(ISC)² Mini eBook

Mike Chapple, CISSP
David Seidl, CISSP

CISSP®

Certified Information Systems Security Professional

FROM THE OFFICIAL PRACTICE TESTS

Second Edition

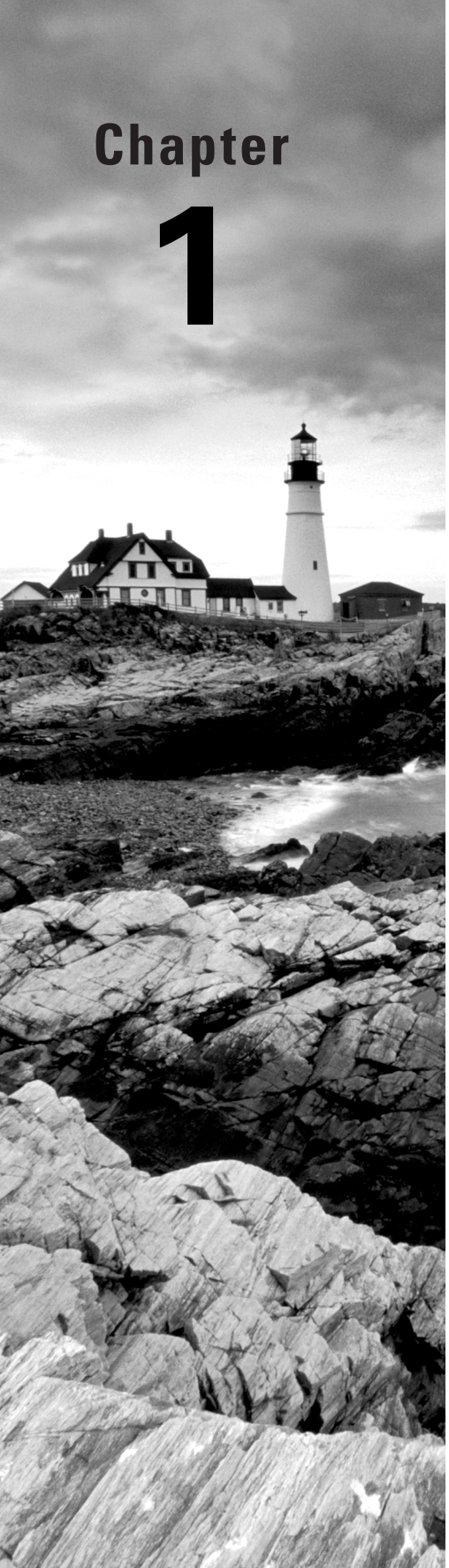
Provides a sneak peek into the Official CISSP Practice Tests book, including 50 CISSP practice test questions

Discount code inside!

SYBEX
A Wiley Brand

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. 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

   - **A.** An attack that relies on an access point to spoof a legitimate access point's SSID and Mandatory Access Control (MAC) address
   - **B.** An access point intended to attract new connections by using an apparently legitimate SSID
   - **C.** An attack that retransmits captured communication to attempt to gain access to a targeted system
   - **D.** 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?
   - **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 (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 be forgotten
   - **D.** The right of data portability

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 United States (U.S.) 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.** Personal identification number (PIN)
   - **C.** Security question
   - **D.** 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?
   - **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 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 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 level 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 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?

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?

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 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 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 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?

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 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

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 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?

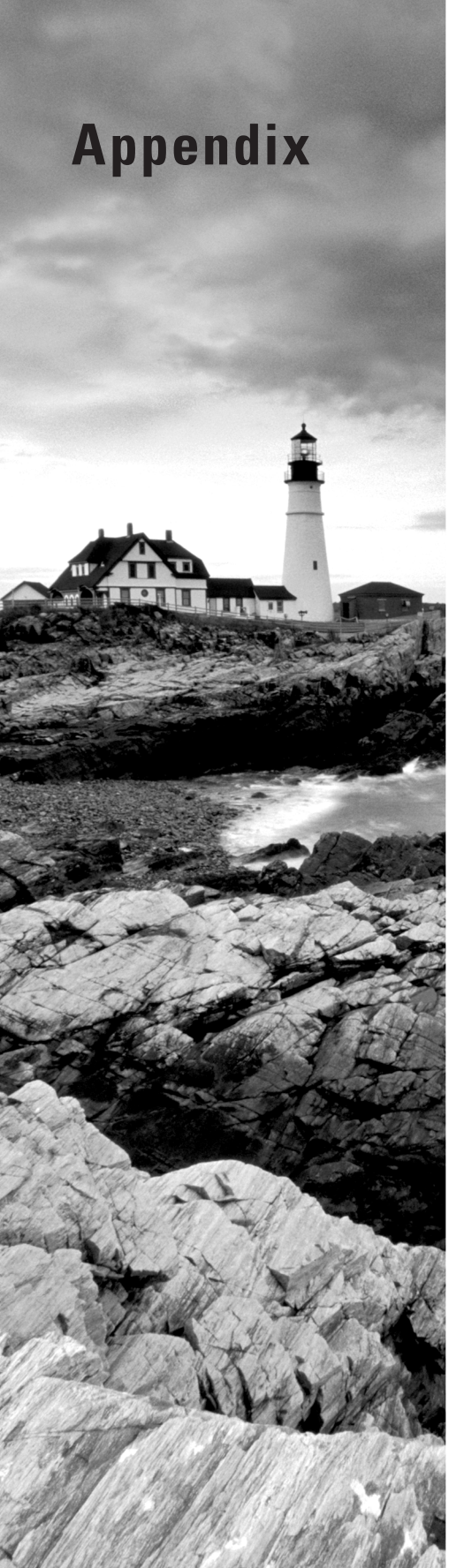
A. Privacy Act of 1974

B. Fourth Amendment

C. First Amendment

D. Electronic Communications Privacy Act of 1986

Appendix



Answers

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 modifiedbetween 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.

What's Next?

THE (ISC)^2 CERTIFICATION PREP KIT

Your Ultimate Guide to Exam Planning

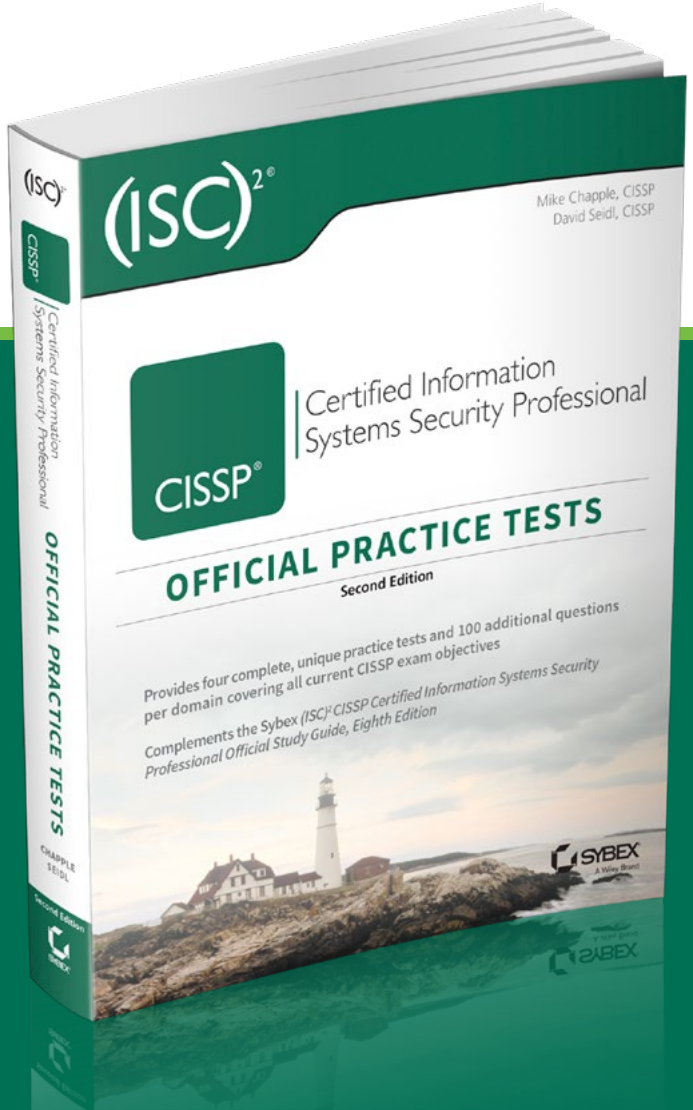
Preparing for the CISSP exam is no small task… Your path to success starts with the right study plan, and the Certification Prep Kit will help you map a course that fits your schedule and learning style. Dive right in for everything you'll need to move ahead with confidence.

Inside this free resource, you'll find…

- Fast Facts on Training and Study Tools
- Training Myths Debunked
- Official Courseware Previews
- Justification for Certification and Training
- The Best Study Options for Your Goals
- Insider Tips, Strategies and Insights

DOWNLOAD YOUR FREE KIT

LOOKING FOR MORE?



Get the FULL VERSION of the *Official (ISC)² CISSP Practice Tests* Book!

SAVE 30%

Use promo code

ISC30

at checkout.

ORDER TODAY