the key elements shown here. What tool is he using?

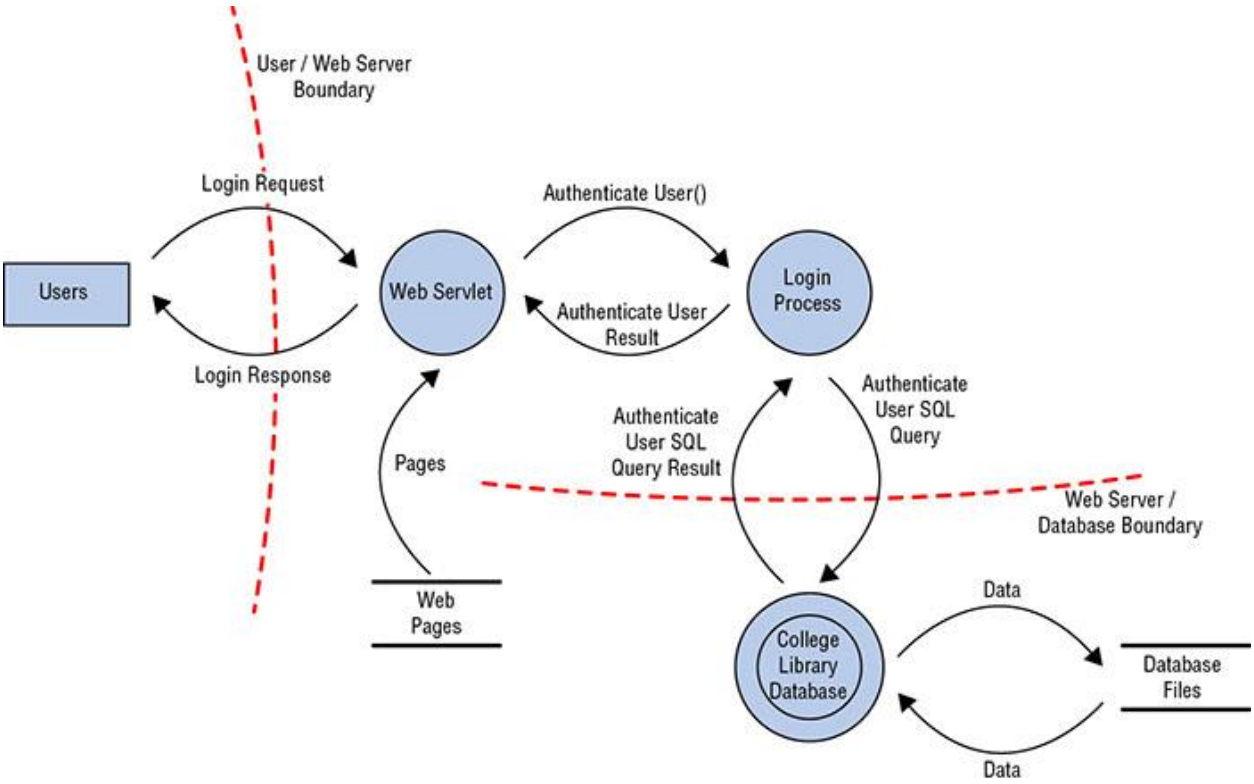


Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide*, 7th Edition © John Wiley & Sons 2015, reprinted with permission.

1. Vulnerability assessment

2. Fuzzing
3. Reduction analysis
4. Data modeling

88. Match the following numbered laws or industry standards to their lettered description:

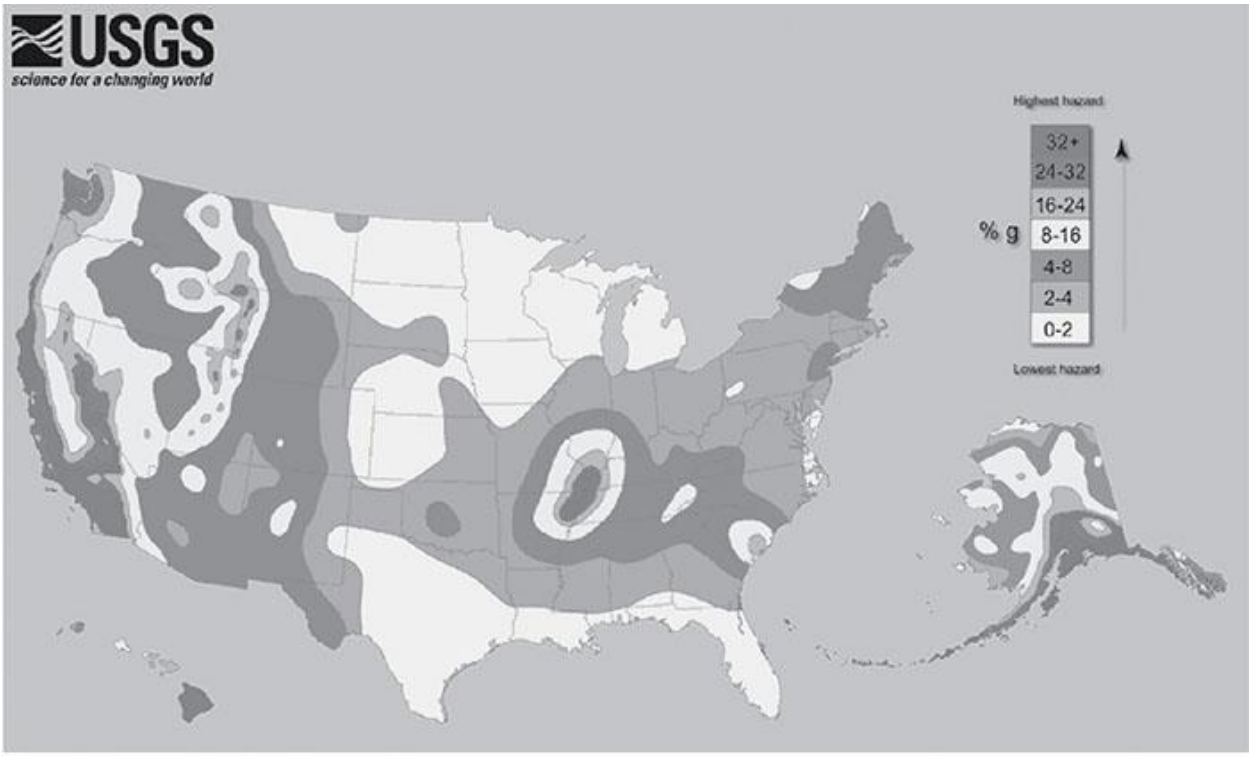
Laws and industry standards

1. GLBA
2. PCI DSS
3. HIPAA
4. SOX

Descriptions

5. A U.S. law that requires covered financial institutions to provide their customers with a privacy notice on a yearly basis
6. A U.S. law that requires internal controls assessments, including IT transaction flows for publicly traded companies
7. An industry standard that covers organizations that handle credit cards
8. A U.S. law that provides data privacy and security requirements for medical information

89. Craig is selecting the site for a new data center and must choose a location somewhere within the United States. He obtained the earthquake risk map shown here from the United States Geological Survey. Which of the following would be the safest location to build his facility if he were primarily concerned with earthquake risk?



(Source: US Geological Survey)

Image reprinted from *CISSP (ISC)* [2] *Certified Information Systems Security Professional Official Study Guide*, 7th Edition © John Wiley & Sons 2015, reprinted with permission.

1. New York
2. North Carolina
3. Indiana
4. Florida

90. Which one of the following tools is most often used for identification purposes and is not suitable for use as an authenticator?
    1. Password
    2. Retinal scan
    3. Username
    4. Token
91. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?
    1. Quantitative
    2. Qualitative
    3. Annualized loss expectancy
    4. Reduction
92. Which one of the following is the first step in developing an organization's vital records program?
    1. Identifying vital records
    2. Locating vital records
    3. Archiving vital records

4. Preserving vital records

93. Which one of the following security programs is designed to provide employees with the knowledge they need to perform their specific work tasks?
    1. Awareness
    2. Training
    3. Education
    4. Indoctrination
94. Which one of the following security programs is designed to establish a minimum standard common denominator of security understanding?
    1. Training
    2. Education
    3. Indoctrination
    4. Awareness
95. Ryan is a security risk analyst for an insurance company. He is currently examining a scenario in which a malicious hacker might use a SQL injection attack to deface a web server due to a missing patch in the company's web application. In this scenario, what is the threat?
    1. Unpatched web application
    2. Web defacement
    3. Malicious hacker
    4. Operating system

    For questions 96–98, please refer to the following scenario:

    Henry is the risk manager for Atwood Landing, a resort community in the midwestern United States. The resort's main data center is located in northern Indiana in an area that is prone to tornados. Henry recently undertook a replacement cost analysis and determined that rebuilding and reconfiguring the data center would cost $10 million.

    Henry consulted with tornado experts, data center specialists, and structural engineers. Together, they determined that a typical tornado would cause approximately $5 million of damage to the facility. The meteorologists determined that Atwood's facility lies in an area where they are likely to experience a tornado once every 200 years.

96. Based upon the information in this scenario, what is the exposure factor for the effect of a tornado on Atwood Landing's data center?
    1. 10%
    2. 25%
    3. 50%
    4. 75%
97. Based upon the information in this scenario, what is the annualized rate of occurrence for a tornado at Atwood Landing's data center?
    1. 0.0025
    2. 0.005

3. 0.01
4. 0.015

98. Based upon the information in this scenario, what is the annualized loss expectancy for a tornado at Atwood Landing's data center?
    1. $25,000
    2. $50,000
    3. $250,000
    4. $500,000
99. John is analyzing an attack against his company in which the attacker found comments embedded in HTML code that provided the clues needed to exploit a software vulnerability. Using the STRIDE model, what type of attack did he uncover?
    1. Spoofing
    2. Repudiation
    3. Information disclosure
    4. Elevation of privilege
100. Which one of the following is an administrative control that can protect the confidentiality of information?
    1. Encryption
    2. Nondisclosure agreement
    3. Firewall
    4. Fault tolerance
101. Chris is worried that the laptops that his organization has recently acquired were modified by a third party to include keyloggers before they were delivered. Where should he focus his efforts to prevent this?
    1. His supply chain
    2. His vendor contracts
    3. His post-purchase build process
    4. The original equipment manufacturer (OEM)
102. STRIDE, PASTA, and VAST are all examples of what type of tool?
    1. Risk assessment methodologies
    2. Control matrices
    3. Threat modeling methodologies
    4. Awareness campaign tools
103. In her role as a developer for an online bank, Lisa is required to submit her code for testing and review. After it passes through this process and it is approved, another employee moves the code to the production environment. What security management does this process describe?
    1. Regression testing
    2. Code review
    3. Change management
    4. Fuzz testing
104. After completing the first year of his security awareness program, Charles reviews the data about how many staff completed training compared to how many were assigned the training to determine whether he hit the 95 percent completion rate he was aiming for. What is this type of measure called?
    1. A KPI

2. A metric
3. An awareness control
4. A return on investment rate

105. Which of the following is not typically included in a prehire screening process?
1. A drug test
2. A background check
3. Social media review
4. Fitness evaluation

106. The $(ISC)^2$ code of ethics applies to all CISSP holders. Which of the following is not one of the four mandatory canons of the code?
1. Protect society, the common good, the necessary public trust and confidence, and the infrastructure
2. Disclose breaches of privacy, trust, and ethics
3. Provide diligent and competent service to the principles
4. Advance and protect the profession

107. Greg's company recently experienced a significant data breach involving the personal data of many of their customers. Which breach laws should they review to ensure that they are taking appropriate action?
1. The breach laws in the state where they are headquartered
2. The breach laws of states they do business in
3. Only federal breach laws
4. Breach laws only cover government agencies, not private businesses

108. Lawrence has been asked to perform vulnerability scans and a risk assessment of systems. Which organizational process are these more likely to be associated with?
1. A merger
2. A divestiture
3. A layoff
4. A financial audit

109. Which of the following is not typically part of a termination process?
1. An exit interview
2. Recovery of property
3. Account termination
4. Signing an NCA

110. Laura has been asked to perform an SCA. What type of organization is she most likely in?
1. Higher education
2. Banking
3. Government
4. Healthcare

111. After conducting a qualitative risk assessment of her organization, Sally recommends purchasing cybersecurity breach insurance. What type of risk response behavior is she recommending?
1. Accept
2. Transfer
3. Reduce
4. Reject

Chapter 2
Asset Security (Domain 2)

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 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. What term is used to describe a starting point for a minimum security standard?
    1. Outline
    2. Baseline
    3. Policy
    4. Configuration guide
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. Information 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. Susan works for an American company that conducts business with customers in the European Union. What is she likely to have to do if she is responsible for handling PII from those customers?
    1. Encrypt the data at all times.
    2. Label and classify the data according to HIPAA.
    3. Conduct yearly assessments to the PCI DSS standard.
    4. Comply with a standard such as the US-EU Privacy Shield.
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. What term is used to describe overwriting media to allow for its reuse in an environment operating at the same sensitivity level?
    1. Clearing
    2. Erasing
    3. Purging
    4. Sanitization
11. Which of the following classification levels is the United States (U.S.) government's classification label for data that could cause damage but wouldn't cause serious or grave damage?
    1. Top Secret
    2. Secret
    3. Confidential
    4. Classified
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. What term describes data that remains after attempts have been made to remove the data?
    1. Residual bytes
    2. Data remanence
    3. Slack space
    4. Zero fill

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 civilian data classifications best fit this data?
    1. Unclassified, confidential, top secret
    2. Public, sensitive, private
    3. Public, sensitive, proprietary
    4. Public, confidential, private
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 should you 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.
    2. The DLP system can adjust labels based on changes in the classification scheme.
    3. The DLP system can notify the firewall that traffic should be allowed through.
    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 proprietary information. Which option best describes what should happen at the end of their lifecycle for workstations he is responsible for?
    1. Erasing
    2. Clearing
    3. Sanitization
    4. Destruction
20. Rearrange the following U.S. government data classification levels in order, from least sensitive to most sensitive.
    1. Secret
    2. Confidential

3. Unclassified
4. Top Secret

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 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 what controls from the baseline a given system or software package should receive?
    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. What problem with FTP and Telnet makes using SFTP and SSH better alternatives?
    1. FTP and Telnet aren't installed on many systems.
    2. FTP and Telnet do not encrypt data.
    3. FTP and Telnet have known bugs and are no longer maintained.
    4. FTP and Telnet are difficult to use, making SFTP and SSH the preferred solution.
27. The government defense contractor that Saria 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 Saria 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 Saria 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. What is the primary information security risk to data at rest?
    1. Improper classification
    2. Data breach
    3. Decryption
    4. Loss of data integrity
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. Sue's employer has asked her to use an IPsec VPN to connect to its network. When Sue connects, what does the IPsec VPN allow her to do?
    1. Send decrypted data over a public network and act like she is on her employer's internal network.
    2. Create a private encrypted network carried via a public network and act like she is on her employer's internal network.
    3. Create a virtual private network using TLS while on her employer's internal network.
    4. Create a tunneled network that connects her employer's network to her internal home network
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
36. 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. Credit card numbers
    3. Social Security numbers
    4. Driver's license numbers

    Categories

    5. PCI DSS
    6. PHI
    7. PII

    For questions 37–39, please refer to the following scenario:

    The healthcare company that Lauren 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.
	Full disk encryption 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."

Classification	Handling Requirements
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.

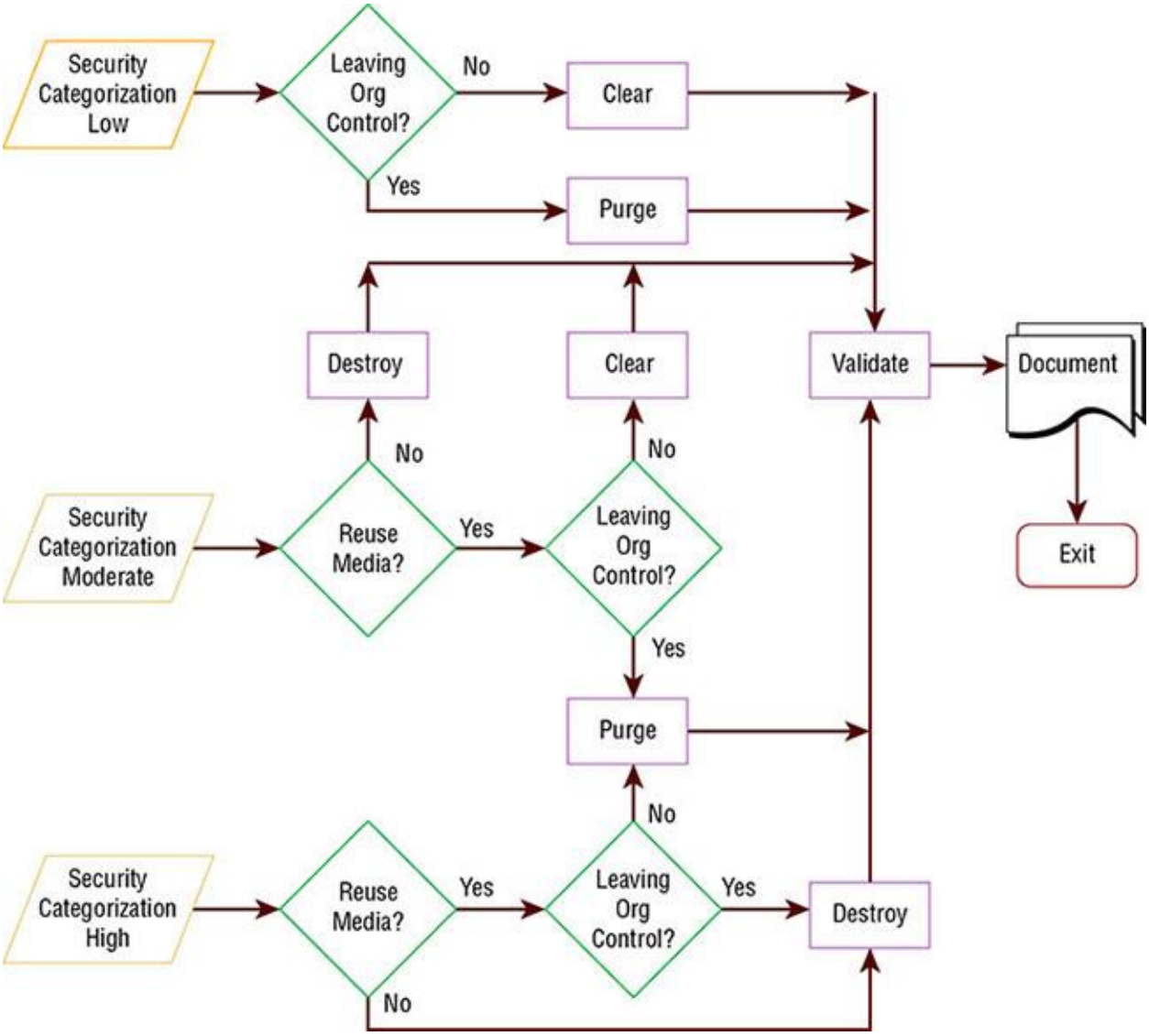
37. What encryption technology would be appropriate for HIPAA documents in transit?
    1. BitLocker
    2. DES
    3. TLS
    4. SSL
38. Lauren’s employer asks Lauren to classify patient X-ray data that has an internal patient identifier associated with it but does not have any way to directly identify 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 Lauren classify the data?
    1. Public
    2. Sensitive
    3. Private
    4. Confidential
39. What technology could Lauren’s employer implement to help prevent confidential data from being emailed out of the organization?
    1. DLP
    2. IDS
    3. A firewall
    4. UDP
40. A U.S. government database contains Secret, Confidential, and Top Secret data. How should it be classified?
    1. Top Secret
    2. Confidential
    3. Secret
    4. Mixed classification
41. What tool is used to prevent employees who leave from sharing proprietary information with their new employers?
    1. Encryption
    2. NDA
    3. Classification
    4. Purging
42. What encryption algorithm is used by both BitLocker and Microsoft’s Encrypting File System?
    1. Blowfish
    2. Serpent

3. AES
4. 3DES

43. 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.
44. What term is used to describe a set of common security configurations, often provided by a third party?
    1. Security policy
    2. Baseline
    3. DSS
    4. NIST SP 800-53
45. What type of policy describes how long data is retained and maintained before destruction?
    1. Classification
    2. Audit
    3. Record retention
    4. Availability
46. Which attack helped drive vendors to move away from SSL toward TLS-only by default?
    1. POODLE
    2. Stuxnet
    3. BEAST
    4. CRIME
47. 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.
48. 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 U.S. 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 not been changed.
    4. It validates who approved the data.
49. What protocol is preferred over Telnet for remote server administration via the command line?
    1. SCP

2. SFTP
3. WDS
4. SSH

50. What method uses a strong magnetic field to erase media?
    1. Magwipe
    2. Degaussing
    3. Sanitization
    4. Purging
51. 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
52. Alex works for a government agency that is required to meet U.S. federal government requirements for data security. To meet these requirements, Alex has been tasked with making sure data is identifiable by its classification level. 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.
53. 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

54. 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
55. 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

56. What U.S. government agency oversees compliance with the Privacy Shield framework for organizations wishing to use the personal data of EU citizens?
    1. The FAA
    2. The FDA
    3. The DoD
    4. The Department of Commerce

    For questions 57–59, 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:

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

57. 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.
58. 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.
59. 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
60. Which of the following is not one of the European Union's General Data Protection Regulation (GDPR) principles?
    1. Information must be processed fairly.
    2. Information must be deleted within one year of acquisition.
    3. Information must be maintained securely.

4. Information must be accurate.

61. Ben's company, which is based in the European Union, hires a third-party organization that processes data for it. Who has responsibility to protect the privacy of the data and ensure that it isn't used for anything other than its intended purpose?
    1. Ben's company is responsible.
    2. The third-party data processor is responsible.
    3. The data controller is responsible.
    4. Both organizations bear equal responsibility.
62. Major Hunter, a member of the armed forces, has been entrusted with information that, if exposed, could cause serious damage to national security. Under U.S. government classification standards, how should this data be classified?
    1. Unclassified
    2. Top Secret
    3. Confidential
    4. Secret
63. When a computer is removed from service and disposed of, the process that ensures that all storage media has been removed or destroyed is known as what?
    1. Sanitization
    2. Purging
    3. Destruction
    4. Declassification
64. Linux systems that use bcrypt are using a tool based on what DES alternative encryption scheme?
    1. 3DES
    2. AES
    3. Diffie–Hellman
    4. Blowfish
65. 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.
66. 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
67. 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:

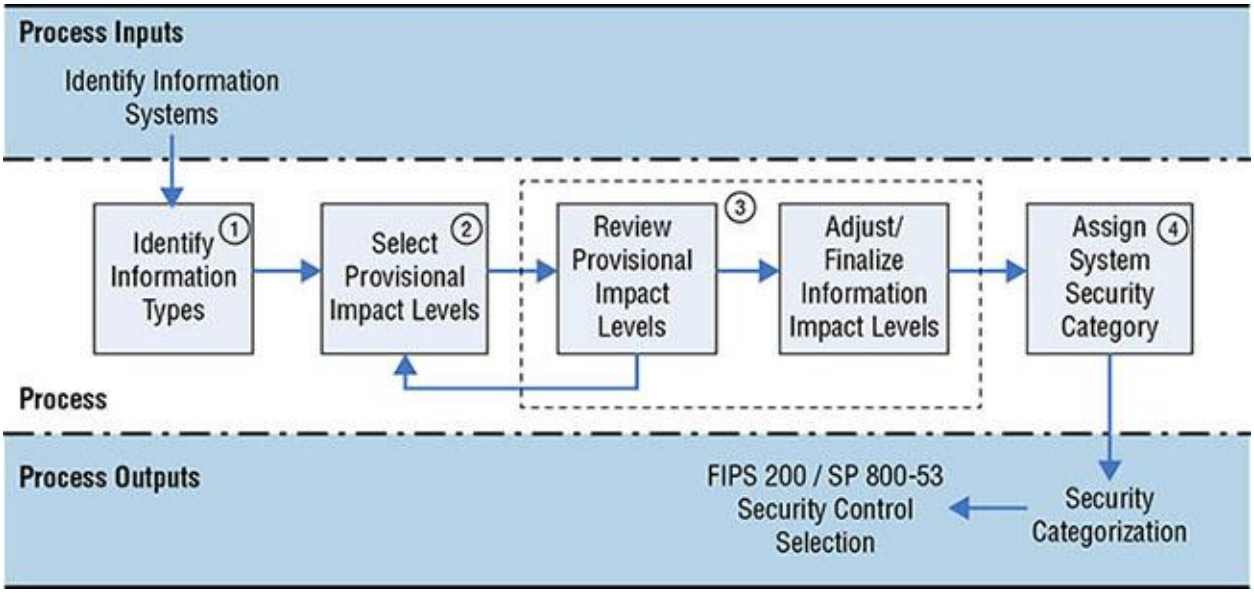
Source: Certificate of Sanitization.

1. Destruction
2. Reuse
3. Data remanence
4. Attribution

68. 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.

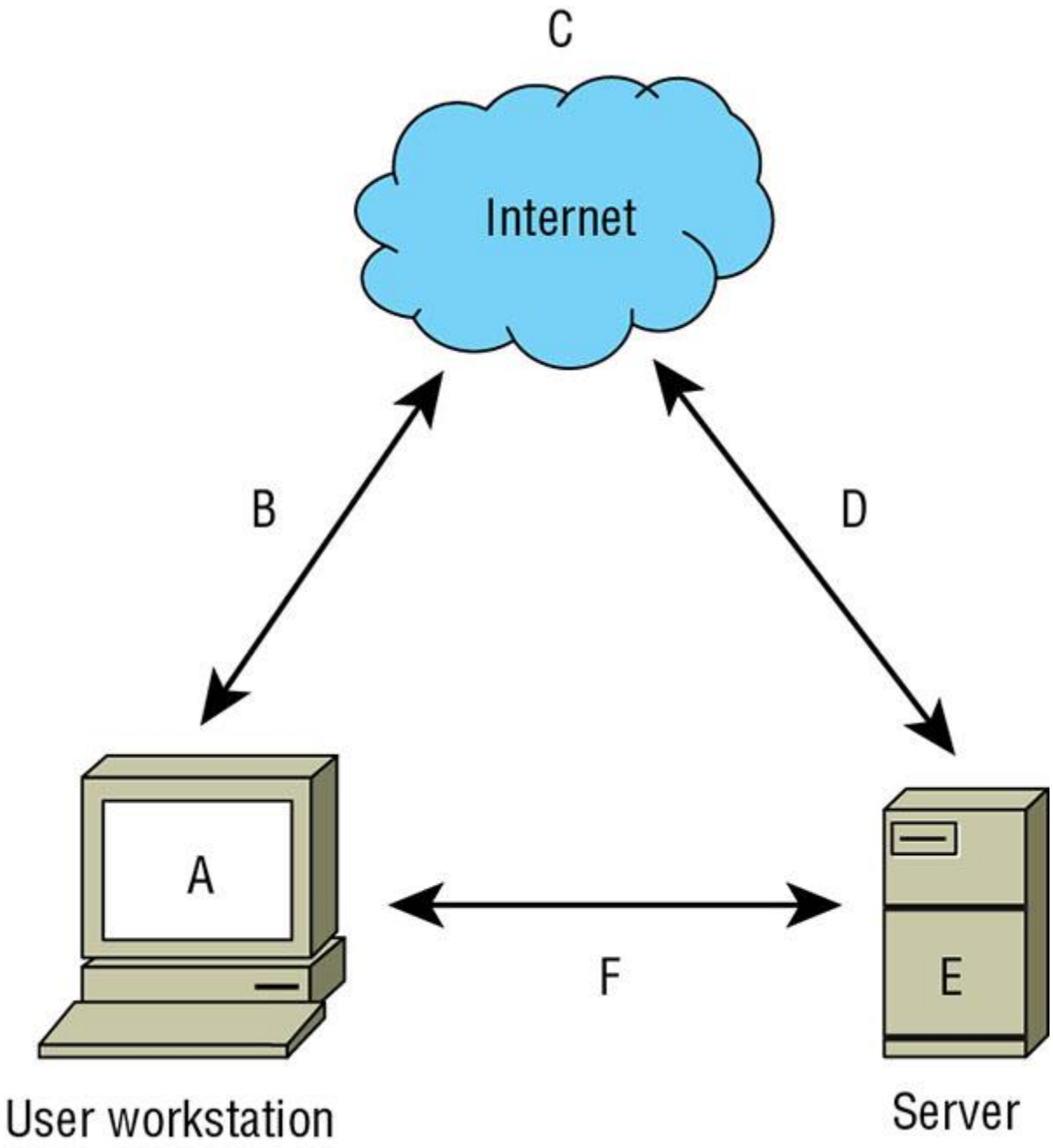
69. Incineration, crushing, shredding, and disintegration all describe what stage in the lifecycle of media?
    1. Sanitization
    2. Degaussing
    3. Purging
    4. Destruction
70. The European Union (EU) General Data Protection Regulation (GDPR) does not include which of the following key elements?
    1. The need to collect information for specified, explicit, and legitimate purposes
    2. The need to ensure that collection is limited to the information necessary to achieve the stated purpose
    3. The need to protect data against accidental destruction
    4. The need to encrypt information at rest
71. 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
72. 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.
73. Which of the following tasks are 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
74. NIST SP 800-60 provides a process shown in the following diagram to assess information systems. What process does this diagram show?



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 75–77, please refer to this diagram.



75. 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
76. What would be the best way to secure data at points B, D, and F?
    1. AES-256
    2. SSL
    3. TLS
    4. 3DES

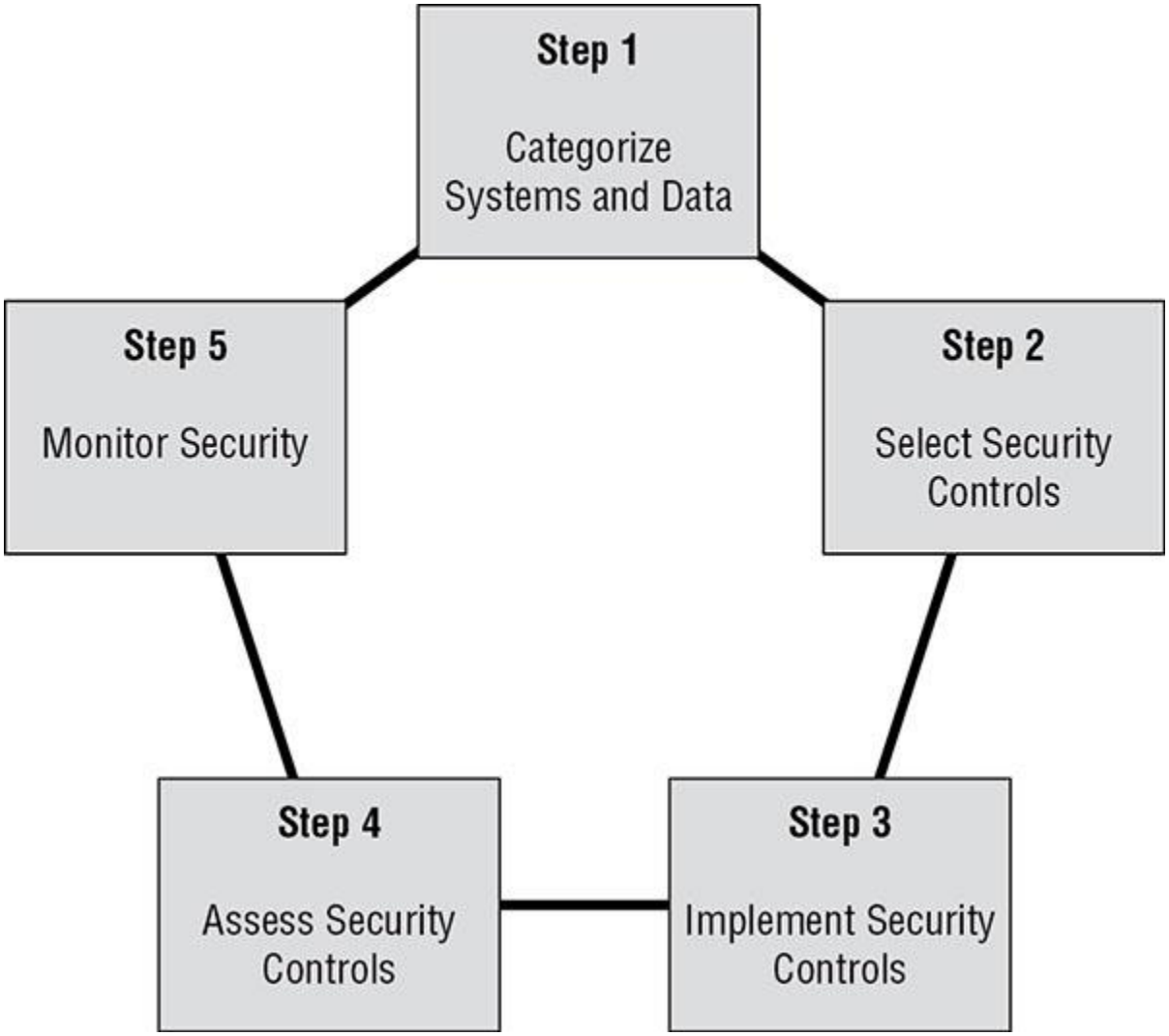
77. What is the best way to secure files that are sent from workstation A via the internet service (C) to remote server E?
    1. Use AES at rest at point A, and use TLS in transit via B and D.
    2. Encrypt the data files and send them.
    3. Use 3DES and TLS to provide double security.
    4. Use full disk encryption at A and E, and use SSL at B and D.
78. 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.
79. What term describes the process of reviewing baseline security controls and selecting only the controls that are appropriate for the IT system you are trying to protect?
    1. Standard creation
    2. CIS benchmarking
    3. Baselining
    4. Scoping
80. What data role does a system that is used to process data have?
    1. Mission owner
    2. Data owner
    3. Data processor
    4. Custodian
81. Which one of the following is not considered PII under U.S. federal government regulations?
    1. Name
    2. Social security number
    3. Student ID number
    4. ZIP code
82. What type of health information is the Health Insurance Portability and Accountability Act required to protect?
    1. PII
    2. PHI
    3. SHI
    4. HPHI
83. What encryption algorithm would provide strong protection for data stored on a USB thumb drive?
    1. TLS
    2. SHA1
    3. AES
    4. DES
84. Lauren’s multinational company wants to ensure compliance with the EU GDPR. Which principle of the GDPR states that the individual should have the right to receive personal information concerning himself or herself and share it with another data controller?
    1. Onward transfer
    2. Data integrity

3. Enforcement
4. Data portability

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

For questions 86–88, 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.



86. 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
87. 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
88. What data security role is primarily responsible for step 5?
    1. Data owners
    2. Data processors
    3. Custodians
    4. Users
89. Susan's organization performs a zero fill 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 remanence while at the third-party site
    2. Mishandling of drives by the third party
    3. Classification mistakes
    4. Data permanence
90. Embedded data used to help identify the owner of a file is an example of what type of label?
    1. Copyright notice
    2. DLP
    3. Digital watermark
    4. Steganography
91. 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
92. 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
93. What type of encryption is typically used for data at rest?
    1. Asymmetric encryption
    2. Symmetric encryption
    3. DES
    4. OTP
94. Which data role is tasked with granting appropriate access to staff members?

1. Data processors
2. Business owners
3. Custodians
4. Administrators

95. Which California law requires conspicuously posted privacy policies on commercial websites that collect the personal information of California residents?
    1. The Personal Information Protection and Electronic Documents Act
    2. The California Online Privacy Protection Act
    3. California Online Web Privacy Act
    4. California Civil Code 1798.82
96. Fred is preparing to send backup tapes offsite 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.
97. 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
98. 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.
99. Ed has been asked to send data that his organization classifies as confidential and proprietary via email. What encryption technology would be appropriate to ensure that the contents of the files attached to the email remain confidential as they traverse the internet?
    1. SSL
    2. TLS
    3. PGP
    4. VPN
100. Which mapping correctly matches data classifications between nongovernment and government classification schemes?
    1. Top Secret – Confidential/Proprietary
    - Secret – Private
    - Confidential – Sensitive

    2. Secret – Business confidential

- Classified – Proprietary
- Confidential – Business internal

3. Top Secret – Business sensitive

- Secret – Business internal
- Confidential – Business proprietary

4. Secret – Proprietary

- Classified – Private
- Unclassified – Public

Chapter 3
Security Architecture and Engineering (Domain 3)

1. Matthew is the security administrator for a consulting firm and must enforce access controls that restrict users' access based upon their previous activity. For example, once a consultant accesses data belonging to Acme Cola, a consulting client, they may no longer access data belonging to any of Acme's competitors. What security model best fits Matthew's needs?
    1. Clark-Wilson
    2. Biba
    3. Bell-LaPadula
    4. Brewer-Nash
2. Referring to the figure shown here, what is the earliest stage of a fire where it is possible to use detection technology to identify it?

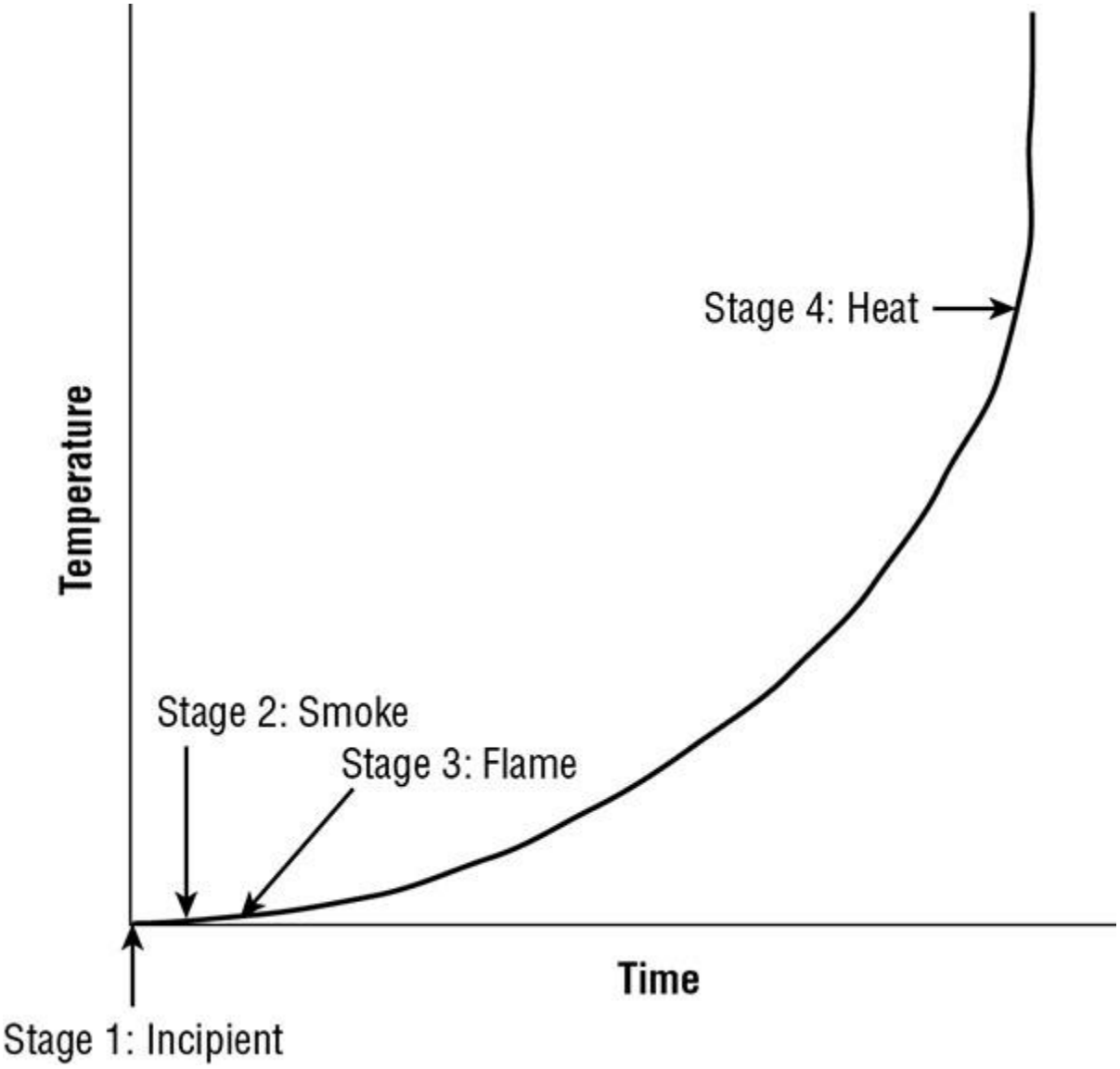


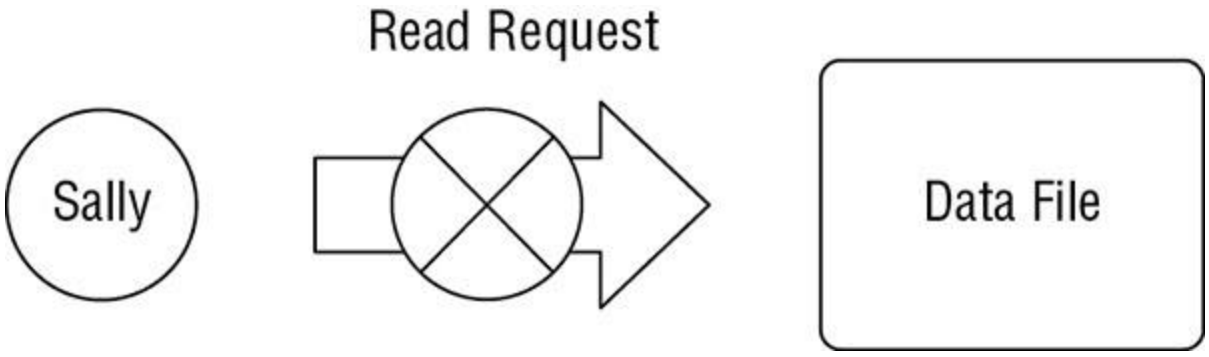
Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Incipient
2. Smoke
3. Flame
4. Heat

3. Ralph is designing a physical security infrastructure for a new computing facility that will remain largely unstaffed. He plans to implement motion detectors in the facility but would also like to include a secondary verification control for physical presence. Which one of the following would best meet his needs?
    1. CCTV
    2. IPS
    3. Turnstiles

    4. Faraday cages
4. Harry would like to retrieve a lost encryption key from a database that uses m of n control, with m = 4 and n = 8. What is the minimum number of escrow agents required to retrieve the key?
    1. 2
    2. 4
    3. 8
    4. 12
5. Fran's company is considering purchasing a web-based email service from a vendor and eliminating its own email server environment as a cost-saving measure. What type of cloud computing environment is Fran's company considering?
    1. SaaS
    2. IaaS
    3. CaaS
    4. PaaS
6. Bob is a security administrator with the federal government and wishes to choose a digital signature approach that is an approved part of the federal Digital Signature Standard under FIPS 186-4. Which one of the following encryption algorithms is not an acceptable choice for use in digital signatures?
    1. DSA
    2. HAVAL
    3. RSA
    4. ECDSA
7. Harry would like to access a document owned by Sally and stored on a file server. Applying the subject/object model to this scenario, who or what is the subject of the resource request?
    1. Harry
    2. Sally
    3. Server
    4. Document
8. Michael is responsible for forensic investigations and is investigating a medium-severity security incident that involved the defacement of a corporate website. The web server in question ran on a virtualization platform, and the marketing team would like to get the website up and running as quickly as possible. What would be the most reasonable next step for Michael to take?
    1. Keep the website offline until the investigation is complete.
    2. Take the virtualization platform offline as evidence.
    3. Take a snapshot of the compromised system and use that for the investigation.
    4. Ignore the incident and focus on quickly restoring the website.
9. Helen is a software engineer and is developing code that she would like to restrict to running within an isolated sandbox for security purposes. What software development technique is Helen using?
    1. Bounds
    2. Input validation
    3. Confinement
    4. TCB

10. What concept describes the degree of confidence that an organization has that its controls satisfy security requirements?
    1. Trust
    2. Credentialing
    3. Verification
    4. Assurance
11. What type of security vulnerability are developers most likely to introduce into code when they seek to facilitate their own access, for testing purposes, to software they developed?
    1. Maintenance hook
    2. Cross-site scripting
    3. SQL injection
    4. Buffer overflow
12. In the figure shown here, Sally is blocked from reading the file due to the Biba integrity model. Sally has a Secret security clearance, and the file has a Confidential classification. What principle of the Biba model is being enforced?



    1. Simple Security Property
    2. Simple Integrity Property
    3. *-Security Property
    4. *-Integrity Property
13. Tom is responsible for maintaining the security of systems used to control industrial processes located within a power plant. What term is used to describe these systems?
    1. POWER
    2. SCADA
    3. HAVAL
    4. COBOL
14. Sonia recently removed an encrypted hard drive from a laptop and moved it to a new device because of a hardware failure. She is having difficulty accessing encrypted content on the drive despite the fact that she knows the user's password. What hardware security feature is likely causing this problem?
    1. TCB
    2. TPM
    3. NIACAP
    4. RSA

15. Chris wants to verify that a software package that he downloaded matches the original version. What hashing tool should he use if he believes that technically sophisticated attackers may have replaced the software package with a version containing a backdoor?
    1. MD5
    2. 3DES
    3. SHA1
    4. SHA 256

    For questions 16–19, please refer to the following scenario:

    Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

16. If Alice wishes to send Bob an encrypted message, what key does she use to encrypt the message?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
17. When Bob receives the encrypted message from Alice, what key does he use to decrypt the message?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
18. Which one of the following keys would Bob not possess in this scenario?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
19. Alice would also like to digitally sign the message that she sends to Bob. What key should she use to create the digital signature?
    1. Alice's public key
    2. Alice's private key
    3. Bob's public key
    4. Bob's private key
20. What name is given to the random value added to a password in an attempt to defeat rainbow table attacks?
    1. Hash
    2. Salt
    3. Extender
    4. Rebar
21. Which one of the following is not an attribute of a hashing algorithm?
    1. They require a cryptographic key.

2. They are irreversible.
3. It is very difficult to find two messages with the same hash value.
4. They take variable-length input.

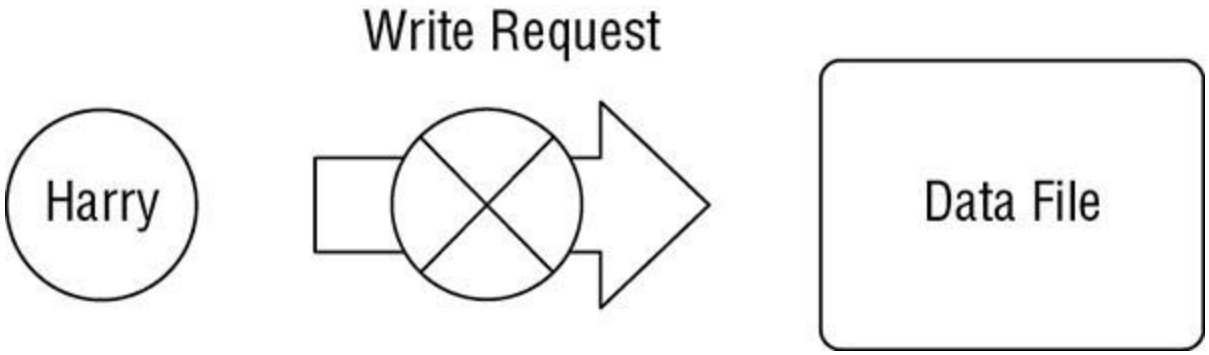
22. What type of fire suppression system fills with water when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water?
    1. Wet pipe
    2. Dry pipe
    3. Deluge
    4. Preaction
23. Susan would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?
    1. AH
    2. ESP
    3. IKE
    4. ISAKMP
24. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?
    1. Nonrepudiation
    2. Authentication
    3. Integrity
    4. Confidentiality
25. What logical operation is described by the truth table shown here?

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

    1. OR
    2. AND
    3. XOR
    4. NOR
26. How many bits of keying material does the Data Encryption Standard use for encrypting information?
    1. 56 bits

2. 64 bits
3. 128 bits
4. 256 bits

27. In the figure shown here, Harry's request to write to the data file is blocked. Harry has a Secret security clearance, and the data file has a Confidential classification. What principle of the Bell-LaPadula model blocked this request?



1. Simple Security Property
2. Simple Integrity Property
3. *-Security Property
4. Discretionary Security Property

28. Florian and Tobias would like to begin communicating using a symmetric cryptosystem, but they have no prearranged secret and are not able to meet in person to exchange keys. What algorithm can they use to securely exchange the secret key?
    1. IDEA
    2. Diffie-Hellman
    3. RSA
    4. MD5
29. Under the Common Criteria, what element describes the security requirements for a product?
    1. TCSEC
    2. ITSEC
    3. PP
    4. ST
30. Which one of the following is not one of the basic requirements for a cryptographic hash function?
    1. The function must work on fixed-length input.
    2. The function must be relatively easy to compute for any input.
    3. The function must be one way.
    4. The function must be collision free.
31. How many possible keys exist for a cipher that uses a key containing 5 bits?
    1. 10
    2. 16
    3. 32
    4. 64

32. What cryptographic principle stands behind the idea that cryptographic algorithms should be open to public inspection?
    1. Security through obscurity
    2. Kerckhoff's principle
    3. Defense in depth
    4. Heisenburg principle
33. Referring to the figure shown here, what is the name of the security control indicated by the arrow?

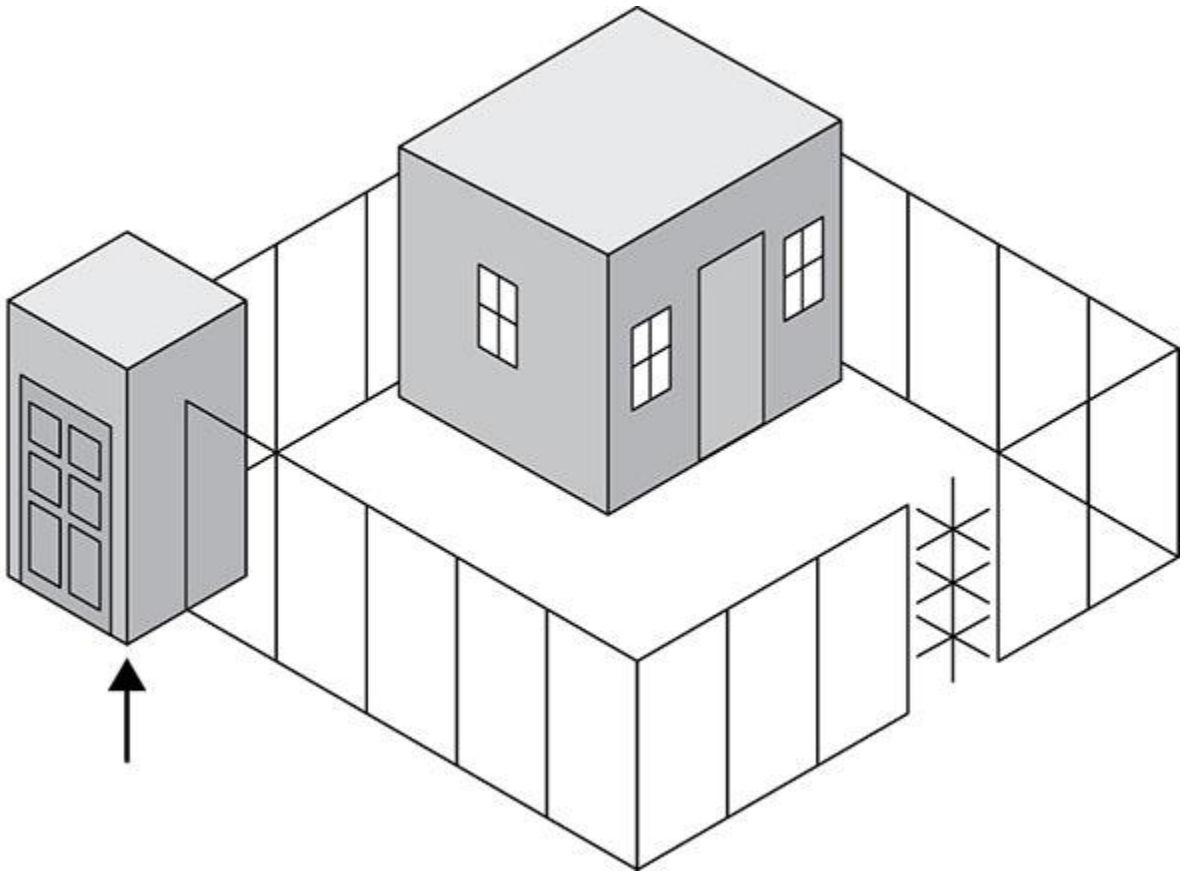
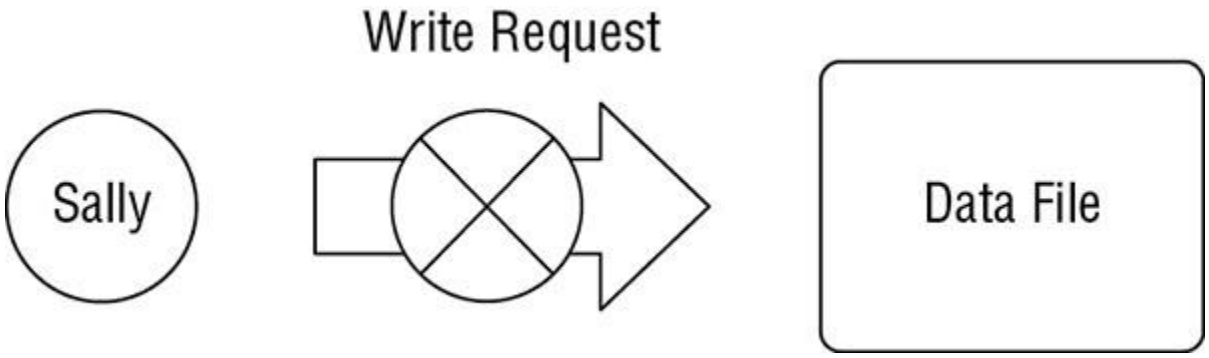


Image reprinted from *CISSP (ISC)* [2] *Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

    1. Mantrap
    2. Turnstile
    3. Intrusion prevention system
    4. Portal
34. Which one of the following does not describe a standard physical security requirement for wiring closets?
    1. Place only in areas monitored by security guards.
    2. Do not store flammable items in the closet.
    3. Use sensors on doors to log entries.
    4. Perform regular inspections of the closet.

35. In the figure shown here, Sally is blocked from writing to the data file by the Biba integrity model. Sally has a Secret security clearance, and the file is classified Top Secret. What principle is preventing her from writing to the file?



    1. Simple Security Property
    2. Simple Integrity Property
    3. *-Security Property
    4. *-Integrity Property

36. Match each of these following numbered architecture security concepts with the appropriate lettered description:

    Architectural security concepts

    1. Time of check
    2. Covert channel
    3. Time of use
    4. Maintenance hooks
    5. Parameter checking
    6. Race condition

    Descriptions

    7. A method used to pass information over a path not normally used for communication
    8. The exploitation of the difference between time of check and time of use
    9. The time at which the subject checks whether an object is available
    10. The time at which a subject can access an object
    11. An access method known only to the developer of the system
    12. A method that can help prevent buffer overflow attacks

37. What is the minimum number of independent parties necessary to implement the Fair Cryptosystems approach to key escrow?
    1. 1
    2. 2
    3. 3
    4. 4

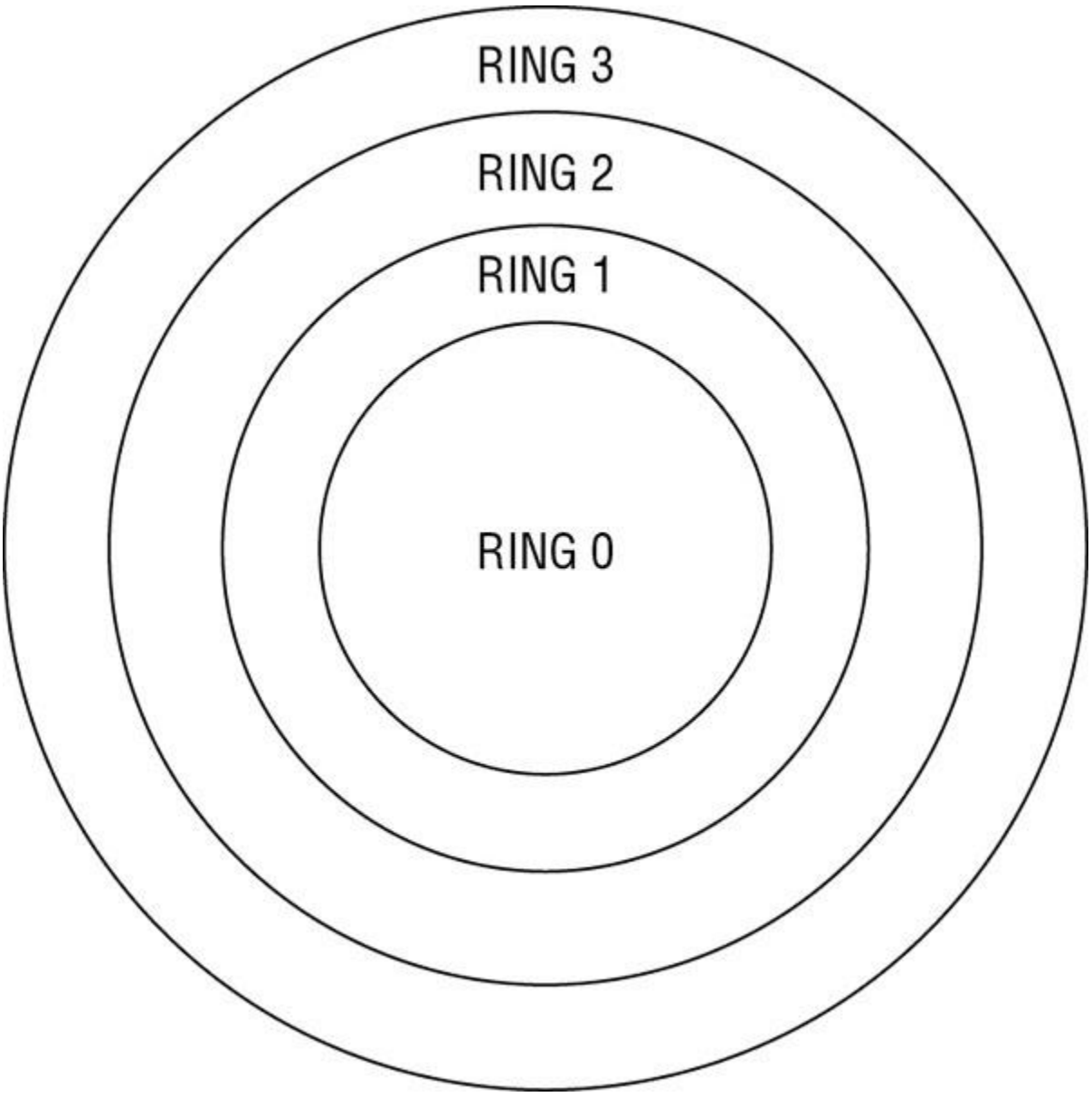
38. In what state does a processor's scheduler place a process when it is prepared to execute but the CPU is not currently available?
    1. Ready
    2. Running
    3. Waiting
    4. Stopped
39. Alan is reviewing a system that has been assigned the EAL1 evaluation assurance level under the Common Criteria. What is the degree of assurance that he may have about the system?
    1. It has been functionally tested.
    2. It has been structurally tested.
    3. It has been formally verified, designed, and tested.
    4. It has been methodically designed, tested, and reviewed.
40. Which one of the following components is used to assign classifications to objects in a mandatory access control system?
    1. Security label
    2. Security token
    3. Security descriptor
    4. Security capability
41. What type of software program exposes the code to anyone who wishes to inspect it?
    1. Closed source
    2. Open source
    3. Fixed source
    4. Unrestricted source
42. Adam recently configured permissions on an NTFS filesystem to describe the access that different users may have to a file by listing each user individually. What did Adam create?
    1. An access control list
    2. An access control entry
    3. Role-based access control
    4. Mandatory access control
43. Betty is concerned about the use of buffer overflow attacks against a custom application developed for use in her organization. What security control would provide the strongest defense against these attacks?
    1. Firewall
    2. Intrusion detection system
    3. Parameter checking
    4. Vulnerability scanning
44. Which one of the following terms is not used to describe a privileged mode of system operation?
    1. User mode
    2. Kernel mode
    3. Supervisory mode
    4. System mode

45. James is working with a Department of Defense system that is authorized to simultaneously handle information classified at the Secret and Top Secret levels. What type of system is he using?
    1. Single state
    2. Unclassified
    3. Compartmented
    4. Multistate
46. Kyle is being granted access to a military computer system that uses System High mode. What is not true about Kyle's security clearance requirements?
    1. Kyle must have a clearance for the highest level of classification processed by the system, regardless of his access.
    2. Kyle must have access approval for all information processed by the system.
    3. Kyle must have a valid need to know for all information processed by the system.
    4. Kyle must have a valid security clearance.
47. Gary intercepts a communication between two individuals and suspects that they are exchanging secret messages. The content of the communication appears to be the image shown here. What type of technique may the individuals use to hide messages inside this image?

    1. Visual cryptography
    2. Steganography
    3. Cryptographic hashing
    4. Transport layer security
48. Which one of the following terms accurately describes the Caesar cipher?
    1. Transposition cipher
    2. Block cipher
    3. Shift cipher

4. Strong cipher

49. In the ring protection model shown here, what ring contains the operating system's kernel?



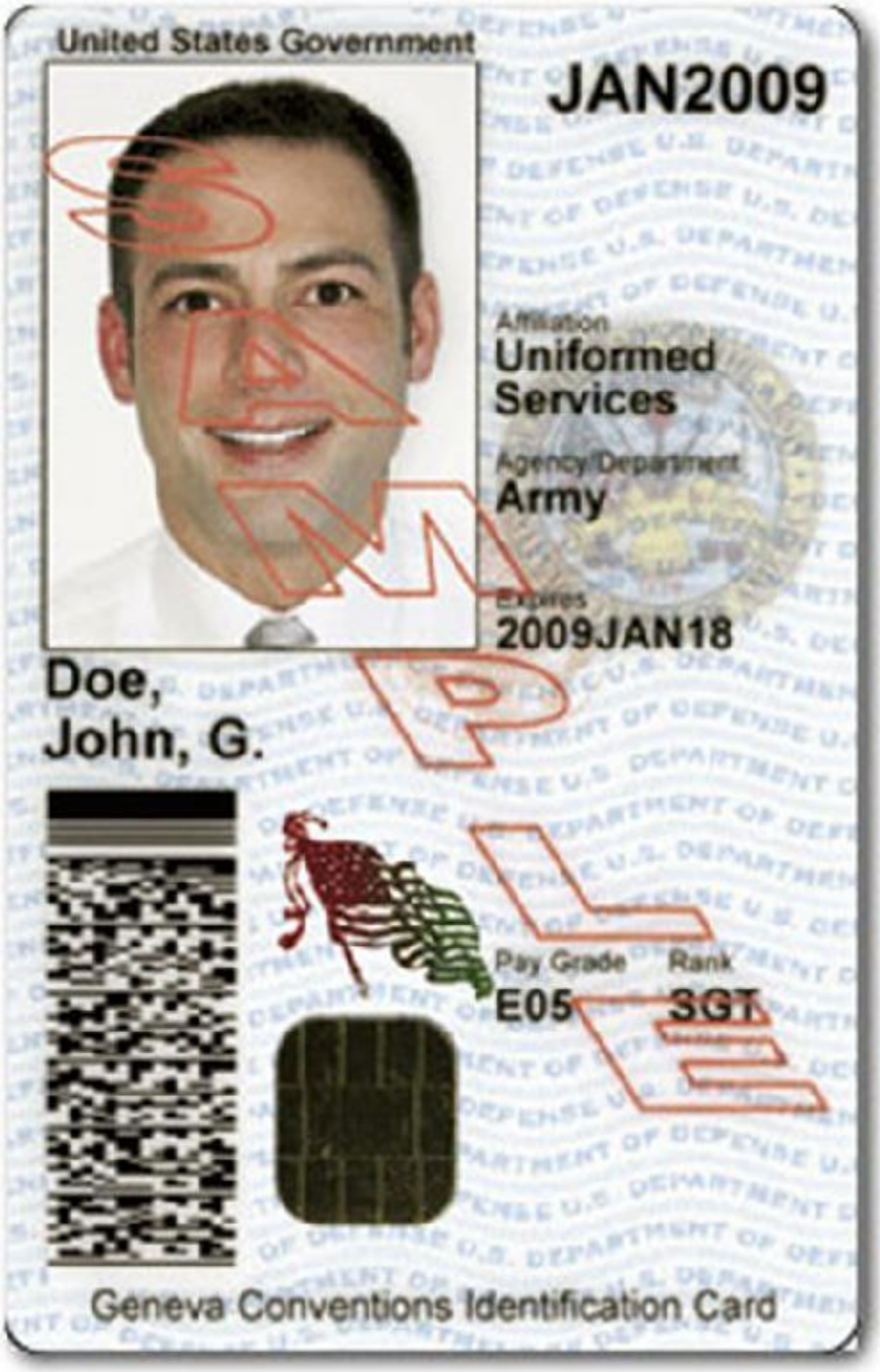
1. Ring 0
2. Ring 1
3. Ring 2
4. Ring 3

50. In an infrastructure as a service (IaaS) environment where a vendor supplies a customer with access to storage services, who is normally responsible for removing sensitive data from drives that are taken out of service?
    1. Customer's security team
    2. Customer's storage team

3. Customer's vendor management team
4. Vendor

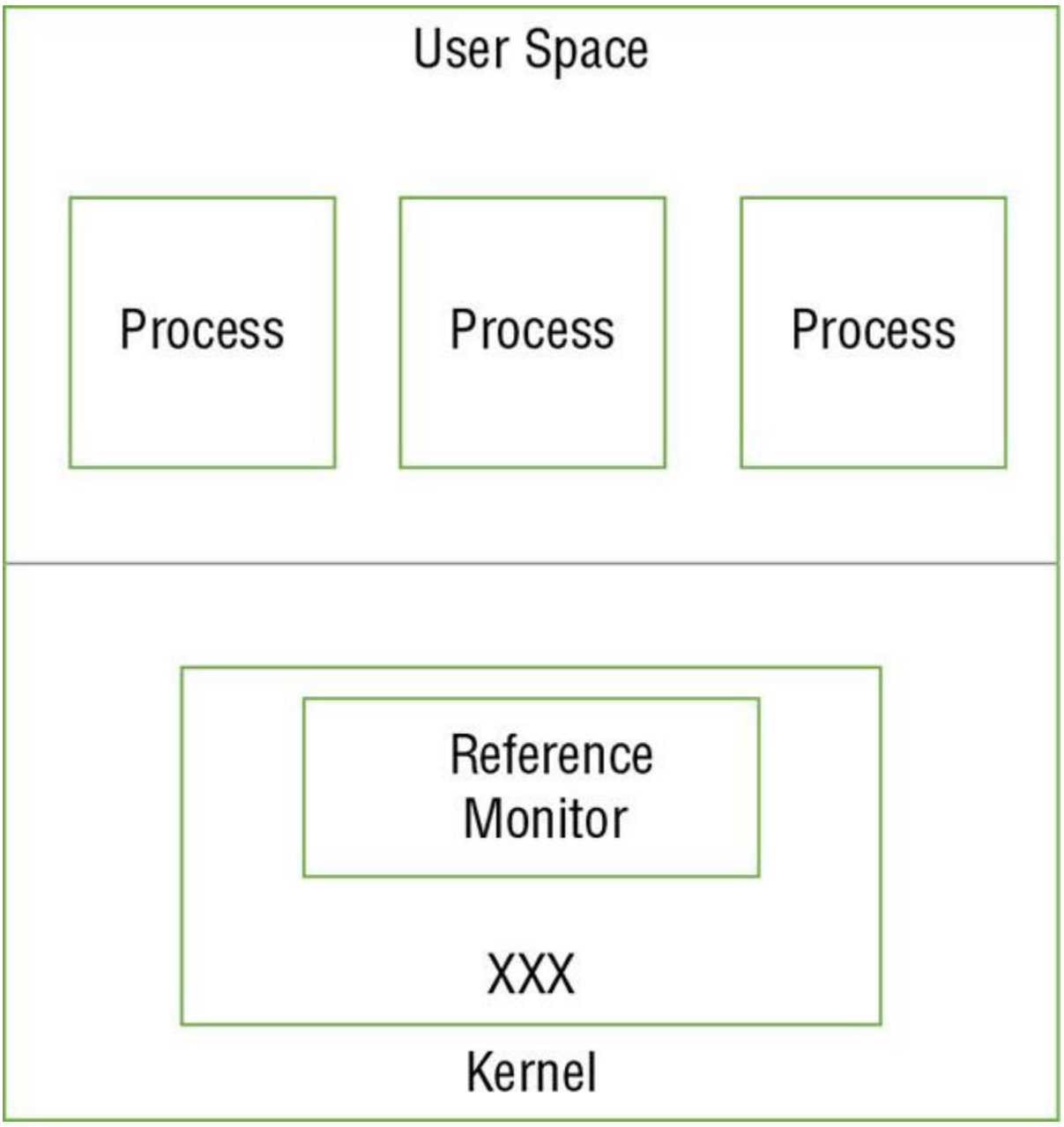
51. Which one of the following is an example of a code, not a cipher?
    1. Data Encryption Standard
    2. "One if by land; two if by sea"
    3. Shifting letters by three
    4. Word scramble
52. Which one of the following systems assurance processes provides an independent third-party evaluation of a system's controls that may be trusted by many different organizations?
    1. Certification
    2. Definition
    3. Verification
    4. Accreditation
53. Process _____ ensures that any behavior will affect only the memory and resources associated with a process.
    1. Restriction
    2. Isolation
    3. Limitation
    4. Parameters
54. Harold is assessing the susceptibility of his environment to hardware failures and would like to identify the expected lifetime of a piece of hardware. What measure should he use for this?
    1. MTTR
    2. MTTF
    3. RTO
    4. MTO
55. What type of fire extinguisher is useful only against common combustibles?
    1. Class A
    2. Class B
    3. Class C
    4. Class D
56. Gary is concerned about applying consistent security settings to the many mobile devices used throughout his organization. What technology would best assist with this challenge?
    1. MDM
    2. IPS
    3. IDS
    4. SIEM
57. Alice sent a message to Bob. Bob would like to demonstrate to Charlie that the message he received definitely came from Alice. What goal of cryptography is Bob attempting to achieve?
    1. Authentication
    2. Confidentiality
    3. Nonrepudiation
    4. Integrity

58. Rhonda is considering the use of new identification cards for physical access control in her organization. She comes across a military system that uses the card shown here. What type of card is this?



1. Smart card
2. Proximity card
3. Magnetic stripe card
4. Phase three card

59. Gordon is concerned about the possibility that hackers may be able to use the Van Eck radiation phenomenon to remotely read the contents of computer monitors in his facility. What technology would protect against this type of attack?
    1. TCSEC
    2. SCSI
    3. GHOST
    4. TEMPEST
60. In the diagram shown here of security boundaries within a computer system, what component's name has been replaced with XXX?



1. Kernel
2. TCB
3. Security perimeter
4. User execution

61. Sherry conducted an inventory of the cryptographic technologies in use within her organization and found the following algorithms and protocols in use. Which one of these technologies should she replace because it is no longer considered secure?
    1. MD5
    2. 3DES
    3. PGP
    4. WPA2

62. What action can you take to prevent accidental data disclosure due to wear leveling on an SSD device before reusing the drive?
    1. Reformatting
    2. Disk encryption
    3. Degaussing
    4. Physical destruction
63. Tom is a cryptanalyst and is working on breaking a cryptographic algorithm's secret key. He has a copy of an intercepted message that is encrypted, and he also has a copy of the decrypted version of that message. He wants to use both the encrypted message and its decrypted plaintext to retrieve the secret key for use in decrypting other messages. What type of attack is Tom engaging in?
    1. Chosen ciphertext
    2. Chosen plaintext
    3. Known plaintext
    4. Brute force
64. A hacker recently violated the integrity of data in James's company by modifying a file using a precise timing attack. The attacker waited until James verified the integrity of a file's contents using a hash value and then modified the file between the time that James verified the integrity and read the contents of the file. What type of attack took place?
    1. Social engineering
    2. TOCTOU
    3. Data diddling
    4. Parameter checking
65. What standard governs the creation and validation of digital certificates for use in a public key infrastructure?
    1. X.509
    2. TLS
    3. SSL
    4. 802.1x
66. What is the minimum fence height that makes a fence difficult to climb easily, deterring most intruders?
    1. 3 feet
    2. 4 feet
    3. 5 feet
    4. 6 feet
67. Johnson Widgets strictly limits access to total sales volume information, classifying it as a competitive secret. However, shipping clerks have unrestricted access to order records to facilitate transaction completion. A shipping clerk recently pulled all of the individual sales records for a quarter and totaled them up to determine the total sales volume. What type of attack occurred?
    1. Social engineering
    2. Inference
    3. Aggregation
    4. Data diddling
68. What physical security control broadcasts false emanations constantly to mask the presence of true electromagnetic emanations from computing equipment?

1. Faraday cage
2. Copper-infused windows
3. Shielded cabling
4. White noise

69. In a software as a service cloud computing environment, who is normally responsible for ensuring that appropriate firewall controls are in place to protect the application?
    1. Customer's security team
    2. Vendor
    3. Customer's networking team
    4. Customer's infrastructure management team
70. Alice has read permissions on an object, and she would like Bob to have those same rights. Which one of the rules in the Take-Grant protection model would allow her to complete this operation?
    1. Create rule
    2. Remove rule
    3. Grant rule
    4. Take rule
71. As part of his incident response process, Charles securely wipes the drive of a compromised machine and reinstalls the operating system (OS) from original media. Once he is done, he patches the machine fully and applies his organization's security templates before reconnecting the system to the network. Almost immediately after the system is returned to service, he discovers that it has reconnected to the same botnet it was part of before. Where should Charles look for the malware that is causing this behavior?
    1. The operating system partition
    2. The system BIOS or firmware
    3. The system memory
    4. The installation media
72. Which one of the following computing models allows the execution of multiple concurrent tasks within a single process?
    1. Multitasking
    2. Multiprocessing
    3. Multiprogramming
    4. Multithreading
73. Alan intercepts an encrypted message and wants to determine what type of algorithm was used to create the message. He first performs a frequency analysis and notes that the frequency of letters in the message closely matches the distribution of letters in the English language. What type of cipher was most likely used to create this message?
    1. Substitution cipher
    2. AES
    3. Transposition cipher
    4. 3DES
74. The Double DES (2DES) encryption algorithm was never used as a viable alternative to the original DES algorithm. What attack is 2DES vulnerable to that does not exist for the DES or 3DES approach?
    1. Chosen ciphertext

2. Brute force
3. Man in the middle
4. Meet in the middle

75. Grace would like to implement application control technology in her organization. Users often need to install new applications for research and testing purposes, and she does not want to interfere with that process. At the same time, she would like to block the use of known malicious software. What type of application control would be appropriate in this situation?
    1. Blacklisting
    2. Graylisting
    3. Whitelisting
    4. Bluelisting
76. Warren is designing a physical intrusion detection system for his data center and wants to include technology that issues an alert if the communications lines for the alarm system are unexpectedly cut. What technology would meet this requirement?
    1. Heartbeat sensor
    2. Emanation security
    3. Motion detector
    4. Faraday cage
77. John and Gary are negotiating a business transaction, and John must demonstrate to Gary that he has access to a system. He engages in an electronic version of the "magic door" scenario shown here. What technique is John using?

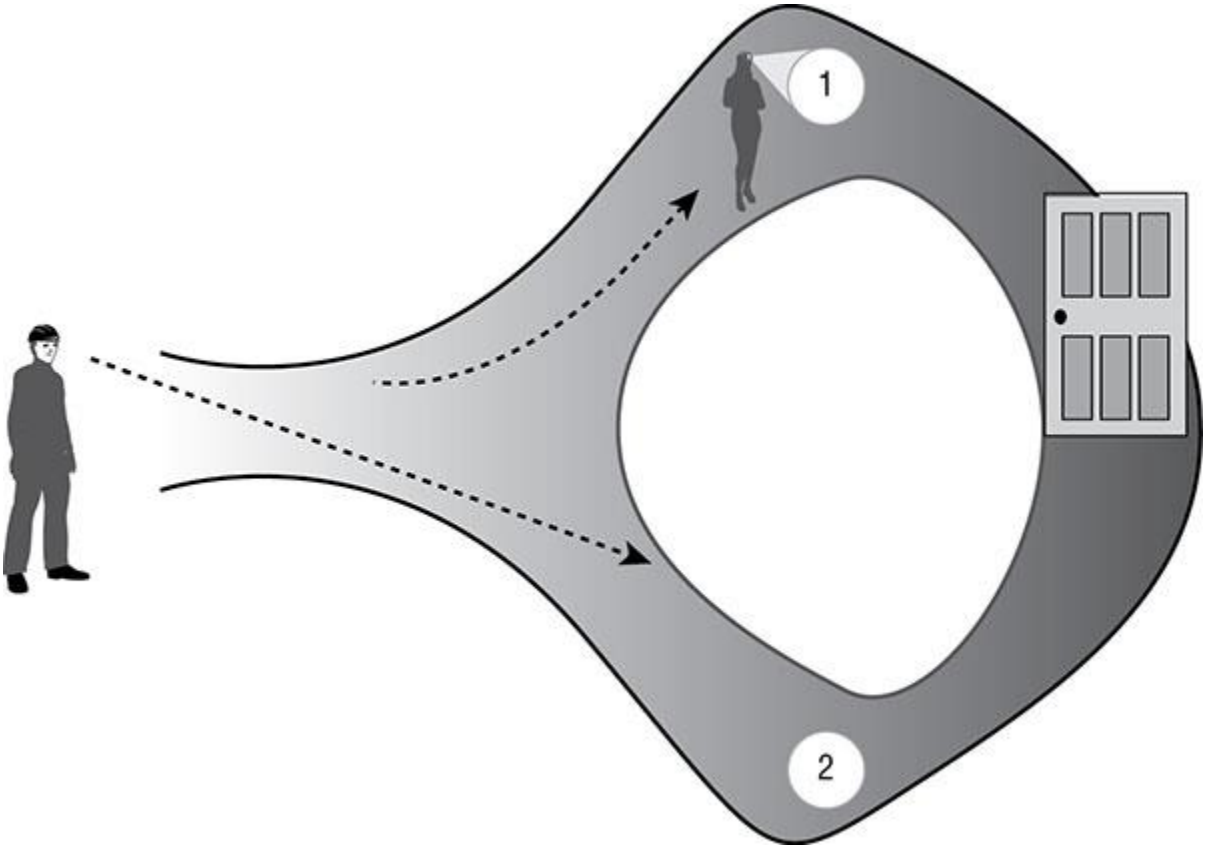


Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Split-knowledge proof
2. Zero-knowledge proof
3. Logical proof
4. Mathematical proof

78. Raj is selecting an encryption algorithm for use in his organization and would like to be able to vary the strength of the encryption with the sensitivity of the information. Which one of the following algorithms allows the use of different key strengths?
    1. Blowfish
    2. DES
    3. Skipjack
    4. IDEA
79. Referring to the fire triangle shown here, which one of the following suppression materials attacks a fire by removing the fuel source?

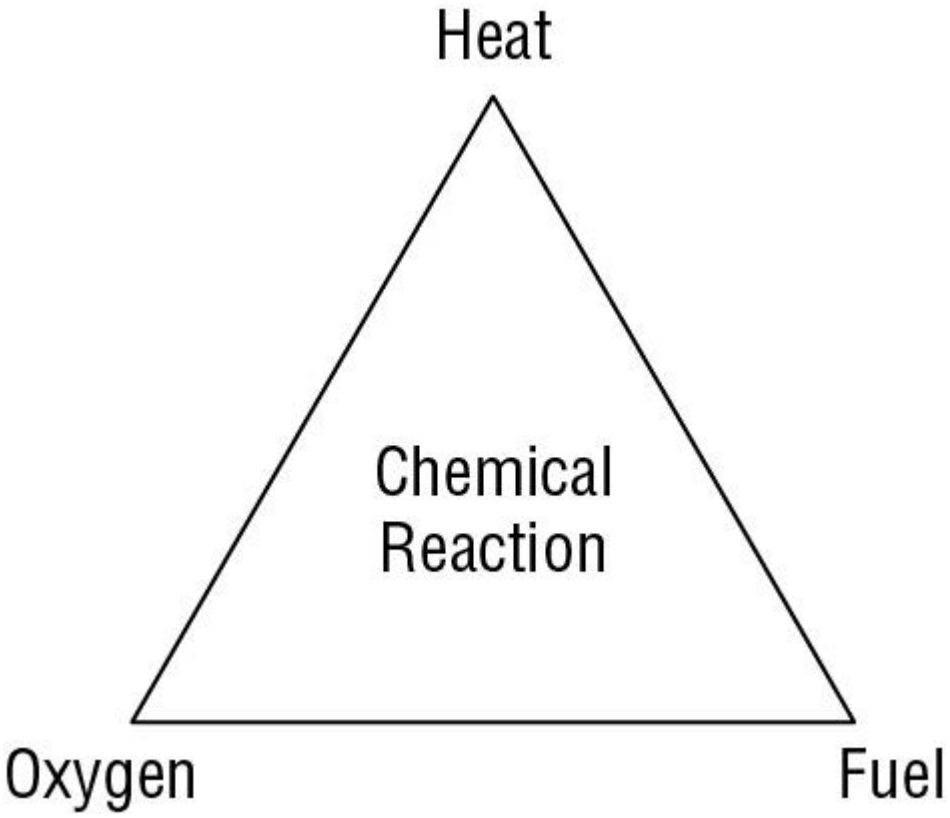


Image reprinted from *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

1. Water
2. Soda acid
3. Carbon dioxide

4. Halon

80. Howard is choosing a cryptographic algorithm for his organization, and he would like to choose an algorithm that supports the creation of digital signatures. Which one of the following algorithms would meet his requirement?
    1. RSA
    2. DES
    3. AES
    4. Blowfish
81. Laura is responsible for securing her company's web-based applications and wishes to conduct an educational program for developers on common web application security vulnerabilities. Where can she turn for a concise listing of the most common web application issues?
    1. CVE
    2. NSA
    3. OWASP
    4. CSA
82. The Bell-LaPadula and Biba models implement state machines in a fashion that uses what specific state machine model?
    1. Information flow
    2. Noninterference
    3. Cascading
    4. Feedback
83. The _____ of a process consist(s) of the limits set on the memory addresses and resources that the process may access.
    1. Perimeter
    2. Confinement limits
    3. Metes
    4. Bounds
84. What type of motion detector senses changes in the electromagnetic fields in monitored areas?
    1. Infrared
    2. Wave pattern
    3. Capacitance
    4. Photoelectric
85. Which one of the following fire suppression systems uses a suppressant that is no longer manufactured due to environmental concerns?
    1. FM-200
    2. Argon
    3. Inergen
    4. Halon
86. Which one of the following statements is correct about the Biba model of access control?
    1. It addresses confidentiality and integrity.
    2. It addresses integrity and availability.
    3. It prevents covert channel attacks.
    4. It focuses on protecting objects from integrity threats.

87. In Transport Layer Security, what type of key is used to encrypt the actual content of communications between a web server and a client?
    1. Ephemeral session key
    2. Client's public key
    3. Server's public key
    4. Server's private key
88. Beth would like to include technology in a secure area of her data center to protect against unwanted electromagnetic emanations. What technology would assist her with this goal?
    1. Heartbeat sensor
    2. Faraday cage
    3. Piggybacking
    4. WPA2
89. In a virtualized computing environment, what component is responsible for enforcing separation between guest machines?
    1. Guest operating system
    2. Hypervisor
    3. Kernel
    4. Protection manager
90. Rick is an application developer who works primarily in Python. He recently decided to evaluate a new service where he provides his Python code to a vendor who then executes it on their server environment. What type of cloud computing environment is this service?
    1. SaaS
    2. PaaS
    3. IaaS
    4. CaaS
91. A software company developed two systems that share information. System A provides information to the input of System B, which then reciprocates by providing information back to System A as input. What type of composition theory best describes this practice?
    1. Cascading
    2. Feedback
    3. Hookup
    4. Elementary
92. Tommy is planning to implement a power conditioning UPS for a rack of servers in his data center. Which one of the following conditions will the UPS be unable to protect against if it persists for an extended period of time?
    1. Fault
    2. Blackout
    3. Sag
    4. Noise
93. Which one of the following humidity values is within the acceptable range for a data center operation?
    1. 0%
    2. 10%
    3. 25%

4. 40%

94. Chris is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an asymmetric encryption system. How many total keys will they need?
    1. 500
    2. 1,000
    3. 2,000
    4. 4,950
95. What term is used to describe the formal declaration by a designated approving authority (DAA) that an information technology (IT) system is approved to operate in a specific environment?
    1. Certification
    2. Accreditation
    3. Evaluation
    4. Approval
96. Object-oriented programming languages use a black box approach to development, where users of an object do not necessarily need to know the object's implementation details. What term is used to describe this concept?
    1. Layering
    2. Abstraction
    3. Data hiding
    4. Process isolation
97. Todd wants to add a certificate to a certificate revocation list. What element of the certificate goes on the list?
    1. Serial number
    2. Public key
    3. Digital signature
    4. Private key
98. Alison is examining a digital certificate presented to her by her bank's website. Which one of the following requirements is not necessary for her to trust the digital certificate?
    1. She knows that the server belongs to the bank.
    2. She trusts the certificate authority.
    3. She verifies that the certificate is not listed on a CRL.
    4. She verifies the digital signature on the certificate.
99. Which one of the following is an example of a covert timing channel when used to exfiltrate information from an organization?
    1. Sending an electronic mail message
    2. Posting a file on a peer-to-peer file sharing service
    3. Typing with the rhythm of Morse code
    4. Writing data to a shared memory space
100. Which one of the following would be a reasonable application for the use of self-signed digital certificates?
    1. E-commerce website
    2. Banking application
    3. Internal scheduling application
    4. Customer portal

101. Mike has been tasked with preventing an outbreak of malware like Mirai. What type of systems should be protected in his organization?
    1. Servers
    2. SCADA
    3. Mobile devices
    4. Internet of Things (IoT) devices
102. A component failure in the primary HVAC system leads to a high temperature alarm in the data center that Kim manages. After resolving the issue, what should Kim consider to prevent future issues like this?
    1. A closed loop chiller
    2. Redundant cooling systems
    3. Swamp coolers
    4. Relocating the data center to a colder climate
103. As part of his team's forensic investigation process, Matt signs drives and other evidence out of storage before working with them. What type of documentation is he creating?
    1. Criminal
    2. Chain of custody
    3. Civil
    4. CYA
104. Lauren implements ASLR to help prevent system compromises. What technique has she used to protect her system?
    1. Encryption
    2. Mandatory access control
    3. Memory address randomization
    4. Discretionary access control
105. During a system audit, Casey notices that the private key for her organization's web server has been stored in a public Amazon S3 storage bucket for more than a year. What should she do?
    1. Remove the key from the bucket
    2. Notify all customers that their data may have been exposed
    3. Request a new certificate using a new key
    4. Nothing, because the private key should be accessible for validation
106. Joanna wants to review the status of the industrial control systems her organization uses for building control. What type of systems should she inquire about access to?
    1. SCADA
    2. DSS
    3. BAS
    4. ICS-CSS
107. After scanning all of the systems on his wireless network, Mike notices that one system is identified as an iOS device running a massively out-of-date version of Apple's mobile operating system. When he investigates further, he discovers that the device is an original iPad and that it cannot be updated to a current secure version of the operating system. What should Mike recommend?
    1. Retire or replace the device

2. Isolate the device on a dedicated wireless network
3. Install a firewall on the tablet
4. Reinstall the OS

108. During a third-party vulnerability scan and security test, Danielle's employer recently discovered that the embedded systems that were installed to manage her company's new buildings have a severe remote access vulnerability. The manufacturer has gone out of business, and there is no patch or update for the devices. What should Danielle recommend that her employer do about the hundreds of devices that are vulnerable?
    1. Identify a replacement device model and replace every device
    2. Turn off all of the devices
    3. Move the devices to a secured network segment
    4. Reverse engineer the devices and build an in-house patch

109. Alex's employer creates most of their work output as PDF files. Alex is concerned about limiting the audience for the PDF files to those individuals who have paid for them. What technology can he use to most effectively control the access to and distribution of these files?
    1. EDM
    2. Encryption
    3. Digital signatures
    4. DRM

110. Match the following numbered security models with the appropriate lettered security descriptions:

Security models

1. Clark-Wilson
2. Graham-Denning
3. Bell-LaPadula
4. Sutherland
5. Biba

Descriptions

6. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.
7. The * property of this model can be summarized as "no write-up."
8. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.
9. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or actions.
10. This integrity model focuses on preventing interference in support of integrity.

Chapter 1: Security and Risk Management (Domain 1)

1. D. The final step of a quantitative risk analysis is conducting a cost/benefit analysis to determine whether the organization should implement proposed countermeasure(s).
2. The wireless attack terms match with their descriptions as follows:
    1. Rogue access point: B. An access point intended to attract new connections by using an apparently legitimate SSID.
    2. Replay: C. An attack that retransmits captured communication to attempt to gain access to a targeted system.
    3. Evil twin: A. An attack that relies on an access point to spoof a legitimate access point's SSID and MAC address.
    4. War driving: D. The process of using detection tools to find wireless networks.
3. C. The DMCA states that providers are not responsible for the transitory activities of their users. Transmission of information over a network would qualify for this exemption. The other activities listed are all nontransitory actions that require remediation by the provider.
4. C. The right to be forgotten, also known as the right to erasure, guarantees the data subject the ability to have their information removed from processing or use. It may be tied to consent given for data processing; if a subject revokes consent for processing, the data controller may need to take additional steps, including erasure.
5. D. The three common threat modeling techniques are focused on attackers, software, and assets. Social engineering is a subset of attackers.
6. A. Most state data breach notification laws are modeled after California's law, which covers Social Security number, driver's license number, state identification card number, credit/debit card numbers, bank account numbers (in conjunction with a PIN or password), medical records, and health insurance information.
7. C. The prudent man rule requires that senior executives take personal responsibility for ensuring the due care that ordinary, prudent individuals would exercise in the same situation. The rule originally applied to financial matters, but the Federal Sentencing Guidelines applied them to information security matters in 1991.
8. D. A fingerprint scan is an example of a "something you are" factor, which would be appropriate for pairing with a "something you know" password to achieve multifactor authentication. A username is not an authentication factor. PINs and security questions are both "something you know," which would not achieve multifactor authentication when paired with a password because both methods would come from the same category, failing the requirement for multifactor authentication.
9. D. The US Department of Commerce is responsible for implementing the EU-U.S. Privacy Shield Agreement. This framework replaced an earlier framework known as Privacy Shield, which was ruled insufficient in the wake of the NSA surveillance disclosures.
10. A. The Gramm-Leach-Bliley Act (GLBA) contains provisions regulating the privacy of customer financial information. It applies specifically to financial institutions.
11. A. The Federal Information Security Management Act (FISMA) specifically applies to government contractors. The Government Information Security Reform Act (GISRA) was the precursor to FISMA and expired in November 2002. HIPAA and PCI DSS apply to healthcare and credit card information, respectively.
12. D. The export of encryption software to certain countries is regulated under US export control laws.

13. D. In an elevation of privilege attack, the attacker transforms a limited user account into an account with greater privileges, powers, and/or access to the system. Spoofing attacks falsify an identity, while repudiation attacks attempt to deny accountability for an action. Tampering attacks attempt to violate the integrity of information or resources.
14. D. Whenever you choose to accept a risk, you should maintain detailed documentation of the risk acceptance process to satisfy auditors in the future. This should happen before implementing security controls, designing a disaster recovery plan, or repeating the business impact analysis (BIA).
15. B. A fence does not have the ability to detect intrusions. It does, however, have the ability to prevent and deter an intrusion. Fences are an example of a physical control.
16. D. Tony would see the best results by combining elements of quantitative and qualitative risk assessment. Quantitative risk assessment excels at analyzing financial risk, while qualitative risk assessment is a good tool for intangible risks. Combining the two techniques provides a well-rounded risk picture.
17. D. The Economic Espionage Act imposes fines and jail sentences on anyone found guilty of stealing trade secrets from a US corporation. It gives true teeth to the intellectual property rights of trade secret owners.
18. C. The due care principle states that an individual should react in a situation using the same level of care that would be expected from any reasonable person. It is a very broad standard. The due diligence principle is a more specific component of due care that states that an individual assigned a responsibility should exercise due care to complete it accurately and in a timely manner.
19. C. RAID level 5, disk striping with parity, requires a minimum of three physical hard disks to operate.
20. B. Awareness training is an example of an administrative control. Firewalls and intrusion detection systems are technical controls. Security guards are physical controls.
21. A. Patents and trade secrets can both protect intellectual property related to a manufacturing process. Trade secrets are appropriate only when the details can be tightly controlled within an organization, so a patent is the appropriate solution in this case.
22. B. RAID technology provides fault tolerance for hard drive failures and is an example of a business continuity action. Restoring from backup tapes, relocating to a cold site, and restarting business operations are all disaster recovery actions.
23. C. After developing a list of assets, the business impact analysis team should assign values to each asset.
24. C. Risk mitigation strategies attempt to lower the probability and/or impact of a risk occurring. Intrusion prevention systems attempt to reduce the probability of a successful attack and are, therefore, examples of risk mitigation.
25. D. Fire suppression systems protect infrastructure from physical damage. Along with uninterruptible power supplies, fire suppression systems are good examples of technology used to harden physical infrastructure. Antivirus software, hardware firewalls, and two-factor authentication are all examples of logical controls.
26. A. Access control lists (ACLs) are used for determining a user's authorization level. Usernames are identification tools. Passwords and tokens are authentication tools.
27. D. Trademark protection extends to words and symbols used to represent an organization, product, or service in the marketplace.
28. A. The message displayed is an example of ransomware, which encrypts the contents of a user's computer to prevent legitimate use. This is an example of an availability attack.

29. B. A health and fitness application developer would not necessarily be collecting or processing healthcare data, and the terms of HIPAA do not apply to this category of business. HIPAA regulates three types of entities—healthcare providers, health information clearinghouses, and health insurance plans—as well as the business associates of any of those covered entities.
30. A. A smurf attack is an example of a denial of service attack, which jeopardizes the availability of a targeted network.
31. D. Strategic plans have a long-term planning horizon of up to five years in most cases. Operational and tactical plans have shorter horizons of a year or less.
32. A. The United States Patent and Trademark Office (USPTO) bears responsibility for the registration of trademarks.
33. B. When following the separation of duties principle, organizations divide critical tasks into discrete components and ensure that no one individual has the ability to perform both actions. This prevents a single rogue individual from performing that task in an unauthorized manner.
34. B. The Federal Information Security Management Act (FISMA) applies to federal government agencies and contractors. Of the entities listed, a defense contractor is the most likely to have government contracts subject to FISMA.
35. B. The Payment Card Industry Data Security Standard (PCI DSS) governs the storage, processing, and transmission of credit card information.
36. A. The data custodian role is assigned to an individual who is responsible for implementing the security controls defined by policy and senior management. The data owner does bear ultimate responsibility for these tasks, but the data owner is typically a senior leader who delegates operational responsibility to a data custodian.
37. B. Written works, such as website content, are normally protected by copyright law. Trade secret status would not be appropriate here because the content is online and available outside the company. Patents protect inventions, and trademarks protect words and symbols used to represent a brand, neither of which is relevant in this scenario.
38. C. The Code of Federal Regulations (CFR) contains the text of all administrative laws promulgated by federal agencies. The United States Code contains criminal and civil law. Supreme Court rulings contain interpretations of law and are not laws themselves. The Compendium of Laws does not exist.
39. D. Installing a device that will block attacks is an attempt to lower risk by reducing the likelihood of a successful application attack.
40. B. The owner of information security programs may be different from the individuals responsible for implementing the controls. This person should be as senior an individual as possible who is able to focus on the management of the security program. The president and CEO would not be an appropriate choice because an executive at this level is unlikely to have the time necessary to focus on security. Of the remaining choices, the CIO is the most senior position who would be the strongest advocate at the executive level.
41. A. Senior managers play several business continuity planning roles. These include setting priorities, obtaining resources, and arbitrating disputes among team members.
42. D. The Service Organizations Control audit program includes business continuity controls in a SOC 2, but not SOC 1, audit. Although FISMA and PCI DSS may audit business continuity, they would not apply to an email service used by a hospital.
43. A. Repudiation threats allow an attacker to deny having performed an action or activity without the other party being able to prove differently.
44. A. Integrity controls, such as the one Beth is implementing in this example, are designed to prevent the unauthorized modification of information.

45. A. SLAs do not normally address issues of data confidentiality. Those provisions are normally included in a nondisclosure agreement (NDA).
46. A. Trademarks protect words and images that represent a product or service and would not protect computer software.
47. B. Virtual private networks (VPNs) provide secure communications channels over otherwise insecure networks (such as the Internet) using encryption. If you establish a VPN connection between the two offices, users in one office could securely access content located on the other office's server over the Internet. Digital signatures are used to provide nonrepudiation, not confidentiality. Virtual LANs (VLANs) provide network segmentation on local networks but do not cross the Internet. Digital content management solutions are designed to manage web content, not access shared files located on a file server.
48. C. RAID uses additional hard drives to protect the server against the failure of a single device. Load balancing and server clustering do add robustness but require the addition of a server. Scheduled backups protect against data loss but do not provide immediate access to data in the event of a hard drive failure.
49. A. Hashing allows you to computationally verify that a file has not been modified between hash evaluations. ACLs and read-only attributes are useful controls that may help you prevent unauthorized modification, but they cannot verify that files were not modified. Firewalls are network security controls and do not verify file integrity.
50. B. The Fourth Amendment directly prohibits government agents from searching private property without a warrant and probable cause. The courts have expanded the interpretation of the Fourth Amendment to include protections against other invasions of privacy.
51. A. Business continuity plan documentation normally includes the continuity planning goals, a statement of importance, statement of priorities, statement of organizational responsibility, statement of urgency and timing, risk assessment and risk acceptance and mitigation documentation, a vital records program, emergency response guidelines, and documentation for maintaining and testing the plan.
52. D. Mandatory vacation programs require that employees take continuous periods of time off each year and revoke their system privileges during that time. This will hopefully disrupt any attempt to engage in the cover-up actions necessary to hide fraud and result in exposing the threat. Separation of duties, least privilege, and defense in depth controls all may help prevent the fraud in the first place but are unlikely to speed the detection of fraud that has already occurred.
53. C. Electronic vaulting is a data backup task that is part of disaster recovery, not business continuity, efforts.
54. C. Denial of service (DoS) attacks and distributed denial of service (DDoS) attacks try to disrupt the availability of information systems and networks by flooding a victim with traffic or otherwise disrupting service.
55. B. Baselines provide the minimum level of security that every system throughout the organization must meet.
56. C. Everyone in the organization should receive a basic awareness training for the business continuity program. Those with specific roles, such as first responders and senior executives, should also receive detailed, role-specific training.
57. C. If the organization's primary concern is the cost of rebuilding the data center, James should use the replacement cost method to determine the current market price for equivalent servers.
58. D. The Computer Security Act of 1987 gave the National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines for federal computer systems. For

this purpose, NIST draws upon the technical advice and assistance of the National Security Agency where appropriate.

59. B. There is no requirement that patents be for inventions made by American citizens. Patentable inventions must, on the other hand, be new, nonobvious, and useful.
60. A. Keyloggers monitor the keystrokes of an individual and report them back to an attacker. They are designed to steal sensitive information, a disruption of the goal of confidentiality.
61. A. Risks exist when there is an intersection of a threat and a vulnerability. This is described using the equation Risk = Threat * Vulnerability.
62. A. The fourth step of the NIST risk management framework is assessing security controls.
63. D. HAL Systems decided to stop offering the service because of the risk. This is an example of a risk avoidance strategy. The company altered its operations in a manner that eliminates the risk of NTP misuse.
64. C. Confidentiality controls prevent the disclosure of sensitive information to unauthorized individuals. Limiting the likelihood of a data breach is an attempt to prevent unauthorized disclosure.
65. A. The emergency response guidelines should include the immediate steps an organization should follow in response to an emergency situation. These include immediate response procedures, a list of individuals who should be notified of the emergency and secondary response procedures for first responders. They do not include long-term actions such as activating business continuity protocols, ordering equipment, or activating DR sites.
66. B. Although the CEO will not normally serve on a BCP team, it is best to obtain top-level management approval for your plan to increase the likelihood of successful adoption.
67. D. The project scope and planning phase includes four actions: a structured analysis of the organization, the creation of a BCP team, an assessment of available resources, and an analysis of the legal and regulatory landscape.
68. D. Keeping a server up and running is an example of an availability control because it increases the likelihood that a server will remain available to answer user requests.
69. A. A cold site includes the basic capabilities required for data center operations: space, power, HVAC, and communications, but it does not include any of the hardware required to restore operations.
70. C. The Computer Fraud and Abuse Act (CFAA) makes it a federal crime to maliciously cause damage in excess of $5,000 to a federal computer system during any one-year period.
71. B. ISO 27002 is an international standard focused on information security and titled "Information technology—Security techniques—Code of practice for information security management." The Information Technology Infrastructure Library (ITIL) does contain security management practices, but it is not the sole focus of the document, and the ITIL security section is derived from ISO 27002. The Capability Maturity Model (CMM) is focused on software development, and the Project Management Body of Knowledge (PMBOK) Guide focuses on project management.
72. B. The Communications Assistance to Law Enforcement Act (CALEA) requires that all communications carriers make wiretaps possible for law enforcement officials who have an appropriate court order.
73. B. The Gramm-Leach-Bliley Act (GLBA) places strict privacy regulations on financial institutions, including providing written notice of privacy practices to customers.
74. C. Nondisclosure agreements (NDAs) typically require either mutual or one-way confidentiality in a business relationship. Service-level agreements (SLAs) specify service uptime and other performance measures. Noncompete agreements (NCAs) limit the future employment

possibilities of employees. Recovery time objectives (RTOs) are used in business continuity planning.

75. D. Router ACLs, encryption, and firewall rules are all examples of technical controls. Data classification is an administrative control.
76. C. While senior management should be represented on the BCP team, it would be highly unusual for the CEO to fill this role personally.
77. D. Nonrepudiation allows a recipient to prove to a third party that a message came from a purported source. Authentication would provide proof to Ben that the sender was authentic, but Ben would not be able to prove this to a third party.
78. C. Defense in depth states that organizations should have overlapping security controls designed to meet the same security objectives whenever possible. This approach provides security in the event of a single control failure.
79. D. Stakeholders should be informed of changes before, not after, they occur. The other items listed are goals of change management programs.
80. B. Ben should encrypt the data to provide an additional layer of protection as a compensating control. The organization has already made a policy exception, so he should not react by objecting to the exception or removing the data without authorization. Purchasing insurance may transfer some of the risk but is not a mitigating control.
81. A. The risk assessment team should pay the most immediate attention to those risks that appear in quadrant I. These are the risks with a high probability of occurring and a high impact on the organization if they do occur.
82. D. Electronic access to company resources must be carefully coordinated. An employee who retains access after being terminated may use that access to take retaliatory action. On the other hand, if access is terminated too early, the employee may figure out that he or she is about to be terminated.
83. D. In a risk acceptance strategy, the organization decides that taking no action is the most beneficial route to managing a risk.
84. A. COPPA requires that websites obtain advance parental consent for the collection of personal information from children under the age of 13.
85. D. The annualized rate of occurrence (ARO) is the frequency at which you should expect a risk to materialize each year. In a 100-year flood plain, risk analysts expect a flood to occur once every 100 years, or 0.01 times per year.
86. D. Wireshark is a protocol analyzer and may be used to eavesdrop on network connections. Eavesdropping is an attack against confidentiality.
87. C. In reduction analysis, the security professional breaks the system down into five key elements: trust boundaries, data flow paths, input points, privileged operations, and details about security controls.
88. The laws or industry standards match to the descriptions as follows:
    1. GLBA: A. A US law that requires covered financial institutions to provide their customers with a privacy notice on a yearly basis.
    2. PCI DSS: C. An industry standard that covers organizations that handle credit cards.
    3. HIPAA: D. A US law that provides data privacy and security requirements for medical information.
    4. SOX: B. A US law that requires internal controls assessments including IT transaction flows for publicly traded companies.
89. D. Of the states listed, Florida is the only one that is not shaded to indicate a serious risk of a major earthquake.

90. C. Usernames are an identification tool. They are not secret, so they are not suitable for use as a password.
91. B. Qualitative tools are often used in business impact assessment to capture the impact on intangible factors such as customer confidence, employee morale, and reputation.
92. A. An organization pursuing a vital records management program should begin by identifying all of the documentation that qualifies as a vital business record. This should include all of the records necessary to restart the business in a new location should the organization invoke its business continuity plan.
93. B. Security training is designed to provide employees with the specific knowledge they need to fulfill their job functions. It is usually designed for individuals with similar job functions.
94. D. Awareness establishes a minimum standard of information security understanding. It is designed to accommodate all personnel in an organization, regardless of their assigned tasks.
95. C. Risks are the combination of a threat and a vulnerability. Threats are the external forces seeking to undermine security, such as the malicious hacker in this case. Vulnerabilities are the internal weaknesses that might allow a threat to succeed. In this case, the missing patch is the vulnerability. In this scenario, if the malicious hacker (threat) attempts a SQL injection attack against the unpatched server (vulnerability), the result is website defacement.
96. C. The exposure factor is the percentage of the facility that risk managers expect will be damaged if a risk materializes. It is calculated by dividing the amount of damage by the asset value. In this case, that is $5 million in damage divided by the $10 million facility value, or 50%.
97. B. The annualized rate of occurrence is the number of times that risk analysts expect a risk to happen in any given year. In this case, the analysts expect tornados once every 200 years, or 0.005 times per year.
98. A. The annualized loss expectancy is calculated by multiplying the single loss expectancy (SLE) by the annualized rate of occurrence (ARO). In this case, the SLE is $5,000,000, and the ARO is 0.005. Multiplying these numbers together gives you the ALE of $25,000.
99. C. Information disclosure attacks rely upon the revelation of private, confidential, or controlled information. Programming comments embedded in HTML code are an example of this type of attack.
100. B. Nondisclosure agreements (NDAs) protect the confidentiality of sensitive information by requiring that employees and affiliates not share confidential information with third parties. NDAs normally remain in force after an employee leaves the company.
101. A. Supply chain management can help ensure the security of hardware, software, and services that an organization acquires. Chris should focus on each step that his laptops take from the original equipment manufacturer to delivery.
102. C. STRIDE, Process for Attack Simulation and Threat Analysis (PASTA), and Visual, Agile, and Simple Threat (VAST) modeling are all threat modeling methodologies. STRIDE was designed for applications and operating systems (but can be used more broadly), PASTA is a risk-centric modeling system, and VAST is a threat modeling concept based on Agile project management and programming techniques.
103. C. Change management is a critical control process that involves systematically managing change. Without it, Lisa might simply deploy her code to production without oversight, documentation, or testing. Regression testing focuses on testing to ensure that new code doesn't bring back old flaws, while fuzz testing feeds unexpected input to code. Code review reviews the source code itself and may be involved in the change management process but isn't what is described here.
104. A. Charles is tracking a key performance indicator (KPI). A KPI is used to measure performance (and success). Without a definition of success, this would simply be a metric, but

Charles is working toward a known goal and can measure against it. There is not a return investment calculation in this problem, and the measure is not a control.

105. D. A fitness evaluation is not a typical part of a hiring process. Drug tests, background checks, and social media checks are all common parts of current hiring practices.
106. B. The $(ISC)^2$ code of ethics also includes "Act honorably, honestly, justly, responsibly, and legally" but does not specifically require credential holders to disclose all breaches of privacy, trust, or ethics.
107. B. In general, companies should be aware of the breach laws in any location where they do business. US states have a diverse collection of breach laws and requirements, meaning that in this case, Greg's company may need to review many different breach laws to determine which they may need to comply with if they conduct business in the state or with the state's residents.
108. A. When organizations merge, it is important to understand the state of the security for both organizations. Running vulnerability scans and performing a risk assessment are both common steps taken when preparing to merge two (or more!) IT environments.
109. D. Signing a noncompete or nondisclosure agreement is typically done at hiring. Exit interviews, recovery of organizational property, and account termination are all common elements of a termination process.
110. C. A security controls assessment (SCA) most often refers to a formal US government process for assessing security controls and is often paired with a Security Test and Evaluation (ST&E) process. This means that Laura is probably part of a government organization or contractor.
111. B. Purchasing insurance is a means of transferring risk. If Sally had worked to decrease the likelihood of the events occurring, she would have been using a reduce or risk mitigation strategy, while simply continuing to function as the organization has would be an example of an acceptance strategy. Rejection, or denial of the risk, is not a valid strategy, even though it occurs!

Chapter 2: Asset Security (Domain 2)

1. C. Encryption is often used to protect traffic like bank transactions from sniffing. While packet injection and man-in-the-middle attacks are possible, they are far less likely to occur, and if a VPN were used, it would be used to provide encryption. TEMPEST is a specification for techniques used to prevent spying using electromagnetic emissions and wouldn't be used to stop attacks at any normal bank.
2. A. Business owners have to balance the need to provide value with regulatory, security, and other requirements. This makes the adoption of a common framework like COBIT attractive. Data owners are more likely to ask that those responsible for control selection identify a standard to use. Data processors are required to perform specific actions under regulations like the EU GDPR. Finally, in many organizations, data stewards are internal roles that oversee how data is used.
3. B. A baseline is used to ensure a minimum security standard. A policy is the foundation that a standard may point to for authority, and a configuration guide may be built from a baseline to help staff who need to implement it to accomplish their task. An outline is helpful, but *outline* isn't the term you're looking for here.
4. B. Media is typically labeled with the highest classification level of data it contains. This prevents the data from being handled or accessed at a lower classification level. Data integrity

requirements may be part of a classification process but don't independently drive labeling in a classification scheme.

5. A. The need to protect sensitive data drives information classification. This allows organizations to focus on data that needs to be protected rather than spending effort on less important data. Remanence describes data left on media after an attempt is made to remove the data. Transmitting data isn't a driver for an administrative process to protect sensitive data, and clearing is a technical process for removing data from media.
6. A. A data retention policy can help to ensure that outdated data is purged, removing potential additional costs for discovery. Many organizations have aggressive retention policies to both reduce the cost of storage and limit the amount of data that is kept on hand and discoverable. Data retention policies are not designed to destroy incriminating data, and legal requirements for data retention must still be met.
7. D. Custodians are delegated the role of handling day-to-day tasks by managing and overseeing how data is handled, stored, and protected. Data processors are systems used to process data. Business owners are typically project or system owners who are tasked with making sure systems provide value to their users or customers.
8. D. Privacy Shield compliance helps US companies meet the EU General Data Protection Regulation. Yearly assessments may be useful, but they aren't required. HIPAA is a US law that applies specifically to healthcare and related organizations, and encrypting all data all the time is impossible (at least if you want to use the data!). PCI DSS is a global contractual regulation for the handling of credit card information.
9. C. Security baselines provide a starting point to scope and tailor security controls to your organization's needs. They aren't always appropriate to specific organizational needs, they cannot ensure that systems are always in a secure state, and they do not prevent liability.
10. A. Clearing describes preparing media for reuse. When media is cleared, unclassified data is written over all addressable locations on the media. Once that's completed, the media can be reused. Erasing is the deletion of files or media. Purging is a more intensive form of clearing for reuse in lower-security areas, and sanitization is a series of processes that removes data from a system or media while ensuring that the data is unrecoverable by any means.
11. C. The US government uses the label Confidential for data that could cause damage if it was disclosed without authorization. Exposure of Top Secret data is considered to potentially cause grave damage, while Secret data could cause serious damage. Classified is not a level in the US government classification scheme.
12. D. Spare sectors, bad sectors, and space provided for wear leveling on SSDs (overprovisioned space) may all contain data that was written to the space that will not be cleared when the drive is wiped. Most wiping utilities only deal with currently addressable space on the drive. SSDs cannot be degaussed, and wear leveling space cannot be reliably used to hide data. These spaces are still addressable by the drive, although they may not be seen by the operating system.
13. B. Data remanence is a term used to describe data left after attempts to erase or remove data. Slack space describes unused space in a disk cluster, zero fill is a wiping methodology that replaces all data bits with zeroes, and *residual bytes* is a made-up term.
14. C. Information shared with customers is public, internal business could be sensitive or private, and trade secrets are proprietary. Thus, public, sensitive, proprietary matches this most closely. Confidential is a military classification, which removes two of the remaining options, and trade secrets are more damaging to lose than a private classification would allow.
15. C. A watermark is used to digitally label data and can be used to indicate ownership. Encryption would have prevented the data from being accessed if it was lost, while classification is part of

the set of security practices that can help make sure the right controls are in place. Finally, metadata is used to label data and might help a data loss prevention system flag it before it leaves your organization.

16. B. AES is a strong modern symmetric encryption algorithm that is appropriate for encrypting data at rest. TLS is frequently used to secure data when it is in transit. A virtual private network is not necessarily an encrypted connection and would be used for data in motion, while DES is an outdated algorithm and should not be used for data that needs strong security.
17. A. Data loss prevention (DLP) systems can use labels on data to determine the appropriate controls to apply to the data. DLP systems won't modify labels in real time and typically don't work directly with firewalls to stop traffic. Deleting unlabeled data would cause big problems for organizations that haven't labeled every piece of data!
18. B. The value of the data contained on media often exceeds the cost of the media, making more expensive media that may have a longer life span or additional capabilities like encryption support a good choice. While expensive media may be less likely to fail, the reason it makes sense is the value of the data, not just that it is less likely to fail. In general, the cost of the media doesn't have anything to do with the ease of encryption, and data integrity isn't ensured by better media.
19. C. Sanitization is a combination of processes that ensure that data from a system cannot be recovered by any means. Erasing and clearing are both prone to mistakes and technical problems that can result in remnant data and don't make sense for systems that handled proprietary information. Destruction is the most complete method of ensuring that data cannot be exposed, and some organizations opt to destroy the entire workstation, but that is not a typical solution due to the cost involved.
20. The US government's classification levels from least to most sensitive are:

- C. Unclassified
- B. Confidential
- A. Secret
- D. Top Secret

21. C. Data at rest is inactive data that is physically stored. Data in an IPsec tunnel or part of an e-commerce transaction is data in motion. Data in RAM is ephemeral and is not inactive.
22. C. PCI DSS, the Payment Card Industry Data Security Standard, provides the set of requirements for credit card processing systems. The Microsoft, NSA, and CIS baseline are all useful for building a Windows 10 security standard, but the PCI DSS standard is a better answer.
23. D. The CIS benchmarks are an example of a security baseline. A risk assessment would help identify which controls were needed, and proper system ownership is an important part of making sure baselines are implemented and maintained. Data labeling can help ensure that controls are applied to the right systems and data.
24. B. Scoping involves selecting only the controls that are appropriate for your IT systems, while tailoring matches your organization's mission and the controls from a selected baseline. Baselining is the process of configuring a system or software to match a baseline or building a baseline itself. *Selection* isn't a technical term used for any of these processes.
25. B. The controls implemented from a security baseline should match the data classification of the data used or stored on the system. Custodians are trusted to ensure the day-to-day security of the data and should do so by ensuring that the baseline is met and maintained. Business owners often have a conflict of interest between functionality and data security, and of course, applying

the same controls everywhere is expensive and may not meet business needs or be a responsible use of resources.

26. B. FTP and Telnet do not provide encryption for the data they transmit and should not be used if they can be avoided. SFTP and SSH provide encryption to protect both the data they send and the credentials that are used to log in via both utilities.
27. B. Many organizations require the destruction of media that contains data at higher levels of classification. Often the cost of the media is lower than the potential costs of data exposure, and it is difficult to guarantee that reused media doesn't contain remnant data. Tapes can be erased by degaussing, but degaussing is not always fully effective. Bitrot describes the slow loss of data on aging media, while *data permanence* is a term sometimes used to describe the life span of data and media.
28. A. NIST Special Publication 800-122 defines PII as any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and other information that is linked or linkable to an individual such as medical, educational, financial, and employment information. PHI is health-related information about a specific person, Social Security numbers are issued to individuals in the United States, and *SII* is a made-up term.
29. B. The biggest threat to data at rest is typically a data breach. Data at rest with a high level of sensitivity is often encrypted to help prevent this. Decryption is not as significant of a threat if strong encryption is used and encryption keys are well secured. Data integrity issues could occur, but proper backups can help prevent this, and of course data could be improperly classified, but this is not the primary threat to the data.
30. B. Full disk encryption only protects data at rest. Since it encrypts the full disk, it does not distinguish between labeled and unlabeled data.
31. B. One way to use an IPsec VPN is to create a private, encrypted network (or tunnel) via a public network, allowing users to be a virtual part of their employer's internal network. IPsec is distinct from TLS and provides encryption for confidentiality and integrity, and of course, in this scenario Sue is connecting to her employer's network rather than the employer connecting to hers.
32. D. Classification identifies the value of data to an organization. This can often help drive IT expenditure prioritization and could help with rough cost estimates if a breach occurred, but that's not the primary purpose. Finally, most breach laws call out specific data types for notification rather than requiring organizations to classify data themselves.
33. B. Downgrading systems and media is rare due to the difficulty of ensuring that sanitization is complete. The need to completely wipe (or destroy) the media that systems use means that the cost of reuse is often significant and may exceed the cost of purchasing a new system or media. The goal of purging is to ensure that no data remains, so commingling data should not be a concern, nor should the exposure of the data; only staff with the proper clearance should handle the systems! Finally, a DLP system should flag data based on labels, not on the system it comes from.
34. A. Classification should be conducted based on the value of the data to the organization, its sensitivity, and the amount of harm that could result from exposure of the data. Cost should be considered when implementing controls and is weighed against the damage that exposure would create.
35. C. Erasing, which describes a typical deletion process in many operating systems, typically removes only the link to the file and leaves the data that makes up the file itself. The data will remain in place but not indexed until the space is needed and it is overwritten. Degaussing works only on magnetic media, but it can be quite effective on it. Purging and clearing both describe more elaborate removal processes.

36. The data elements match with the categories as follows:

- **Data elements**

-
    1. Medical records: B. PHI.
    2. Credit card numbers: A. PCI DSS.
    3. Social Security numbers: C. PII.
    4. Driver's license numbers: C. PII.

- Medical records are an example of protected health information (PHI). Credit card numbers are personally identifiable information (PII), but they are also covered by the Payment Card Industry Data Security Standard (PCI DSS), which is a more specific category governing only credit card information and is a better answer. Social Security numbers and driver's license numbers are examples of PII.

37. C. TLS is a modern encryption method used to encrypt and protect data in transit. BitLocker is a full disk encryption technology used for data at rest. DES and SSL are both outdated encryption methods and should not be used for data that requires high levels of security.
38. C. We know that the data classification will not be the top level classification of "Confidential" because the loss of the data would not cause severe damage. This means we have to choose between private (PHI) and sensitive (confidential). Calling this private due to the patient's personal health information fits the classification scheme, giving us the correct answer.
39. A. A data loss prevention (DLP) system or software is designed to identify labeled data or data that fits specific patterns and descriptions to help prevent it from leaving the organization. An IDS is designed to identify intrusions. Although some IDS systems can detect specific types of sensitive data using pattern matching, they have no ability to stop traffic. A firewall uses rules to control traffic routing, while UDP is a network protocol.
40. A. When data is stored in a mixed classification environment, it is typically classified based on the highest classification of data included. In this case, the US government's highest classification is Top Secret. Mixed classification is not a valid classification in this scheme.
41. B. A nondisclosure agreement, or NDA, is a legal agreement that prevents employees from sharing proprietary data with their new employers. Purging is used on media, while classification is used on data. Encryption can help secure data, but it doesn't stop employees who can decrypt or copy the data from sharing it.
42. C. By default, BitLocker and Microsoft's Encrypting File System (EFS) both use AES (Advanced Encryption Standard), which is the NIST-approved replacement for DES (Data Encryption Standard). Serpent was a competitor of AES, and 3DES was created as a possible replacement for DES.
43. B. Group Policy provides the ability to monitor and apply settings in a security baseline. Manual checks by users and using startup scripts provide fewer reviews and may be prone to failure, while periodic review of the baseline won't result in compliance being checked.
44. B. A baseline is a set of security configurations that can be adopted and modified to fit an organization's security needs. A security policy is written to describe an organization's approach to security, while DSS is the second half of the Payment Card Industry Data Security Standard. The NIST SP-800 series of documents address computer security in a variety of areas.
45. C. Record retention policies describe how long an organization should retain data and may also specify how and when destruction should occur. Classification policies describe how and why

classification should occur and who is responsible, while availability and audit policies may be created for specific purposes.

46. A. The POODLE (or Padding Oracle On Downgraded Legacy Encryption) attack helped force the move from SSL 3.0 to TLS because it allowed attackers to easily access SSL encrypted messages. Stuxnet was a worm aimed at the Iranian nuclear program, while CRIME and BEAST were earlier attacks against SSL.
47. D. Using strong encryption, like AES-256, can help ensure that loss of removable media like tapes doesn't result in a data breach. Security labels may help with handling processes, but they won't help once the media is stolen or lost. Having multiple copies will ensure that you can still access the data but won't increase the security of the media. Finally, using hard drives instead of tape only changes the media type and not the risk from theft or loss.
48. D. Electronic signatures, as used in this rule, prove that the signature was provided by the intended signer. Electronic signatures as part of the FDA code are intended to ensure that electronic records are "trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper." Signatures cannot provide confidentiality or integrity and don't ensure that someone has reviewed the data.
49. D. Secure Shell (SSH) is an encrypted protocol for remote login and command-line access. SCP and SFTP are both secure file transfer protocols, while WDS is the acronym for Windows Deployment Services, which provides remote installation capabilities for Windows operating systems.
50. B. Degaussing uses strong magnetic fields to erase magnetic media. *Magwipe* is a made-up term. Sanitization is a combination of processes used to remove data from a system or media to ensure that it cannot be recovered. Purging is a form of clearing used on media that will be reused in a lower classification or lower-security environment.
51. B. Nondisclosure agreements (NDAs) are used to enforce confidentiality agreements with employees and may remain in effect even after an employee leaves the organization. Other controls, such as sanitization, clearing, and encryption, would not be effective against information in an employee's memory.
52. C. Data labels are crucial to identify the classification level of information contained on the media. Digital rights management (DRM) tools provide ways to control how data is used, while encrypting it can help maintain the confidentiality and integrity of the data. Classifying the data is necessary to label it, but it doesn't automatically place a label on the data.
53. D. The NIST SP 800-88 process for sanitization and disposition shows that media that will be reused and was classified at a moderate level should be purged and then that purge should be validated. Finally, it should be documented.
54. D. Data in transit is data that is traversing a network or is otherwise in motion. TLS, VPNs, and IPsec tunnels are all techniques used to protect data in transit. AES, Serpent, and IDEA are all symmetric algorithms, while Telnet, ISDN, and UDP are all protocols. BitLocker and FileVault are both used to encrypt data, but they protect only stored data, not data in transit.
55. C. The data owner has ultimate responsibility for data belonging to an organization and is typically the CEO, president, or another senior employee. Business and mission owners typically own processes or programs. System owners own a system that processes sensitive data.
56. D. The US Department of Commerce oversees Privacy Shield. Only US organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or US air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DOT) are permitted to participate in Safe Harbor.
57. A. Chris is most likely to be responsible for classifying the data that he owns as well as assisting with or advising the system owners on security requirements and control selection. In an

organization with multiple data owners, Chris is unlikely to set criteria for classifying data on his own. As a data owner, Chris will also not typically have direct responsibility for scoping, tailoring, applying, or enforcing those controls.

58. B. The system administrators are acting in the roles of data administrators who grant access and will also act as custodians who are tasked with the day-to-day application of security controls. They are not acting as data owners who own the data itself. Typically, system administrators are delegated authority by system owners, such as a department head, and of course they are tasked with providing access to users.
59. C. Third-party organizations that process personal data on behalf of a data controller are known as data processors. The organization that they are contracting with would act in the role of the business or mission owners, and others within Chris's organization would have the role of data administrators, granting access as needed to the data based on their operational procedures and data classification.
60. B. The GDPR does include requirements that data be processed fairly, maintained securely, and maintained accurately. It does not include a requirement that information be deleted within one year, although it does specify that information should not be kept longer than necessary.
61. D. Under EU regulations, both the organization sharing data and the third-party data processor bear responsibility for maintaining the privacy and security of personal information.
62. D. The U.S. government specifies Secret as the classification level for information that, if disclosed, could cause serious harm to national security. Top Secret is reserved for information that could cause exceptionally grave harm, while confidential data could be expected to cause less harm. Unclassified is not an actual classification but only indicates that the data may be released to unclassified individuals. Organizations may still restrict access to unclassified information.
63. A. Sanitization is the combination of processes used to remove data from a system or media. When a PC is disposed of, sanitization includes the removal or destruction of drives, media, and any other storage devices it may have. Purging, destruction, and declassification are all other handling methods.
64. D. Bcrypt is based on Blowfish (the *b* is a key hint here). AES and 3DES are both replacements for DES, while Diffie-Hellman is a protocol for key exchange.
65. B. Requiring all media to have a label means that when unlabeled media is found, it should immediately be considered suspicious. This helps to prevent mistakes that might leave sensitive data unlabeled. Prelabeled media is not necessarily cheaper (nor may it make sense to buy!), while reusing public media simply means that it must be classified based on the data it now contains. HIPAA does not have specific media labeling requirements.
66. B. Data in use is data that is in a temporary storage location while an application or process is using it. Thus, data in memory is best described as data in use or ephemeral data. Data at rest is in storage, while data in transit is traveling over a network or other channel. *Data at large* is a made-up term.
67. C. Validation processes are conducted to ensure that the sanitization process was completed, avoiding data remanence. A form like this one helps to ensure that each device has been checked and that it was properly wiped, purged, or sanitized. This can allow reuse, does not prevent destruction, and does not help with attribution, which is a concept used with encryption to prove who created or sent a file.
68. C. Ensuring that data cannot be recovered is difficult, and the time and effort required to securely and completely wipe media as part of declassification can exceed the cost of new media. Sanitization, purging, and clearing may be part of declassification, but they are not

reasons that it is not frequently chosen as an option for organizations with data security concerns.

69. D. Destruction is the final stage in the lifecycle of media and can be done via disintegration, incineration, or a variety of other methods that result in the media and data being nonrecoverable. Sanitization is a combination of processes used when data is being removed from a system or media. Purging is an intense form of clearing, and degaussing uses strong magnetic fields to wipe data from magnetic media.
70. D. The GDPR does include the need to collect information for specified, explicit, and legitimate purposes; the need to ensure that collection is limited to the information necessary to achieve the stated purpose; and the need to protect data against accidental destruction. It does not include a specific requirement to encrypt information at rest.
71. D. Visual indicators like a distinctive screen background can help employees remember what level of classification they are dealing with and thus the handling requirements that they are expected to follow.
72. C. If an organization allows media to be downgraded, the purging process should be followed, and then the media should be relabeled. Degaussing may be used for magnetic media but won't handle all types of media. Pulverizing would destroy the media, preventing reuse, while relabeling first could lead to mistakes that result in media that hasn't been purged entering use.
73. B. The data owner sets the rules for use and protection of data. The remaining options all describe tasks for the system owner, including implementation of security controls.
74. B. In the NIST SP 800-60 diagram, the process determines appropriate categorization levels resulting in security categorization and then uses that as an input to determine controls. Standard selection would occur at an organizational level, while baselining occurs when systems are configured to meet a baseline. Sanitization would require the intentional removal of data from machines or media.
75. C. A and E can both be expected to have data at rest. C, the Internet, is an unknown, and the data can't be guaranteed to be at rest. B, D, and F are all data in transit across network links.
76. C. B, D, and F all show network links. Of the answers provided, Transport Layer Security (TLS) provides the best security for data in motion. AES-256 and 3DES are both symmetric ciphers and are more likely to be used for data at rest. SSL has been replaced with TLS and should not be a preferred solution.
77. B. Sending a file that is encrypted before it leaves means that exposure of the file in transit will not result in a confidentiality breach and the file will remain secure until decrypted at location E. Since answers A, C, and D do not provide any information about what happens at point C, they should be considered insecure, as the file may be at rest at point C in an unencrypted form.
78. C. Encrypting and labeling sensitive email will ensure that it remains confidential and can be identified. Performing these actions only on sensitive email will reduce the cost and effort of encrypting all email, allowing only sensitive email to be the focus of the organization's efforts. Only encrypting highly sensitive email not only skips labeling but might expose other classifications of email that shouldn't be exposed.
79. D. Scoping is performed when you match baseline controls to the IT system you're working to secure. Creation of standards is part of the configuration process and may involve the use of baselines. Baselining can mean the process of creating a security baseline or configuring systems to meet the baseline. CIS, the Center for Internet Security, provides a variety of security baselines.
80. C. Systems used to process data are data processors. Data owners are typically CEOs or other very senior staff, custodians are granted rights to perform day-to-day tasks when handling data, and mission owners are typically program or information system owners.

81. D. Personally identifiable information includes any information that can uniquely identify an individual. This would include name, Social Security number, and any other unique identifier (including a student ID number). ZIP code, by itself, does not uniquely identify an individual.
82. B. Protected health information, or PHI, includes a variety of data in multiple formats, including oral and recorded data, such as that created or received by healthcare providers, employers, and life insurance providers. PHI must be protected by HIPAA. PII is personally identifiable information. *SHI* and *HPHI* are both made-up acronyms.
83. C. AES is a strong symmetric cipher that is appropriate for use with data at rest. SHA1 is a cryptographic hash, while TLS is appropriate for data in motion. DES is an outdated and insecure symmetric encryption method.
84. D. The principle of data portability says that the data subject has the right to receive personal information and to transfer that information to another data controller. The principle of data integrity states that data should be reliable and that information should not be used for purposes other than those that users are made aware of by notice and that they have accepted through choice. Enforcement is aimed at ensuring that compliance with principles is assured. Onward transfer limits transfers to other organizations that comply with the principles of notice and choice.
85. C. Due to problems with remnant data, the US National Security Agency requires physical destruction of SSDs. This process, known as disintegration, results in very small fragments via a shredding process. Zero fill wipes a drive by replacing data with zeros, degaussing uses magnets to wipe magnetic media, and clearing is the process of preparing media for reuse.
86. A. The data owner bears responsibility for categorizing information systems and delegates selection of controls to system owners, while custodians implement the controls. Users don't perform any of these actions, while business owners are tasked with ensuring that systems are fulfilling their business purpose.
87. B. PCI DSS provides a set of required security controls and standards. Step 2 would be guided by the requirements of PCI DSS. PCI DSS will not greatly influence step 1 because all of the systems handle credit card information, making PCI DSS apply to all systems covered. Steps 3 and 4 will be conducted after PCI DSS has guided the decisions in step 2.
88. C. Custodians are tasked with the day-to-day monitoring of the integrity and security of data. Step 5 requires monitoring, which is a custodial task. A data owner may grant rights to custodians but will not be responsible for conducting monitoring. Data processors process data on behalf of the data controller, and a user simply uses the data via a computing system.
89. B. Susan's organization is limiting its risk by sending drives that have been sanitized before they are destroyed. This limits the possibility of a data breach if drives are mishandled by the third party, allowing them to be stolen, resold, or simply copied. The destruction of the drives will handle any issues with data remanence, while classification mistakes are not important if the drives have been destroyed. Data permanence and the life span of the data are not important on a destroyed drive.
90. C. A digital watermark is used to identify the owner of a file or to otherwise label it. A copyright notice provides information about the copyright asserted on the file, while data loss prevention (DLP) is a solution designed to prevent data loss. Steganography is the science of hiding information, often in images or files.
91. D. Record retention is the process of retaining and maintaining information for as long as it is needed. A data storage policy describes how and why data is stored, while data storage is the process of actually keeping the data. Asset maintenance is a non-information-security-related process for maintaining physical assets.

92. C. The cost of the data is not directly included in the classification process. Instead, the impact to the organization if the data were exposed or breached is considered. Who can access the data and what regulatory or compliance requirements cover the data are also important considerations.
93. B. Symmetric encryption like AES is typically used for data at rest. Asymmetric encryption is often used during transactions or communications when the ability to have public and private keys is necessary. DES is an outdated encryption standard, and OTP is the acronym for *onetime password*.
94. D. Administrators have the rights to assign permissions to access and handle data. Custodians are trusted with day-to-day data handling tasks. Business owners are typically system or project owners, and data processors are systems used to process data.
95. B. The California Online Privacy Protection Act (COPPA) requires that operators of commercial websites and services post a prominently displayed privacy policy if they collect personal information on California residents.

    The Personal Information Protection and Electronic Documents Act is a Canadian privacy law, while California Civil Code 1798.82 is part of the set of California codes that requires breach notification. The California Online Web Privacy Act does not exist.

96. A. Tapes are frequently exposed due to theft or loss in transit. That means that tapes that are leaving their normal storage facility should be handled according to the organization's classification schemes and handling requirements. Purging the tapes would cause the loss of data, while increasing the classification level of the tapes. The tapes should be encrypted rather than decrypted.
97. A. The correct answer is the tape that is being shipped to a storage facility. You might think that the tape in shipment is "in motion," but the key concept is that the data is not being accessed and is instead in storage. Data in a TCP packet, in an e-commerce transaction, or in local RAM is in motion and is actively being used.
98. D. When the value of data changes due to legal, compliance, or business reasons, reviewing classifications and reclassifying the data is an appropriate response. Once the review is complete, data can be reclassified and handled according to its classification level. Simply relabeling the data avoids the classification process and may not result in the data being handled appropriately. Similarly, selecting a new baseline or simply encrypting the data may not handle all of the needs that the changes affecting the data create.
99. C. PGP, or Pretty Good Privacy (or its open-source alternative, GPG) provide strong encryption of files, which can then be sent via email. Email traverses multiple servers and will be unencrypted at rest at multiple points along its path as it is stored and forwarded to its destination.
100. A. While many nongovernment organizations create their own classification schemes, a common model with levels that align with the US government's classification labels is shown here. In the given options, B and D do not match the US government's Top Secret, Secret, Confidential scheme, and C incorrectly matches business proprietary data with confidential data as well as Top Secret data with business sensitive data. *Business internal* is often another term

for *business sensitive*, meaning that it is used to match two classifications!

US Government Classification	DAMAGE DESCRIPTION	CIVILIAN CLASSIFICATION
Top Secret	Exceptionally grave damage	Confidential/Proprietary
Secret	Serious damage	Private
Confidential	Damage	Sensitive

Chapter 3: Security Architecture and Engineering (Domain 3)

1. D. The Brewer-Nash model allows access controls to change dynamically based upon a user's actions. It is often used in environments like Matthew's to implement a "Chinese wall" between data belonging to different clients.
2. A. Fires may be detected as early as the incipient stage. During this stage, air ionization takes place, and specialized incipient fire detection systems can identify these changes to provide early warning of a fire.
3. A. Closed-circuit television (CCTV) systems act as a secondary verification mechanism for physical presence because they allow security officials to view the interior of the facility when a motion alarm sounds to determine the current occupants and their activities.
4. B. In an *m of n* control system, at least *m of n* possible escrow agents must collaborate to retrieve an encryption key from the escrow database.
5. A. This is an example of a vendor offering a fully functional application as a web-based service. Therefore, it fits under the definition of software as a service (SaaS). In infrastructure as a service (IaaS), compute as a service (CaaS), and platform as a service (PaaS) approaches, the customer provides their own software. In this example, the vendor is providing the email software, so none of those choices is appropriate.
6. B. The Digital Signature Standard approves three encryption algorithms for use in digital signatures: the Digital Signature Algorithm (DSA); the Rivest, Shamir, Adleman (RSA) algorithm; and the Elliptic Curve DSA (ECDSA) algorithm. HAVAL is a hash function, not an encryption algorithm. While hash functions are used as part of the digital signature process, they do not provide encryption.
7. A. In the subject/object model of access control, the user or process making the request for a resource is the subject of that request. In this example, Harry is requesting resource access and is, therefore, the subject.
8. C. Michael should conduct his investigation, but there is a pressing business need to bring the website back online. The most reasonable course of action would be to take a snapshot of the compromised system and use the snapshot for the investigation, restoring the website to operation as quickly as possible while using the results of the investigation to improve the security of the site.
9. C. The use of a sandbox is an example of confinement, where the system restricts the access of a particular process to limit its ability to affect other processes running on the same system.
10. D. Assurance is the degree of confidence that an organization has that its security controls are correctly implemented. It must be continually monitored and reverified.
11. A. Maintenance hooks, otherwise known as backdoors, provide developers with easy access to a system, bypassing normal security controls. If not removed prior to finalizing code, they pose a significant security vulnerability if an attacker discovers the maintenance hook.
12. B. The Simple Integrity Property states that an individual may not read a file classified at a lower security level than the individual's security clearance.

13. B. Supervisory control and data acquisition (SCADA) systems are used to control and gather data from industrial processes. They are commonly found in power plants and other industrial environments.
14. B. The Trusted Platform Module (TPM) is a hardware security technique that stores an encryption key on a chip on the motherboard and prevents someone from accessing an encrypted drive by installing it in another computer.
15. D. Intentional collisions have been created with MD5, and a real-world collision attack against SHA 1 was announced in early 2017. 3DES is not a hashing tool, leaving SHA 256 (sometimes called SHA 2) as the only real choice that Chris has in this list.
16. C. In an asymmetric cryptosystem, the sender of a message always encrypts the message using the recipient's public key.
17. D. When Bob receives the message, he uses his own private key to decrypt it. Since he is the only one with his private key, he is the only one who should be able to decrypt it, thus preserving confidentiality.
18. B. Each user retains their private key as secret information. In this scenario, Bob would only have access to his own private key and would not have access to the private key of Alice or any other user.
19. B. Alice creates the digital signature using her own private key. Then Bob, or any other user, can verify the digital signature using Alice's public key.
20. B. The salt is a random value added to a password before it is hashed by the operating system. The salt is then stored in a password file with the hashed password. This increases the complexity of cryptanalytic attacks by negating the usefulness of attacks that use precomputed hash values, such as rainbow tables.
21. A. Hash functions do not include any element of secrecy and, therefore, do not require a cryptographic key.
22. D. A preaction fire suppression system activates in two steps. The pipes fill with water once the early signs of a fire are detected. The system does not dispense water until heat sensors on the sprinkler heads trigger the second phase.
23. B. The Encapsulating Security Payload (ESP) protocol provides confidentiality and integrity for packet contents. It encrypts packet payloads and provides limited authentication and protection against replay attacks.
24. D. The greatest risk when a device is lost or stolen is that sensitive data contained on the device will fall into the wrong hands. Confidentiality protects against this risk.
25. C. The exclusive or (XOR) operation is true when one and only one of the input values is true.
26. A. DES uses a 64-bit encryption key, but only 56 of those bits are actually used as keying material in the encryption operation. The remaining 8 bits are used to detect tampering or corruption of the key.
27. C. The *-Security Property states that an individual may not write to a file at a lower classification level than that of the individual. This is also known as the confinement property.
28. B. The Diffie-Hellman algorithm allows for the secure exchange of symmetric encryption keys over a public network.
29. C. Protection Profiles (PPs) specify the security requirements and protections that must be in place for a product to be accepted under the Common Criteria.
30. A. Hash functions must be able to work on any variable-length input and produce a fixed-length output from that input, regardless of the length of the input.
31. C. Binary keyspaces contain a number of keys equal to two raised to the power of the number of bits. Two to the fifth power is 32, so a 5-bit keyspace contains 32 possible keys.

32. B. Kerckhoff's principle says that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
33. A. Mantraps use a double set of doors to prevent piggybacking by allowing only a single individual to enter a facility at a time.
34. A. While it would be ideal to have wiring closets in a location where they are monitored by security staff, this is not feasible in most environments. Wiring closets must be distributed geographically in multiple locations across each building used by an organization.
35. D. The *-Integrity Property states that a subject cannot modify an object at a higher integrity level than that possessed by the subject.
36. The architecture security concepts match with the descriptions as follows:
    1. Time of check: C. The time at which the subject checks whether an object is available.
    2. Covert channel: A. A method used to pass information over a path not normally used for communication.
    3. Time of use: D. The time at which a subject can access an object.
    4. Maintenance hooks: E. An access method known only to the developer of the system.
    5. Parameter checking: F. A method that can help prevent buffer overflow attacks.
    6. Race condition: B. The exploitation of difference between time of check and time of use.
37. B. In the Fair Cryptosystem approach to key escrow, the secret keys used in communications are divided into two or more pieces, each of which is given to an independent third party.
38. A. The Ready state is used when a process is prepared to execute but the CPU is not available. The Running state is used when a process is executing on the CPU. The Waiting state is used when a process is blocked waiting for an external event. The Stopped state is used when a process terminates.
39. A. EAL1 assurance applies when the system in question has been functionally tested. It is the lowest level of assurance under the Common Criteria.
40. A. Administrators and processes may attach security labels to objects that provide information on an object's attributes. Labels are commonly used to apply classifications in a mandatory access control system.
41. B. Open-source software exposes the source code to public inspection and modification. The open-source community includes major software packages such as the Linux operating system.
42. A. Adam created a list of individual users that may access the file. This is an access control list, which consists of multiple access control entries. It includes the names of users, so it is not role-based, and Adam was able to modify the list, so it is not mandatory access control.
43. C. Parameter checking, or input validation, is used to ensure that input provided by users to an application matches the expected parameters for the application. Developers may use parameter checking to ensure that input does not exceed the expected length, preventing a buffer overflow attack.
44. A. *Kernel mode*, *supervisory mode*, and *system mode* are all terms used to describe privileged modes of system operation. User mode is an unprivileged mode.
45. D. Multistate systems are certified to handle data from different security classifications simultaneously by implementing protection mechanisms that segregate data appropriately.
46. C. For systems running in System High mode, the user must have a valid security clearance for all information processed by the system, access approval for all information processed by the system, and a valid need to know for some, but not necessarily all, information processed by the system.
47. B. Steganography is the art of using cryptographic techniques to embed secret messages within other content. Some steganographic algorithms work by making alterations to the least significant bits of the many bits that make up image files.

48. C. The Caesar cipher is a shift cipher that works on a stream of text and is also a substitution cipher. It is not a block cipher or a transposition cipher. It is extremely weak as a cryptographic algorithm.
49. A. The kernel lies within the central ring, Ring 0. Conceptually, Ring 1 contains other operating system components. Ring 2 is used for drivers and protocols. User-level programs and applications run at Ring 3. Rings 0 through 2 run in privileged mode while Ring 3 runs in user mode. It is important to note that many modern operating systems do not fully implement this model.
50. D. In an infrastructure as a service environment, security duties follow a shared responsibility model. Since the vendor is responsible for managing the storage hardware, the vendor would retain responsibility for destroying or wiping drives as they are taken out of service. However, it is still the customer's responsibility to validate that the vendor's sanitization procedures meet their requirements prior to utilizing the vendor's storage services.
51. B. The major difference between a code and a cipher is that ciphers alter messages at the character or bit level, not at the word level. DES, shift ciphers, and word scrambles all work at the character or bit level and are ciphers. "One if by land; two if by sea" is a message with hidden meaning in the words and is an example of a code.
52. C. The verification process is similar to the certification process in that it validates security controls. Verification may go a step further by involving a third-party testing service and compiling results that may be trusted by many different organizations. Accreditation is the act of management formally accepting an evaluating system, not evaluating the system itself.
53. B. When a process is confined within certain access bounds, that process runs in isolation. Isolation protects the operating environment, the operating system kernel, and other processes running on the system.
54. B. The mean time to failure (MTTF) provides the average amount of time before a device of that particular specification fails.
55. A. Class A fire extinguishers are useful only against common combustible materials. They use water or soda acid as their suppressant. Class B extinguishers are for liquid fires. Class C extinguishers are for electrical fires, and Class D fire extinguishers are for combustible metals.
56. A. Mobile Device Management (MDM) products provide a consistent, centralized interface for applying security configuration settings to mobile devices.
57. C. Nonrepudiation occurs when the recipient of a message is able to demonstrate to a third party that the message came from the purported sender.
58. A. The card shown in the image has a smart chip underneath the American flag. Therefore, it is an example of a smart card. This is the most secure type of identification card technology.
59. D. The TEMPEST program creates technology that is not susceptible to Van Eck phreaking attacks because it reduces or suppresses natural electromagnetic emanations.
60. B. The Trusted Computing Base (TCB) is a small subset of the system contained within the kernel that carries out critical system activities.
61. A. The MD5 hash algorithm has known collisions and, as of 2005, is no longer considered secure for use in modern environments.
62. B. Encrypting data on SSD drives does protect against wear leveling. Disk formatting does not effectively remove data from any device. Degaussing is only effective for magnetic media. Physically destroying the drive would not permit reuse.
63. C. In a known plaintext attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate that ciphertext.

64. B. In a time of check to time of use (TOCTOU) attack, the attacker exploits the difference in time between when a security control is verified and the data protected by the control is actually used.
65. A. The X.509 standard, developed by the International Telecommunications Union, contains the specification for digital certificates.
66. D. Fences designed to deter more than the casual intruder should be at least 6 feet high. If a physical security system is designed to deter even determined intruders, it should be at least 8 feet high and topped with three strands of barbed wire.
67. C. In an aggregation attack, individual(s) use their access to specific pieces of information to piece together a larger picture that they are not authorized to access.
68. D. While all of the controls mentioned protect against unwanted electromagnetic emanations, only white noise is an active control. White noise generates false emanations that effectively "jam" the true emanations from electronic equipment.
69. B. In a software as a service environment, the customer has no access to any underlying infrastructure, so firewall management is a vendor responsibility under the cloud computing shared responsibility model.
70. C. The grant rule allows a subject to grant rights that it possesses on an object to another subject.
71. B. The system Charles is remediating may have a firmware or BIOS infection, with malware resident on the system board. While uncommon, this type of malware can be difficult to find and remove. Since he used original media, it is unlikely that the malware came from the software vendor. Charles wiped the system partition, and the system would have been rebooted before being rebuilt, thus clearing system memory.
72. D. Multithreading permits multiple tasks to execute concurrently within a single process. These tasks are known as threads and may be alternated between without switching processes.
73. C. This message was most likely encrypted with a transposition cipher. The use of a substitution cipher, a category that includes AES and 3DES, would change the frequency distribution so that it did not mirror that of the English language.
74. D. The meet-in-the-middle attack uses a known plaintext message and uses both encryption of the plaintext and decryption of the ciphertext simultaneously in a brute-force manner to identify the encryption key in approximately double the time of a brute-force attack against the basic DES algorithm.
75. A. The blacklisting approach to application control allows users to install any software they wish except for packages specifically identified by the administrator as prohibited. This would be an appropriate approach in a scenario where users should be able to install any nonmalicious software they wish to use.
76. A. Heartbeat sensors send periodic status messages from the alarm system to the monitoring center. The monitoring center triggers an alarm if it does not receive a status message for a prolonged period of time, indicating that communications were disrupted.
77. B. In a zero-knowledge proof, one individual demonstrates to another that they can achieve a result that requires sensitive information without actually disclosing the sensitive information.
78. A. Blowfish allows the user to select any key length between 32 and 448 bits.
79. B. Soda acid and other dry powder extinguishers work to remove the fuel supply. Water suppresses temperature, while halon and carbon dioxide remove the oxygen supply from a fire.
80. A. Digital signatures are possible only when using an asymmetric encryption algorithm. Of the algorithms listed, only RSA is asymmetric and supports digital signature capabilities.
81. C. The Open Web Application Security Project (OWASP) produces an annual list of the top ten web application security issues that developers and security professionals around the world rely

upon for education and training purposes. The OWASP vulnerabilities form the basis for many web application security testing products.

82. A. The information flow model applies state machines to the flow of information. The Bell-LaPadula model applies the information flow model to confidentiality while the Biba model applies it to integrity.
83. D. Each process that runs on a system is assigned certain physical or logical bounds for resource access, such as memory.
84. C. Capacitance motion detectors monitor the electromagnetic field in a monitored area, sensing disturbances that correspond to motion.
85. D. Halon fire suppression systems use a chlorofluorocarbon (CFC) suppressant material that was banned in the Montreal Protocol because it depletes the ozone layer.
86. D. The Biba model focuses only on protecting integrity and does not provide protection against confidentiality or availability threats. It also does not provide protection against covert channel attacks. The Biba model focuses on external threats and assumes that internal threats are addressed programmatically.
87. A. In TLS, both the server and the client first communicate using an ephemeral symmetric session key. They exchange this key using asymmetric cryptography, but all encrypted content is protected using symmetric cryptography.
88. B. A Faraday cage is a metal skin that prevents electromagnetic emanations from exiting. It is a rarely used technology because it is unwieldy and expensive, but it is quite effective at blocking unwanted radiation.
89. B. The hypervisor is responsible for coordinating access to physical hardware and enforcing isolation between different virtual machines running on the same physical platform.
90. B. Cloud computing systems where the customer only provides application code for execution on a vendor-supplied computing platform are examples of platform as a service (PaaS) computing.
91. B. The feedback model of composition theory occurs when one system provides input for a second system and then the second system provides input for the first system. This is a specialized case of the cascading model, so the feedback model is the most appropriate answer.
92. B. UPSs are designed to protect against short-term power losses, such as power faults. When they conduct power conditioning, they are also able to protect against sags and noise. UPSs have limited-life batteries and are not able to maintain continuous operating during a sustained blackout.
93. D. Data center humidity should be maintained between 40% and 60%. Values below this range increase the risk of static electricity, while values above this range may generate moisture that damages equipment.
94. C. Asymmetric cryptosystems use a pair of keys for each user. In this case, with 1,000 users, the system will require 2,000 keys.
95. B. Accreditation is the formal approval by a DAA that an IT system may operate in a described risk environment.
96. B. Abstraction uses a black box approach to hide the implementation details of an object from the users of that object.
97. A. The certificate revocation list contains the serial numbers of digital certificates issued by a certificate authority that have later been revoked.
98. A. The point of the digital certificate is to prove to Alison that the server belongs to the bank, so she does not need to have this trust in advance. To trust the certificate, she must verify the CA's digital signature on the certificate, trust the CA, verify that the certificate is not listed on a CRL, and verify that the certificate contains the name of the bank.

99. C. Covert channels use surreptitious communications' paths. Covert timing channels alter the use of a resource in a measurable fashion to exfiltrate information. If a user types using a specific rhythm of Morse code, this is an example of a covert timing channel. Someone watching or listening to the keystrokes could receive a secret message with no trace of the message left in logs.
100. C. Self-signed digital certificates should be used only for internal-facing applications, where the user base trusts the internally generated digital certificate.
101. D. Mirai targeted "Internet of Things" devices, including routers, cameras, and DVRs. As organizations bring an increasing number of devices like these into their corporate networks, protecting both internal and external targets from insecure, infrequently updated, and often vulnerable IoT devices is increasing important.
102. B. A well-designed data center should have redundant systems and capabilities for each critical part of its infrastructure. That means that power, cooling, and network connectivity should all be redundant. Kim should determine how to ensure that a single system failure cannot take her data center offline.
103. B. Matt is helping to maintain the chain of custody documentation for his electronic evidence. This can be important if his organization needs to prove that the digital evidence they handled has not been tampered with. A better process would involve more than one person to ensure that no tampering was possible.
104. C. Lauren has implemented address space layout randomization, a memory protection methodology that randomizes memory locations, which prevents attackers from using known address spaces and contiguous memory regions to execute code via overflow or stack smashing attacks.
105. C. The first thing Casey should do is notify her management, but after that, replacing the certificate and using proper key management practices with the new certificate's key should be at the top of her list.
106. A. Supervisory Control and Data Acquisition systems, or SCADA systems, provide a graphical interface to monitor industrial control systems (ICS). Joanna should ask about access to her organization's SCADA systems.
107. A. When operating system patches are no longer available for mobile devices, the best option is typically to retire or replace the device. Building isolated networks will not stop the device from being used for browsing or other purposes, which means it is likely to continue to be exposed to threats. Installing a firewall will not remediate the security flaws in the OS, although it may help somewhat. Finally, reinstalling the OS will not allow new updates or fix the root issue.
108. C. The most reasonable choice presented is to move the devices to a secure and isolated network segment. This will allow the devices to continue to serve their intended function while preventing them from being compromised. All of the other scenarios either create major new costs or deprive her organization of the functionality that the devices were purchased to provide.
109. D. Alex can use digital rights management technology to limit use of the PDFs to paying customers. While DRM is rarely a perfect solution, in this case, it may fit his organization's needs. EDM is electronic dance music, which his customers may appreciate but which won't solve the problem. Encryption and digital signatures can help to keep the files secure and to prove who they came from but won't solve the rights management issue Alex is tackling.
110. The security models match with the descriptions as follows:
    1. Clark-Wilson: C. This model uses security labels to grant access to objects via transformation procedures and a restricted interface model.

2. Graham-Denning: D. This model focuses on the secure creation and deletion of subjects and objects using eight primary protection rules or actions.
3. Bell-LaPadula: A. This model blocks lower-classified objects from accessing higher-classified objects, thus ensuring confidentiality.
4. Sutherland: E. This integrity model focuses on preventing interference in support of integrity.
5. Biba: B. The * property of this model can be summarized as “no write-up.”