Chapter 1

Security and Risk Management (Domain 1)
1. What is the final step of a quantitative risk analysis?
   A. Determine asset value.
   B. Assess the annualized rate of occurrence.
   C. Derive the annualized loss expectancy.
   D. Conduct a cost/benefit analysis.

2. An evil twin attack that broadcasts a legitimate SSID for an unauthorized network is an example of what category of threat?
   A. Spoofing
   B. Information disclosure
   C. Repudiation
   D. Tampering

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?
   A. Storage of information by a customer on a provider’s server
   B. Caching of information by the provider
   C. Transmission of information over the provider’s network by a customer
   D. Caching of information in a provider search engine

4. FlyAway Travel has offices in both the European Union and the United States and transfers personal information between those offices regularly. Which of the seven requirements for processing personal information states that organizations must inform individuals about how the information they collect is used?
   A. Notice
   B. Choice
   C. Onward Transfer
   D. Enforcement

5. Which one of the following is not one of the three common threat modeling techniques?
   A. Focused on assets
   B. Focused on attackers
   C. Focused on software
   D. Focused on social engineering

6. Which one of the following elements of information is not considered personally identifiable information that would trigger most US state data breach laws?
   A. Student identification number
   B. Social Security number
C. Driver's license number  
D. 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?  
A. Due diligence rule  
B. Personal liability rule  
C. Prudent man rule  
D. 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?  
A. Username  
B. PIN  
C. Security question  
D. Fingerprint scan  

9. What United States government agency is responsible for administering the terms of safe harbor agreements between the European Union and the United States under the EU Data Protection Directive?  
A. Department of Defense  
B. Department of the Treasury  
C. State Department  
D. 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?  
A. GLBA  
B. SOX  
C. HIPAA  
D. 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?  
A. FISMA  
B. PCI DSS  
C. HIPAA  
D. 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?
   A. Memory chips
   B. Office productivity applications
   C. Hard drives
   D. 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 model?
   A. Spoofing
   B. Repudiation
   C. Tampering
   D. 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?
   A. Implement new security controls to reduce the risk level.
   B. Design a disaster recovery plan.
   C. Repeat the business impact assessment.
   D. Document your decision-making process.

15. Which one of the following control categories does not accurately describe a fence around a facility?
   A. Physical
   B. Detective
   C. Deterrent
   D. 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?
   A. Quantitative risk assessment
   B. Qualitative risk assessment
   C. Neither quantitative nor qualitative risk assessment
   D. Combination of quantitative and qualitative risk assessment

17. What law provides intellectual property protection to the holders of trade secrets?
   A. Copyright Law
   B. Lanham Act
C. Glass-Steagall Act  
D. 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?  
A. Due diligence  
B. Separation of duties  
C. Due care  
D. Least privilege  

19. Darcy is designing a fault tolerant system and wants to implement RAID-5 for her system. What is the minimum number of physical hard disks she can use to build this system?  
A. One  
B. Two  
C. Three  
D. Five  

20. Which one of the following is an example of an administrative control?  
A. Intrusion detection system  
B. Security awareness training  
C. Firewalls  
D. 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?  
A. Patent  
B. Trade secret  
C. Copyright  
D. Trademark  

22. Which one of the following actions might be taken as part of a business continuity plan?  
A. Restoring from backup tapes  
B. Implementing RAID  
C. Relocating to a cold site  
D. Restarting business operations
23. When developing a business impact analysis, the team should first create a list of assets. What should happen next?
   A. Identify vulnerabilities in each asset.
   B. Determine the risks facing the asset.
   C. Develop a value for each asset.
   D. 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?
   A. Risk acceptance
   B. Risk avoidance
   C. Risk mitigation
   D. Risk transference

25. Which one of the following is an example of physical infrastructure hardening?
   A. Antivirus software
   B. Hardware-based network firewall
   C. Two-factor authentication
   D. Fire suppression system

26. Which one of the following is normally used as an authorization tool?
   A. ACL
   B. Token
   C. Username
   D. Password

27. The International Information Systems Security Certification Consortium uses the logo below 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?
   A. Copyright
   B. Patent
   C. Trade secret
   D. Trademark
28. Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?

![Image of a computer screen with a message about encrypted files]

A. Availability  
B. Confidentiality  
C. Disclosure  
D. Distributed

29. Which one of the following organizations would not be automatically subject to the terms of HIPAA if they engage in electronic transactions?

A. Healthcare provider  
B. Health and fitness application developer  
C. Health information clearinghouse  
D. Health insurance plan

30. John's network begins to experience symptoms of slowness. Upon investigation, he realizes that the network is being bombarded with ICMP ECHO REPLY packets and believes that his organization is the victim of a Smurf attack. What principle of information security is being violated?

A. Availability  
B. Integrity
C. Confidentiality
D. 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?
   A. Operational
   B. Tactical
   C. Summary
   D. Strategic

32. What government agency is responsible for the evaluation and registration of trademarks?
   A. USPTO
   B. Library of Congress
   C. TVA
   D. 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?
   A. Mandatory vacation
   B. Separation of duties
   C. Defense in depth
   D. Job rotation

34. Which one of the following categories of organizations is most likely to be covered by the provisions of FISMA?
   A. Banks
   B. Defense contractors
   C. School districts
   D. Hospitals

35. Robert is responsible for securing systems used to process credit card information. What standard should guide his actions?
   A. HIPAA
   B. PCI DSS
   C. SOX
   D. 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?
A. Data custodian  
B. Data owner  
C. User  
D. 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?  
A. Trade secret  
B. Copyright  
C. Trademark  
D. 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?  
A. United States Code  
B. Supreme Court rulings  
C. Code of Federal Regulations  
D. Compendium of Laws

39. Tom is installing a next-generation firewall (NGFW) in his data center that is designed to block many types of application attacks. When viewed from a risk management perspective, what metric is Tom attempting to lower?  
A. Impact  
B. RPO  
C. MTO  
D. Likelihood

40. Which one of the following individuals would be the most effective organizational owner for an information security program?  
A. CISSP-certified analyst  
B. Chief information officer  
C. Manager of network security  
D. President and CEO

41. What important function do senior managers normally fill on a business continuity planning team?  
A. Arbitrating disputes about criticality  
B. Evaluating the legal environment  
C. Training staff  
D. 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?
   A. SOC-1
   B. FISMA
   C. PCI DSS
   D. 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?
   A. Repudiation
   B. Information disclosure
   C. Tampering
   D. 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?
   A. Integrity
   B. Availability
   C. Confidentiality
   D. Denial

45. Which one of the following issues is not normally addressed in a service-level agreement (SLA)?
   A. Confidentiality of customer information
   B. Failover time
   C. Uptime
   D. 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?
   A. Trademark
   B. Copyright
   C. Patent
   D. Trade secret
Questions 47–49 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 LAN contains modern switch equipment connected to both wired and wireless networks.

Each office has its own file server, and the 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?
   A. Digital signatures
   B. Virtual private network
   C. Virtual LAN
   D. 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?
   A. Server clustering
   B. Load balancing
   C. RAID
   D. 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?
   A. Hashing
   B. ACLs
   C. Read-only attributes
   D. Firewalls

50. What law serves as the basis for privacy rights in the United States?
   A. Privacy Act of 1974
   B. Fourth Amendment
   C. First Amendment
   D. Electronic Communications Privacy Act of 1986
51. Which one of the following is not normally included in business continuity plan documentation?
   A. Statement of accounts
   B. Statement of importance
   C. Statement of priorities
   D. Statement of organizational responsibility

52. An accounting employee at Doolitte 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?
   A. Separation of duties
   B. Least privilege
   C. Defense in depth
   D. Mandatory vacation

53. Which one of the following is not normally considered a business continuity task?
   A. Business impact assessment
   B. Emergency response guidelines
   C. Electronic vaulting
   D. Vital records program

54. Which information security goal is impacted when an organization experiences a DoS or DDoS attack?
   A. Confidentiality
   B. Integrity
   C. Availability
   D. 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?
   A. Policy
   B. Baseline
   C. Guideline
   D. Procedure

56. Who should receive initial business continuity plan training in an organization?
   A. Senior executives
   B. Those with specific business continuity roles
C. Everyone in the organization
D. 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?
A. Purchase cost  
B. Depreciated cost  
C. Replacement cost  
D. 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?
A. National Security Agency  
B. Federal Communications Commission  
C. Department of Defense  
D. National Institute of Standards and Technology

59. Which one of the following is not a requirement for an invention to be patentable?
A. It must be new.  
B. It must be invented by an American citizen.  
C. It must be nonobvious.  
D. 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?
A. Confidentiality  
B. Integrity  
C. Availability  
D. Denial

61. What is the formula used to determine risk?
A. Risk = Threat * Vulnerability  
B. Risk = Threat / Vulnerability  
C. Risk = Asset * Threat  
D. Risk = Asset / Threat
62. The graphic below shows the NIST risk management framework with step 4 missing. What is the missing step?

A. Assess security controls
B. Determine control gaps
C. Remediate control gaps
D. 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?

A. Risk mitigation
B. Risk acceptance
C. Risk transference
D. 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?

A. Availability
B. Denial
C. Confidentiality
D. Integrity
65. Which one of the following components should be included in an organization’s emergency response guidelines?
   A. List of individuals who should be notified of an emergency incident
   B. Long-term business continuity protocols
   C. Activation procedures for the organization’s cold sites
   D. Contact information for ordering equipment

66. Who is the ideal person to approve an organization’s business continuity plan?
   A. Chief information officer
   B. Chief executive officer
   C. Chief information security officer
   D. 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?
   A. Structured analysis of the organization
   B. Review of the legal and regulatory landscape
   C. Creation of a BCP team
   D. Documentation of the plan

68. Gary is implementing a new RAID-based disk system designed to keep a server up and running even in the event of a single disk failure. What principle of information security is Gary seeking to enforce?
   A. Denial
   B. Confidentiality
   C. Integrity
   D. 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?
   A. Cold site
   B. Warm site
   C. Hot site
   D. Mobile site

70. What is the threshold for malicious damage to a federal computer system that triggers the Computer Fraud and Abuse Act?
   A. $500
   B. $2,500
   C. $5,000
   D. $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?
   A. ITIL
   B. ISO 27002
   C. CMM
   D. PMBOK Guide

72. Which one of the following laws requires that communications service providers cooperate with law enforcement requests?
   A. ECPA
   B. CALEA
   C. Privacy Act
   D. 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?
   A. FERPA
   B. GLBA
   C. HIPAA
   D. HITECH

74. Which one of the following agreements typically requires that a vendor not disclose confidential information learned during the scope of an engagement?
   A. NCA
   B. SLA
   C. NDA
   D. RTO

75. Which one of the following is not an example of a technical control?
   A. Router ACL
   B. Firewall rule
   C. Encryption
   D. Data classification

76. Which one of the following stakeholders is not typically included on a business continuity planning team?
   A. Core business function leaders
   B. Information technology staff
   C. CEO
   D. 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?

A. Authentication  
B. Authorization  
C. Integrity  
D. Nonrepudiation

78. What principle of information security states that an organization should implement overlapping security controls whenever possible?

A. Least privilege  
B. Separation of duties  
C. Defense in depth  
D. Security through obscurity

79. Which one of the following is not a goal of a formal change management program?

A. Implement change in an orderly fashion.  
B. Test changes prior to implementation.  
C. Provide rollback plans for changes.  
D. 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?

A. Purchasing insurance  
B. Encrypting the database contents  
C. Removing the data  
D. 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 below. Which quadrant contains the risks that require the most immediate attention?

![Risk Matrix](image-url)
A. I
B. II
C. III
D. 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?
   A. Informing other employees of the termination
   B. Retrieval of photo ID
   C. Calculation of final paycheck
   D. Revocation of 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?
   A. Risk avoidance
   B. Risk mitigation
   C. Risk transference
   D. 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?
   A. 13
   B. 15
   C. 17
   D. 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 below, 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?

A. 100
B. 1
C. 0.1
D. 0.01
86. You discover that a user on your network has been using the Wireshark tool, as shown in the following screen shot. Further investigation revealed that he was using it for illicit purposes. What pillar of information security has most likely been violated?

A. Integrity  
B. Denial  
C. Availability  
D. Confidentiality

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

A. Vulnerability assessment
B. Fuzzing
C. Reduction analysis
D. Data modeling

88. What law governs the handling of information related to the financial statements of publicly traded companies?
   A. GLBA
   B. PCI DSS
   C. HIPAA
   D. SOX

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 below 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?
90. Which one of the following tools is most often used for identification purposes and is not suitable for use as an authenticator?
   A. Password
   B. Retinal scan
   C. Username
   D. Token

91. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?
   A. Quantitative
   B. Qualitative
   C. Annualized loss expectancy
   D. Reduction

92. Which one of the following is the first step in developing an organization’s vital records program?
   A. Identifying vital records
   B. Locating vital records
C. Archiving vital records
D. 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?
   A. Awareness
   B. Training
   C. Education
   D. Indoctrination

94. Which one of the following security programs is designed to establish a minimum standard common denominator of security understanding?
   A. Training
   B. Education
   C. Indoctrination
   D. Awareness

95. Ryan is a security risk analyst for an insurance company. He is currently examining a scenario in which a 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?
   A. Unpatched web application
   B. Web defacement
   C. Hacker
   D. Operating system

Questions 96–98 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?
   A. 10%
   B. 25%
   C. 50%
   D. 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?
   A. 0.0025
   B. 0.005
   C. 0.01
   D. 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?
   A. $25,000
   B. $50,000
   C. $250,000
   D. $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?
   A. Spoofing
   B. Repudiation
   C. Information disclosure
   D. Elevation of privilege

100. Which one of the following is an administrative control that can protect the confidentiality of information?
    A. Encryption
    B. Non-disclosure agreement
    C. Firewall
    D. Fault tolerance