Chapter 1

Security and Risk Management (Domain 1)

SUBDOMAINS

- ✓ 1.1 Understand, adhere to, and promote professional ethics
- ✓ 1.2 Understand and apply security concepts
- ✓ 1.3 Evaluate, apply, and sustain security governance principles
- ✓ 1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context
- ✓ 1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- ✓ 1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
- ✓ 1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements
- ✓ 1.8 Contribute to and enforce personnel security policies and procedures
- ✓ 1.9 Understand and apply risk management concepts
- ✓ 1.10 Understand and apply threat modeling concepts and methodologies
- ✓ 1.11 Apply Supply Chain Risk Management (SCRM) concepts
- ✓ 1.12 Establish and maintain a security awareness, education, and training program

1. Alyssa is responsible for her organization's security awareness program. She is concerned that changes in technology may make the content outdated. What control can she put in place to protect against this risk?
   - **A.** Gamification
   - **B.** Computer-based training
   - **C.** Content reviews
   - **D.** Live training

2. Gavin is creating a report for management on the results of his most recent risk assessment. In his report, he would like to identify the remaining level of risk to the organization after adopting security controls. What term best describes this current level of risk?
   - **A.** Inherent risk
   - **B.** Residual risk
   - **C.** Control risk
   - **D.** Mitigated risk

3. Francine is a security specialist for an online service provider in the United States. She recently received a claim from a copyright holder that a user is storing information on her service that violates the third party's copyright. What law governs the actions that Francine must take?
   - **A.** Copyright Act
   - **B.** Lanham Act
   - **C.** Digital Millennium Copyright Act
   - **D.** Gramm-Leach-Bliley Act

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?
   - **A.** The right to access
   - **B.** Privacy by Design
   - **C.** The right to erasure
   - **D.** The right of data portability

5. After conducting a qualitative risk assessment of her organization, Sally recommends purchasing cybersecurity breach insurance. What type of risk response behavior is she recommending?
   - **A.** Accept
   - **B.** Transfer
   - **C.** Reduce
   - **D.** Reject

6. Which one of the following elements of information is not considered personally identifiable information that would trigger most United States state data breach laws?
   - **A.** Student identification number
   - **B.** Social Security number
   - **C.** Driver's license number
   - **D.** Credit card number

7. Renee is purchasing a new software product and is working with the vendor on the negotiation of a license agreement that will specify customized terms of use and a discounted price. What type of agreement would normally be used to document the results of this negotiation?
   - **A.** Perpetual license
   - **B.** Subscription license
   - **C.** Enterprise license agreement
   - **D.** End-user license agreement

8. Henry recently assisted one of his co-workers in preparing for the CISSP® exam. During this process, Henry disclosed confidential information about the content of the exam, in violation of Canon IV of the Code of Ethics: "Advance and protect the profession." Who may bring ethics charges against Henry for this violation?
   - **A.** Anyone may bring charges.
   - **B.** Any certified or licensed professional may bring charges.
   - **C.** Only Henry's employer may bring charges.
   - **D.** Only the affected employee may bring charges.

9. Wanda is working with one of her organization's European Union business partners to facilitate the exchange of customer information. Wanda's organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?
   - **A.** Binding corporate rules
   - **B.** Privacy Shield
   - **C.** Standard contractual clauses
   - **D.** Safe harbor

10. Yolanda is the chief privacy officer for a financial institution and is researching privacy requirements 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 threat 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 want 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. You are completing a review of the controls used to protect a media storage facility in your organization and would like to properly categorize each control that is currently in place. Which of the following control categories accurately describe a fence around a facility? (Select all that apply.)

A. Physical

B. Detection

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. Vincent believes that a former employee took trade secret information from his firm and brought it with him to a competitor. He wants to pursue legal action. Under what law could he pursue charges?

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. Brenda's organization recently completed the acquisition of a competitor firm. Which one of the following tasks would be LEAST likely to be part of the organizational processes addressed during the acquisition?

A. Consolidation of security functions

B. Integration of security tools

C. Protection of intellectual property

D. Documentation of security policies

20. Kelly believes that an employee engaged in the unauthorized use of computing resources for a side business. After consulting with management, she decides to launch an administrative investigation. What is the burden of proof that she must meet in this investigation?

A. Preponderance of the evidence.

B. Beyond a reasonable doubt.

C. Beyond the shadow of a doubt.

D. There is no standard.

21. Keenan Systems recently developed a new manufacturing process for microprocessors. The company wants to license the technology to other companies for use but wants 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. Laura has been asked to perform a security controls assessment (SCA). What type of organization is she most likely in?

A. Higher education

B. Banking

C. Government

D. Healthcare

26. Carl is a federal agent investigating a computer crime case. He identified an attacker who engaged in illegal conduct and wants to pursue a case against that individual that will lead to imprisonment. What standard of proof must Carl meet?

A. Beyond the shadow of a doubt

B. Preponderance of the evidence

C. Beyond a reasonable doubt

D. Majority of the evidence

27. ISC2 uses the logo shown here to represent itself online and in a variety of forums. What type of intellectual property protection can it use to protect its rights in this logo?

Source: ISC2, Inc.

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?

Source: CryptoLocker

A. Availability

B. Confidentiality

C. Disclosure

D. Distributed

29. Which one of the following organizations would not be automatically subject to the privacy and security requirements 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 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?

A. Availability

B. Integrity

C. Confidentiality

D. Denial

31. Renee is designing a long-term security plan for her organization and has a three- to five-year planning horizon. Her primary goal is to align the security function with the broader plans and objectives of the business. What type of plan is she developing?

A. Operational

B. Tactical

C. Summary

D. Strategic

32. Gina is working to protect a logo that her company will use for a new product they are launching. She has questions about the intellectual property protection process for this logo. What U.S. government agency would be best able to answer her questions?

A. USPTO

B. Library of Congress

C. NSA

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. Segregation 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 security control framework 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 U.S. federal government agency announcing that a new administrative law will affect his business operations. Where should he go to find the text of the law?

A. U.S. Code

B. Supreme Court rulings

C. Code of Federal Regulations

D. 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 by implementing this countermeasure?

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 (CIO)

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. You want to perform a control assessment 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

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?

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 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. Beth is a human resources specialist preparing to assist in the termination of an employee. Which of the following is not typically part of a termination process?

A. An exit interview

B. Recovery of organizational property

C. Account termination

D. Signing an NCA

51. Frances is reviewing her organization's business continuity plan documentation for completeness. 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 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?

A. Separation of duties

B. Least privilege

C. Defense in depth

D. Mandatory vacation

53. Jeff would like to adopt an industry-standard approach for assessing the processes his organization uses to manage risk. What maturity model would be most appropriate for his use?

A. CMM

B. SW-CMM

C. RMM

D. COBIT

54. Chris' organization recently suffered an attack that rendered their website inaccessible to paying customers for several hours. Which information security goal was most directly impacted?

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. Roger's organization suffered a breach of customer credit card records. Under the terms of PCI DSS, what organization may choose to pursue an investigation of this matter?

A. FBI

B. Local law enforcement

C. Bank

D. PCI SSC

59. Rick recently engaged critical employees in each of his organization's business units to ask for their assistance with his security awareness program. They will be responsible for sharing security messages with their peers and answering questions about cybersecurity matters. What term best describes this relationship?

A. Security champion

B. Security expert

C. Gamification

D. Peer review

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. Elise is helping her organization prepare to evaluate and adopt a new cloud-based human resource management (HRM) system vendor. What would be the most appropriate minimum security standard for her to require of possible vendors?

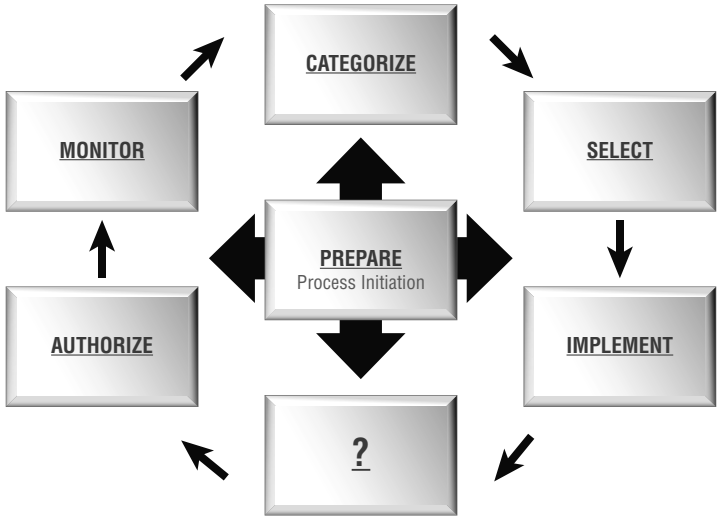
A. Compliance with all laws and regulations

B. Handling information in the same manner her organization would

C. Elimination of all identified security risks

D. Compliance with the vendor's own policies

62. The following graphic shows the NIST risk management framework with a step 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 disclosure 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. Chas recently completed the development of his organization's business continuity plan (BCP). 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 website architecture that uses multiple small web servers behind a load balancer. 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. Greg's company recently experienced a significant data breach involving the personal data of many of their customers. The company operates only in the United States and has facilities in several different states. The personal information relates only to residents of the United States. Which breach laws should they review to ensure that they are taking appropriate action?

A. The breach laws in the state where they are headquartered along with federal breach laws.

B. The breach laws of states they do business in or where their customers reside along with federal breach laws.

C. Only federal breach laws.

D. Breach laws only cover government agencies, not private businesses.

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. Matt works for a telecommunications firm and was approached by a federal agent seeking assistance with wiretapping one of Matt's clients pursuant to a search warrant. 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. The ISC2 Code of Ethics applies to all CISSP holders. Which of the following is not one of the four mandatory canons of the code?

A. Protect society, the common good, the necessary public trust and confidence, and the infrastructure.

B. Disclose breaches of privacy, trust, and ethics.

C. Provide diligent and competent service to the principals.

D. Advance and protect the profession.

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. Ryan is a CISSP-certified cybersecurity professional working in a nonprofit organization. Which of the following ethical obligations apply to his work? (Select all that apply.)

A. ISC2 Code of Ethics

B. Organizational code of ethics

C. Federal code of ethics

D. RFC 1087

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?

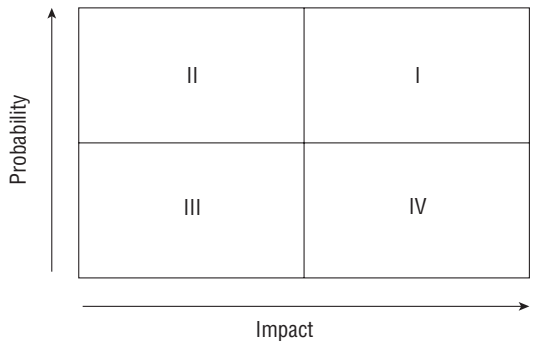
A. Purchasing insurance

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 here. Which quadrant contains the risks that require the most immediate attention?



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. Retrieving the employee's photo ID

C. Calculating the final paycheck

D. 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?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

84. Helen is the owner of a U.S. website that provides information for middle and high school students preparing for exams. She is writing the site's privacy policy and would like to ensure that it complies with the provisions 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?

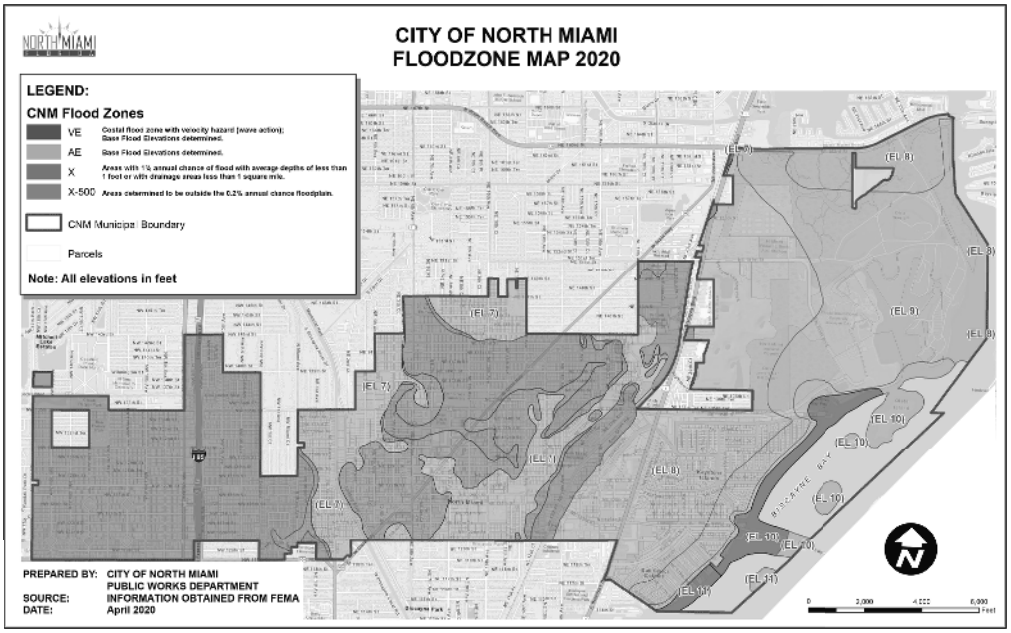
A. 13

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 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?



Source: The City of North Miami

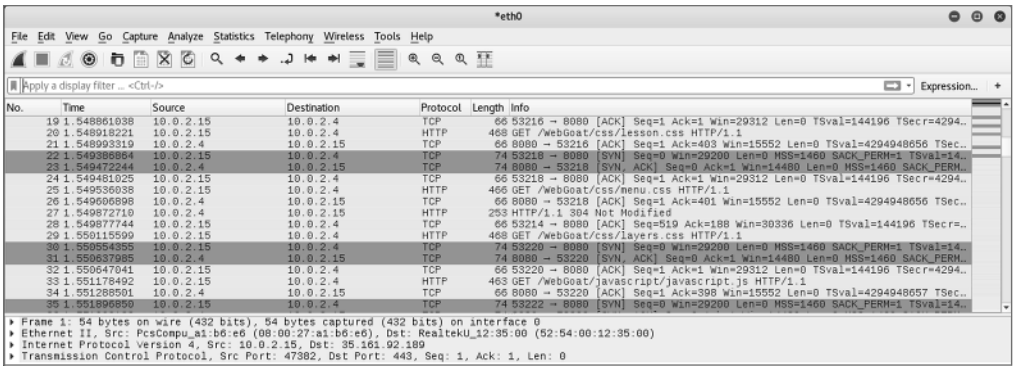
A. 100

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 here. Further investigation revealed that he was using it for illicit purposes. What pillar of information security has most likely been violated?



Source: The Wireshark Foundation

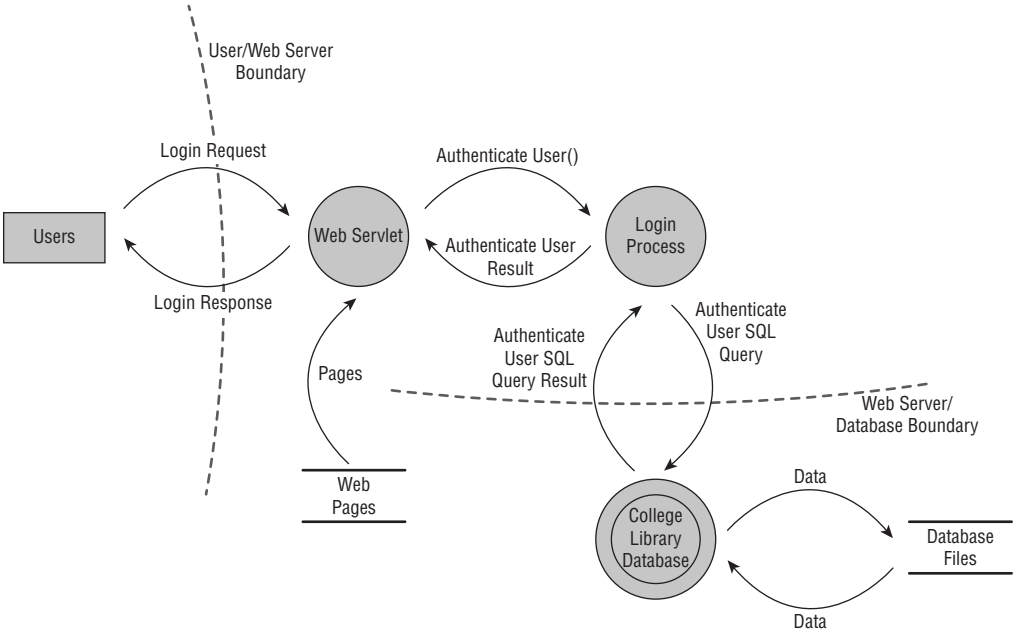
A. Integrity

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 core elements shown here. What tool is he using?



A. Vulnerability assessment

B. Fuzzing

C. Reduction analysis

D. Data modeling

88. Shahla is reviewing the privacy laws that apply to a new enterprise that her company will be launching in South Africa. This is the company's first expansion into that country, and the enterprise will involve handling the personal information of residents of South Africa. What law will likely affect this operation?

A. PIPL

B. PCI DSS

C. PIPEDA

D. POPIA

89. 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

90. 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?

A. Unpatched web application

B. Web defacement

C. Malicious hacker

D. Operating system

For questions 91–93, 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.

91. 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%

92. 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

93. 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

94. 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

95. 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?

A. His supply chain

B. His vendor contracts

C. His post-purchase build process

D. The original equipment manufacturer (OEM)

96. 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?

A. Regression testing

B. Code review

C. Change management

D. Fuzz testing

97. 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% completion rate he was aiming for. What is this type of measure called?

- **A.** A KPI
- **B.** A metric
- **C.** An awareness control
- **D.** A return on investment rate

98. Which of the following is not typically included in a prehire screening process?

- **A.** A drug test
- **B.** A background check
- **C.** Social media review
- **D.** Fitness evaluation

99. Which of the following would normally be considered a supply chain risk? (Select all that apply.)

- **A.** Adversary tampering with hardware prior to being shipped to the end customer
- **B.** Adversary hacking into a web server run by the organization in an IaaS environment
- **C.** Adversary using social engineering to compromise an employee of a SaaS vendor to gain access to customer accounts
- **D.** Adversary conducting a denial-of-service attack using a botnet

100. 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:

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