# CHAPTER 1

**1. Policies define which of the following?**

**A.** Rules

**B.** Expectations

**C.** Patterns of behavior

**D.** All of the above

**2. Without policy, human beings would live in a state of _.**

**A.** chaos

**B.** bliss

**C.** harmony

**D.** laziness

**3. A guiding principle is best described as which of the following?**

**A.** A financial target

**B.** A fundamental philosophy or belief

**C.** A regulatory requirement

**D.** A person in charge

**4. Which of the following best describes corporate culture?**

**A.** Shared attitudes, values, and goals

**B.** Multiculturalism

**C.** A requirement to all act the same

**D.** A religion

**5. Which of the following is a true statement?**

**A.** Corporate culture is the same as policy.

**B.** Guiding principles set the tone for a corporate culture.

**C.** All corporate cultures are positive.

**D.** Guiding principles should be kept secret.

**6. Which of the following best describes the role of policy?**

**A.** To codify guiding principles

**B.** To shape behavior

**C.** To serve as a roadmap

**D.** All of the above

### 7. An information security policy is a directive that defines which of the following?

**A.** How employees should do their jobs

**B.** How to pass an annual audit

**C.** How an organization protects information assets and systems

**D.** How much security insurance a company should have

### 8. Which of the following is not an example of an information asset?

**A.** Customer financial records

**B.** Marketing plan

**C.** Patient medical history

**D.** Building graffiti

### 9. What are the seven characteristics of a successful policy?

**A.** Endorsed, relevant, realistic, cost-effective, adaptable, enforceable, inclusive

**B.** Endorsed, relevant, realistic, attainable, adaptable, enforceable, inclusive

**C.** Endorsed, relevant, realistic, technical, adaptable, enforceable, inclusive

**D.** Endorsed, relevant, realistic, legal, adaptable, enforceable, inclusive

### 10. A policy that has been endorsed has the support of which of the following?

**A.** Customers

**B.** Creditors

**C.** The union

**D.** Management

**11. Who should always be exempt from policy requirements?**

**A.** Employees
**B.** Executives
**C.** No one
**D.** Salespeople

**12. "Attainable" means that the policy _.**

**A.** can be successfully implemented
**B.** is expensive
**C.** only applies to suppliers
**D.** must be modified annually

**13. Which of the following statements is always true?**

**A.** Policies stifle innovation.
**B.** Policies make innovation more expensive.
**C.** Policies should be adaptable.
**D.** Effective policies never change.

**14. If a policy is violated and there is no consequence, the policy is considered to be which of the following?**

**A.** Meaningless
**B.** Inclusive
**C.** Legal
**D.** Expired

**15. Who must approve the retirement of a policy?**

**A.** A compliance officer
**B.** An auditor
**C.** Executive management or the Board of Directors
**D.** Legal counsel

**16. Which of the following sectors is not considered part of the "critical infrastructure"?**

**A.** Public health
**B.** Commerce
**C.** Banking
**D.** Chemical industry

**17. Which term best describes government intervention with the purpose of causing a specific set of actions?**

**A.** Deregulation

**B.** Politics

**C.** Regulation

**D.** Amendments

**18. The objectives of GLBA and HIPAA, respectively, are to protect _.**

**A.** financial and medical records

**B.** financial and credit card records

**C.** medical and student records

**D.** judicial and medical records

**19. Which of the following states was the first to enact consumer breach notification?**

**A.** Kentucky

**B.** Colorado

**C.** Connecticut

**D.** California

**20. In 2010, Massachusetts became the first state in the nation to require .**

**A.** minimum standards for the protection of personally identifiable information of non-residents

**B.** minimum standards for the protection of personally identifiable information of Massachusetts residents

**C.** maximum standards for the protection of personally identifiable information of Massachusetts residents

**D.** consumer notification of a breach

**21. Which of the following terms best describes the process of developing, publishing, adopting, and reviewing a policy?**

**A.** Policy two-step

**B.** Policy aging

**C.** Policy retirement

**D.** Policy lifecycle

**22. Who should be involved in the process of developing policies?**

**A.** Only upper-management-level executives

**B.** Only part-time employees

**C.** Personnel throughout the company

**D.** Only outside, third-party consultants

**23. Which of the following does not happen in the policy development phase?**

**A.** Planning

**B.** Enforcement

**C.** Authorization

**D.** Approval

**24. Which of the following occurs in the policy publication phase?**

**A.** Communication

**B.** Policy dissemination

**C.** Education

**D.** All of the above

**25. Normative integration is the goal of the adoption phase. This means _.**

**A.** A here are no exceptions to the policy.

**B.** The policy passes the stress test.

**C.** The policy becomes expected behavior, all others being deviant.

**D.** The policy costs little to implement.

### 26. How often should policies be reviewed?

**A.** Never

**B.** Only when there is a significant change

**C.** Annually

**D.** At least annually or sooner if there is a significant change

### 27. Which of the following phrases best describes the concept of “championing a policy”?

**A.** A willingness to lead by example, encourage, and educate

**B.** Winning a compliance award
**C.** Voting to authorize a policy
**D.** None of the above

### 28. Which of the following phrases best describes the philosophy of “honoring the public trust”?

**A.** Being respectful of law enforcement

**B.** Contributing to political campaigns

**C.** Being a careful steward of information in your care

**D.** Visiting government monuments

### 29. Who should authorize policies?

**A.** Directors or executive management

**B.** Operational managers

**C.** Employees

**D.** Legal counsel

### 30. Which of the following statements is not an objective of information security?

**A.** To protect information and information systems from intentional misuse

**B.** To protect information and information systems from compromise

**C.** To protect information and information systems from destruction

**D.** To protect information and information systems from authorized users

A. Discussion Question 1

In addition to the Bible and the U.S. Constitution, identify another written policy that had (or still has) a profound effect on societies across the globe, including our own.

Answer: Students' answers will vary. An acceptable policy should have been created out of a perceived need to guide human behavior in foreseeable circumstances, and even to guide human behavior when circumstances could not be or were not foreseen.

B. Discussion Question 2

How do policies communicate corporate culture?

Answer: Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company or corporation. These attitudes, values, goals, and practices are communicated to all the organization's employees, vendors, partners, and customers with policies that support organizational goals and provide expectations to help sustain consistency in the organization's services and products.

## CHAPTER 2

### 1. The policy hierarchy is the relationships between which of the following?

**A.** Guiding principles, regulations, laws, and procedures

**B.** Guiding principles, standards, guidelines, and procedures
**C.** Guiding principles, instructions, guidelines, and programs
**D.** None of the above

### 2. Which of the following statements best describes the purpose of a standard?

**A.** To state the beliefs of an organization

**B.** To reflect the guiding principles

**C.** To dictate mandatory requirements

**D.** To make suggestions

### 3. Which of the following statements best describes the purpose of a guideline?

**A.** To state the beliefs of an organization

**B.** To reflect the guiding principles

**C.** To dictate mandatory requirements

**D.** To make suggestions

### 4. Which of the following statements best describes the purpose of a baseline?

**A.** To measure compliance

**B.** To ensure uniformity across a similar set of devices

**C.** To ensure uniformity across different devices

**D.** To make suggestions

**5. Simple Step, Hierarchical, Graphic, and Flowchart are examples of which of the following formats?**

**A.** Policy

**B.** Program

**C.** Procedure

**D.** Standard

**6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources?**

**A.** Plan

**B.** Policy

**C.** Procedure

**D.** Package

**7. Which of the following statements best describes a disadvantage to using the singular policy format?**

**A.** The policy can be short.

**B.** The policy can be targeted.

**C.** You may end up with too many policies to maintain.

**D.** The policy can easily be updated.

**8. Which of the following statements best describes a disadvantage to using the consolidated policy format?**

**A.** Consistent language is used throughout the document.

**B.** Only one policy document must be maintained.

**C.** The format must include a composite management statement.

**D.** The potential size of the document.

**9. Policies, standards, guidelines, and procedures should all be in the same document.**

**A.** True

**B.** False

**C.** Only if the company is multinational

**D.** Only if the documents have the same author

**10. Version control is the management of changes to a document and should include which of the following elements?**

**A.** Version or revision number

**B.** Date of authorization

**C.** Change description

**D.** All of the above

**11. Which of the following is not a policy introduction objective?**

**A.** To convey the importance of understanding and adhering to the policy

**B.** To provide explicit instructions on how to comply with the policy

**C.** To explain the exemption process as well as the consequence of non-compliance

**D.** To thank the reader and to reinforce the authority of the policy

**12. The name of the policy, policy number, and overview belong in which of the following sections?**

**A.** Introduction

**B.** Policy Heading

**C.** Policy Goals and Objectives

**D.** Policy Statement

**13. The aim or intent of a policy is stated in the _.**

**A.** introduction

**B.** policy heading

**C.** policy goals and objectives

**D.** policy statement

**14. Which of the following statements is true?**

**A.** A security policy should only include one objective.
**B.** A security policy should not include any exceptions.
**C.** A security policy should not include a glossary.

**D.** A security policy should not list all step-by-step measures that need to be taken.

**15. The_____ contains the rules that must be followed.**

**A.** policy heading

**B.** policy statement

**C.** policy enforcement clause

**D.** policy goals and objectives

**16. A policy should be considered_____.**

**A.** mandatory

**B.** discretionary

**C.** situational

**D.** optional

**17. Which of the following best describes policy definitions?**

**A.** A glossary of terms used

**B.** A detailed list of the possible penalties associated with breaking rules set forth in the policy

**C.** A list of all the members of the security policy creation team

**D.** None of the above

**18. The _____contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.**

**A.** policy heading

**B.** policy statement

**C.** policy enforcement clause

**D.** policy statement of authority

**19. What component of a security policy does the following phrase belong to?**

"Wireless networks are allowed only if they are separate and distinct from the corporate network."

**A.** Introduction

**B.** Administrative notation

**C.** The policy heading

**D.** The policy statement

**20. There may be situations where it is not possible to comply with a policy directive. Where should the exemption or waiver process be explained?**

**A.** Introduction

**B.** The policy statement

**C.** The policy enforcement clause

**D.** The policy exceptions

**21. The name of the person/group (for example, executive committee) that authorized the policy should be included in _____ _.**

**A.** the version control table or the policy statement

**B.** the heading or the policy statement

**C.** the policy statement or the policy exceptions

**D.** the version control table or the policy heading

**22. When you're drafting a list of exceptions for a security policy, the language should _____.**

**A.** be as specific as possible

**B.** be as vague as possible

**C.** reference another, dedicated document

**D.** None of the above

**23. If supporting documentation would be of use to the reader, it should be_____.**

**A.** included in full in the policy document

**B.** ignored because supporting documentation does not belong in a policy document

**C.** listed in either the Policy Heading or Administrative Notation section

**D.** included in a policy appendix

**24. When writing a policy, standard, guideline, or procedure, you should use language that is _____.**

**A.** technical

**B.** clear and concise

**C.** legalese

**D.** complex

**25. Readers prefer "plain language" because it _____ .**

**A.** helps them locate pertinent information
**B.** helps them understand the information
**C.** saves time

**D.** All of the above

**26. Which of the following is not a characteristic of plain language?**

**A.** Short sentences

**B.** Using active voice

**C.** Technical jargon

**D.** Seven or fewer lines per paragraph

**27. Which of the following terms is best to use when indicating a mandatory requirement?**

**A.** must

**B.** shall

**C.** should not

**D.** may not

**28. A company that uses the term "employees" to refer to workers who are on the company payroll should refer to them throughout their policies as _____.**

**A.** workforce members

**B.** employees

**C.** hired hands

**D.** workers

**29. "The ball was thrown by Sam to Sally" is a passive sentence. Which of the following sentences represents an active version of this sentence?**

**A.** The ball was thrown to Sally by Sam.

**B.** Sally caught the ball.

**C.** Sam threw the ball to Sally.

**D.** The ball was thrown by Sam to Sally, who caught it.

**30. Even the best-written policy will fail if which of the following is true?**

**A.** The policy is too long.

**B.** The policy is mandated by the government.

**C.** The policy doesn't have the support of management.

**D.** All of the above.

A. Discussion Question 1

What is the difference between a policy objective and a policy purpose?

Answer: Students' answers will vary. Essentially, the policy objective is to achieve a broad goal to more efficiently protect the company. The policy purpose explains how the company will protect itself from specific threats using the actual rules of the policy.

B. Discussion Question 2

Why are policy definitions an important part of any policy?

Answer: Student answers should focus on the use of definitions to enhance understanding of the policy and the need to define a target audience. Another important reason for definitions is to remove all ambiguity from the policy. A security policy should be viewed as a legal document and crafted carefully

## CHAPTER 3

**1. Which of the following are the three principles in the CIA triad?**

**A.** Confidence, integration, availability

**B.** Consistency, integrity, authentication

**C.** Confidentiality, integrity, availability **D.** Confidentiality, integrity, awareness

**2. Which of the following is an example of acting upon the goal of integrity?**

**A.** Ensuing that only authorized users can access data

**B.** Ensuring that systems have 99.9% uptime

**C.** Ensuring that all modifications go through a change-control process

**D.** Ensuring that changes can be traced back to the editor

**3. Which of the following is a control that relates to availability?**

**A.** Disaster recovery site

**B.** Firewall

**C.** Training

**D.** Encryption

**4. Which of the following is an objective of confidentiality?**

**A.** Protection from unauthorized access

**B.** Protection from manipulation

**C.** Protection from denial of service

**D.** Protection from authorized access

**5. As it pertains to information security, assurance is _____.**

**A.** the process of tracing actions to their source

**B.** the processes, policies, and controls used to develop confidence that security measures are working as intended

**C.** the positive identification of the person or system seeking access to secured information or systems

**D.** the logging of access and usage of information resources

**6. Which of the following terms best describes the granting of users and systems a predetermined level of access to information resources?**

**A.** Availability

**B.** Accountability

**C.** Assurance

**D.** Authorization

**7. Which of the following statements identify threats to availability? (Select all that apply.)**

**A.** Loss of processing capabilities due to natural disaster or human error

**B.** Loss of confidentiality due to unauthorized access

**C.** Loss of personnel due to accident

**D.** Loss of reputation from unauthorized event

**8. Which of the following terms best describes the logging of access and usage of information resources?**

**A.** Accountability

**B.** Acceptance

**C.** Accounting **D.** Actuality

**9. Which of the following combination of terms best describes the Five A's of information security?**

**A.** Awareness, acceptance, availability, accountability, authentication

**B.** Awareness, acceptance, authority, authentication, availability

**C.** Accountability, assurance, authorization, authentication, accounting

**D.** Acceptance, authentication, availability, assurance, accounting

**10. An information owner is responsible for _____.**

**A.** maintaining the systems that store, process, and transmit information

**B.** protecting the information and the business results derived from use of that information

**C.** protecting the people and processes used to access digital information

**D.** none of the above

**11. Which of the following terms best describes ISO?**

**A.** Internal Standards Organization

**B.** International Organization for Standardization

**C.** International Standards Organization

**D.** Internal Organization of Systemization

**12. Which of the following statements best describes opportunistic crime?**

**A.** Crime that is well-planned

**B.** Crime that is targeted

**C.** Crime that takes advantage of an identified weakness

**D.** Crime that is quick and easy

**13. Which of the following terms best describes the motivation for hactivism?**

**A.** Financial
**B.** Political **C.**
Personal **E.**
Fun

**14. The greater the criminal work factor, the _____**

**A.** more time it takes

**B.** more profitable the crime is

**C.** better chance of success

**D.** less chance of getting caught

**15. Which of the following terms best describes an attack whose purpose is to make a machine or network resource unavailable for its intended use?**

**A.** Man-in-the-middle

**B.** Data breach

**C.** Denial of service

**D.** SQL injection

**16. Information custodians are responsible for ___**

**A.** writing policy

**B.** classifying data

**C.** approving budgets

**E.** implementing safeguards

**17. The National Institute of Standards and Technology (NIST) is a(n) _____**

**A.** international organization

**B.** privately funded organization

**C.** U.S. government agency

**D.** European Union agency

**18. The Internal Organization for Standardization (ISO) is _____**

**A.** a nongovernmental organization

**B.** an international organization

**C.** headquartered in Geneva

**D.** all of the above

**19. The current ISO family of standards that relates to information security is _____.**

**A.** BS 7799:1995

**B.** ISO 17799:2006

**C.** ISO/IEC 27000

**D.** None of the above

**20. Which of the following terms best describes the security domain that relates to determining the appropriate safeguards as it relates to the likelihood of a threat to an organization?**

**A.** Security policy
**B.** Access control
**C.** Compliance

**D.** Risk assessment

**21. Which of the following terms best describes the security domain that relates to how data is classified and valued?**

**A.** Security policy

**B.** Asset management

**C.** Compliance

**D.** Access control

**22. Which of the following terms best describes the security domain that includes HVAC, fire suppression, and secure offices?**

**A.** Operations

**B.** Communications

**C.** Risk assessment

**D.** Physical and environmental controls

**23. Which of the following terms best describes the security domain that aligns most closely with the objective of confidentiality?**

**A.** Access control

**B.** Compliance

**C.** Incident management

**D.** Business continuity

**24. The primary objective of the_____domain is to ensure conformance with GLBA, HIPAA, PCI/DSS, FERPA, and FISMA.**

**A.** Security Policy

**B.** Compliance

**C.** Access Control

**D.** Contract and Regulatory

**25. Processes that include responding to a malware infection, conducting forensics investigations, and reporting breaches are included in the _____domain.**

**A.** Security Policy

**B.** Operations and Communications

**C.** Incident Management

**D.** Business Continuity Management

**26. Which of the following terms best describes a synonym for business continuity?**

**A.** Authorization
**B.** Authentication
**C.** Availability

**D.** Accountability

**27. The _____can be held legally responsible for the safeguarding of legally protected information.**

**A.** information user

**B.** information owner

**C.** information custodian

**D.** information author

**28. Personnel screening, acceptable use, confidentiality agreements, and training are controls that relate to the _____ domain.**

**A.** Operations and Communications

**B.** Security Policy

**C.** Human Resources

**D.** Legal and Compliance

**29. Defining organizational roles, responsibilities, and authority relate to the_____ domain.**

**A.** Operations and Communications

**B.** Security Policy

**C.** Governance

**D.** Legal and Compliance

**30. Which of the following security objectives is most important to an organization?**

**A.** Confidentiality

**B.** Integrity

**C.** Availability

**D.** The answer may vary from organization to organization.

A. Discussion Question 1

How does the ISO 27002:2013 standard relate to an organization's information security policy?

Answer: Student answers will vary. The standard is a comprehensive set of information security recommendations comprising best practices in information security. As such, it provides a framework to help organizations of any size develop appropriate controls to maintain the confidentiality, integrity, and availability of information.

B. Discussion Question 2

Describe an effective policy.

Answer: Student answers will vary. For policies to be effective, they must be meaningful and relevant as well as appropriate to the size and complexity of the organization. The key is to understand what policy and control may be needed in any given environment and then develop, adopt, and implement the controls and policies that make sense for the organization.

## CHAPTER 4

**1. When an information security program is said to be "strategically aligned," this indicates that _____.**

**A.** It supports business objectives

**B.** It adds value

**C.** It maintains compliance with regulatory requirements

**D.** All of the above

**2. How often should information security policies be reviewed?**

**A.** Once a year

**B.** Only when a change needs to be made

**C.** At a minimum, once a year and whenever there is a change trigger

**D.** Only as required by law

**3. Information security policies should be authorized by _____.**

**A.** the Board of Directors (or equivalent)

**B.** business unit managers

**C.** legal counsel

**D.** stockholders

**4. Which of the following statements best describes policies?**

**A.** Policies are the implementation of specifications.

**B.** Policies are suggested actions or recommendations.

**C.** Policies are instructions.

**D.** Policies are the directives that codify organizational requirements.

**5. Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive information security policy?**

**A.** Sections of the comprehensive policy may not be applicable to all employees.

**B.** The comprehensive policy may include unknown acronyms.

**C.** The comprehensive document may contain confidential information.

**D.** The more understandable and relevant a policy is, the more likely users will positively respond to it.

**6. Which of the following is a common element of all federal information security regulations?**

**A.** Covered entities must have a written information security policy.

**B.** Covered entities must use federally mandated technology.

**C.** Covered entities must self-report compliance.

**D.** Covered entities must notify law enforcement if there is a policy violation.

**7. Organizations that choose to adopt the ISO 27002:2103 framework must _____.**

**A.** use every policy, standard, and guideline recommended

**B.** create policies for every security domain

**C.** evaluate the applicability and customize as appropriate

**D.** register with the ISO

**8. Evidence-based techniques used by information security auditors include which of the following elements?**

**A.** Structured interviews, observation, financial analysis, and documentation sampling

**B.** Structured interviews, observation, review of practices, and documentation sampling

**C.** Structured interviews, customer service surveys, review of practices, and documentation sampling

**D.** Casual conversations, observation, review of practices, and documentation sampling

**9. Which of the following statements best describes independence in the context of auditing?**

**A.** The auditor is not an employee of the company.

**B.** The auditor is certified to conduct audits.

**C.** The auditor is not responsible for, benefited from, or in any way influenced by the audit target.

**D.** Each auditor presents his or her own opinion.

**10. Which of the following states is not included in a CMM?**

**A.** Average

**B.** Optimized

**C.** Ad hoc

**D.** Manage

**11. Which of the following activities is not considered a governance activity?**

**A. Managing**

**B. Influencing**

**C. Evaluating**

**D.** Purchasing

**12. To avoid conflict of interest, the CISO could report to which of the following individuals?**

**A.** The Chief Information Officer (CIO)

**B.** The Chief Technology Officer (CTO)

**C.** The Chief Financial Officer (CFO)

**D.** The Chief Compliance Officer (CCO)

**13. Which of the following statements best describes the role of the Information Security Steering Committee?**

**A.** The committee authorizes policy.

**B.** The committee serves in an advisory capacity.

**C.** The committee approves the InfoSec budget.

**D.** None of the above.

**14. Defining protection requirements is the responsibility of_____**

**A. the ISO**

**B. the data custodian**

**C. data owners**

**D. the Compliance Officer**

**15. Designating an individual or team to coordinate or manage information security is required by _____.**

**A. GLBA**

**B.MA CMR 17 301**

**C.PCI DSS**

**D. All of the above**

**16. Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?**

**A. Threat**

**B. Risk**

**C. Vulnerability**

**D. Impact**

**17.** Inherent risk is the state before _____.

**A.** an assessment has been conducted

**B.** security measures have been implemented

**C.** the risk has been accepted

**D. None of the above**

**18. Which of the following terms best describes the natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact?**

**A. Risk**

**B. Threat source**

**C. Threat**

**D. Vulnerability**

### 19. Which of the following terms best describes a disgruntled employee with intent to do harm?

**A. Risk**

**B. Threat source**

**C. Threat**

**D. Vulnerability**

### 20. Which if the following activities is not considered an element of risk management?

**A.** The process of determining an acceptable level of risk
**B.** Assessing the current level of risk for a given situation
**C.** Accepting the risk

**D. Installing risk-mitigation safeguards**

### 21. How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as _____.

**A. risk acceptance**

**B.** risk tolerance

**D. risk Mitigation**

**D. risk avoidance**

### 22. Which of the following statements best describes a vulnerability?

**A.** A vulnerability is a weakness that could be exploited by a threat source.

**B.** A vulnerability is a weakness that can never be fixed.

**C.** A vulnerability is a weakness that can only be identified by testing.

**D.** A vulnerability is a weakness that must be addressed regardless of the cost.

### 23. A control is a security measure that is designed to _____ a threat source.

**A.** detect

**B.** deter

**C.** prevent

**D.** All of the above

### 24. Which of the following is not a risk-mitigation action?

**A.** Risk acceptance

**B.** Risk sharing or transference

**C.** Risk reduction

**D.** Risk avoidance

### 25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?

**A.** Inherent risk

**B. Expected risk**

**C.** Residual risk

**D.** Accepted risk

### 26. Which of the following risk types best describes an example of insurance?

**A.** Risk avoidance

**B.** Risk transfer

**C.** Risk acknowledgement

**D.** Risk acceptance

### 27. Which of the following risk types relates to negative public opinion?

**A.** Operational risk

**B.** Financial risk

**C.** Reputation risk

**D.** Strategic risk

### 28. Compliance risk as it relates to federal and state regulations can never be _____.

**A.** avoided

**B.** transferred

**C.** accepted

**D.** None of the above

### 29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?

**A.** They must have different policies for each regulation.

**B.** They must have multiple ISOs.

**C.** They must ensure that their information security program includes all applicable requirements.

**D.** They must choose the one regulation that takes precedence.

### 30. Which of the following terms best describes "duty of care" as applied to corporate directors and executive officers?

**A.** It's a legal obligation.

**B.** It's an outdated requirement.

**C.** It's ignored by most organizations.

**D.** It's a factor only when there is a loss greater than $1,000.

A. Discussion Question 1

Why should a statement of authority reflect the organization's culture?

Answer: Students' answers will vary. The SOA should be thought of as a teaching tool sprinkled with a motivational "pep talk," so the most effective communication will take into account the audience's background, education, experience, age, and even native language. Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company or corporation.

B. Discussion Question 2

Ideally, who is involved in designing and maintaining a secure organizational environment?

Answer: Students' answers will vary. This is a huge undertaking that requires input from professionals throughout an organization, including members of management, developers, network engineers and administrators, Human Resources, and legal and financial communities. Following the rules is possible only if the infrastructure is designed in such a way that following the rules is easy and doesn't hinder performance or productivity, which requires input

from all levels of the organization.

## CHAPTER 5

### 1. Which of the following terms best describes a definable piece of information, stored in any manner, that is recognized as having value to the organization?

**A.** NPPI

**B.** Information asset

**C.** Information system

**D.** Classified data

### 2. Information systems _____, _____, and _____ information.

**A.** create, modify, and delete

**B.** classify, reclassify, and declassify

**C.** store, process, and transmit

**D.** use, label, and handle

### 3. Information owners are responsible for which of the following tasks?

**A.** Classifying information

B. Maintaining
information

**C.** Using information

**D.** Registering information

### 4. Which of the following roles is responsible for implementing and maintaining security controls?

A.Information owner

**B.**Information
vendor

**C.** Information user

**D.** Information custodian

### 5. FIPS-199 requires that federal government information and information systems be classified as _____.

**A.** Low security

**B.** Moderate security

**C.** High security

**D.** None of the above

### 6. Information classification systems are used in which of the following organizations?

**A.** Government

**B.** Military

**C.** Financial institutions

**D.** All of the above

### 7. FIPS requires that information be evaluated for_____requirements with respect to the impact of unauthorized disclosure as well as the use of the information.

**A.** integrity

**B.** availability

**C.** confidentiality

**D.** secrecy

**8. Which of the following National Security classifications requires the most protection?**

**A.** Secret

**B.** Top Secret

**C.**
**Confidential**

**D.**
Unclassified

**9. Which of the following National Security classifications requires the least protection?**

**A.** Secret

**B.** Unclassified

**C.** Confidential

**D.** Sensitive But Unclassified (SBU)

**10. The Freedom of Information Act (FOIA) allows anyone access to which of the following?**

**A.** Access to all government information just by asking

**B.** Access to all classified documents

**C.** Access to classified documents on a “need to know” basis

**D.** Access to any records from federal agencies unless the documents can be officially declared exempt

**11. Which of the following terms best describes the CIA attribute associated with the modification of information?**

**A.** Classified

**B.** Integrity

**C.** Availability

**D.** Intelligence

**12. Is it mandatory for all private businesses to classify information?**

**A.** Yes.

**B.** Yes, but only if they want to pay less taxes.

**C.** Yes, but only if they do business with the government.

**D.** No.

**13. Which of the following is not a criterion for classifying information?**

**A.** The information is not intended for the public domain.

**B.** The information has no value to the organization.

**C.** The information needs to be protected from those outside of the organization.

**D.** The information is subject to government regulations.

### 14. Data that is considered to be personal in nature and, if disclosed, is an invasion of privacy and a compromise of security is known as which of the following?

**A.** Non-personal public information

**B.** Non-private personal information

**C.** Non-public personalinformation

**D.** None of the above

### 15. Most organizations restrict access to protected, confidential, and internal-use data to which of the following roles within the organization?

**A.** Executives

**B.** Information owners

**C.** Users who have a "nee d to know"

**D.** Vendors

### 16. Labeling is the vehicle for communicating classification levels to which of the following roles within the organization?

**A.** Employees

**B.** Information custodians

**C.** Contractors

**D.** All of the above

### 17. Which of the following terms best describes rules for how to store, retain, and destroy data based on classification?

**A.** Handling standards

**B.** Classification procedures

**C.** Use policies

**D.** Material guidelines

### 18. Which of the following terms best describes the process of removing restricted classification levels?

**A.** Declassification

**B.** Classification

**C.** Reclassification

**D.** Negative classification

**19. Which of the following terms best describes the process of upgrading or changing classification levels?**

**A.** Declassification

**B.** Classification

**C.** Reclassification

**D.** Negative classification

**20. The impact of destruction and/or permanent loss of information is used to determine which of the following safeguards?**

**A.** Authorization

**B.** Availability

**C.** Authentication

**D.** Accounting

**21. Which of the following terms best describes an example of a hardware asset?**

**A.** Server

**B.** Database

**C.** Hammer

**D.** Radio waves

**22. Which of the following statements best describes a MAC address?**

**A.** A MAC address is a unique network address.

**B.** A MAC address is a unique host name.

**C.** A MAC address is a unique hardware identifier.

**D.** A MAC address is a unique alias.

**23. 10.1.45.245 is an example of which of the following?**

**A.** A MAC address

**B.** A host name

**C.** An IP address

**D.** An IP domain name

**24. Code and databases are examples of which of the following?**

**A.** Software assets

**B.** Proprietary information

**C.** Internal-use classification

**D.** Intellectual property (IP)

**25. Which of the following terms best describes the act of classifying information based on an original classification decision already made by an authorized original classification authority?**

**A.** Reclassification

**B.** Derivative classification

**C.** Declassification

**D.** Original classification

**26. Which of the following types of information would not be considered NPPI?**

**A.** Social security number

**B.** Date of birth

**C.** Debit card PIN

**D.** Home address

**27. In keeping with best practices and regulatory expectations, legally protected data that is stored on mobile devices should be ____.**

**A.** masked

**B.** encrypted

**C.** labeled

**D.** segregated

**28. Which of the following statements best describes how written documents that contain NPPI should be handled?**

**A.** Written documents that contain NPPI should be stored in locked areas or in a locked cabinet.

**B.** Written documents that contain NPPI should be destroyed by cross-cut shredding.

**C.** Written documents that contain NPPI should be subject to company retention policies.

**D.** All of the above.

**29. Which of the following address types represents a device location on a network?**

**A.** A physical address

**B.** A MAC address

**C.** A logical address

**D.** A static address

### 30. Which of the following statements is true?

**A.** Small businesses do *not* need to classify data because it is unusual for a small business to have NPPI.

**B.** Small businesses do *not* need to classify data because small businesses do not have regulatory obligations.

**C.** Small businesses need to classify data because small businesses are responsible for protecting NPPI, employee data, and company data.

**D.** Small businesses need to classify data because every organization is legally required to have a classification system.

A. Discussion Question 1

Many organizations do not have an up-to-date inventory of information systems. What are the benefits of such an inventory?

Answer: Students' answers will vary. Identified benefits of an information systems inventory may include consolidation and/or merger of redundant systems (or information); improved business impact and disaster recovery planning insurance coverage; business valuation; and enhanced criticality and risk analysis.

B. Discussion Question 2

What sorts of routine, seemingly unimportant information would help you learn about or break into another company's network?

Answer: Student answers will vary. Possible answers include policy and procedure manuals, telephone and email lists, corporate web pages, network maps or other information (for example, server names), and discarded paperwork.

## CHAPTER 6

### 1. Which of the following statements best describes the employee lifecycle?

**A.** The employee lifecycle spans recruitment to career development.

**B.** The employee lifecycle spans onboarding to orientation.

**C.** The employee lifecycle spans user provision to termination.

**D.** The employee lifecycle spans recruitment to termination.

### 2. At which of the following phases of the hiring process should personnel security practices begin?

**A.** Interview

**B.** Offer

**C.** Recruitment

**D.** Orientation

### 3. A published job description for a web designer should not include which of the following?

**A.** Job title

**B.** Salary range

**C.** Specifics about the web development tool the company is using

**D.** Company location

### 4. Data submitted by potential candidates must be

. **A.** protected as required by applicable law and organizational policy

**B.** not protected unless the candidate is hired

**C.** stored only in paper form

**D.** publicly accessible

### 5. During the course of an interview, a job candidate should be given a tour of which of the following locations?

**A.** The entire facility

**B.** Public areas only (unless otherwise authorized)

**C.** The server room

**D.** The wiring closet

### 6. Which of the following facts is an interviewer permitted to reveal to a job candidate?

**A.** A detailed client list

**B.** The home phone numbers of senior management

**C.** The organization's security weaknesses

**D.** The duties and responsibilities of the position

### 7. Which of the following statements best describes the reason for conducting background checks?

**A.** To verify the truthfulness, reliability, and trustworthiness of the applicant

**B.** To find out if the applicant ever got in trouble in high school

**C.** To find out if the applicant has a significant other

**D.** To verify the applicant's hobbies, number of children, and type of house

### 8. Which of the following statements best describes the background check criteria?

**A.** Criteria should be the same for all prospective employees.

**B.** Criteria should differ according to gender or ethnicity.

**C.** Criteria should be specific to the job for which an applicant is applying.

**D.** None of the above.

**9. Social media profiles often include gender, race, and religious affiliation. Which of the following statements best describes how this information should be used in the hiring process?**

**A.** Gender, race, and religious affiliation can legally be used in making hiring decisions.

**B.** Gender, race, and religious affiliation cannot legally be used in making hiring decisions.

**C.** Gender, race, and religious affiliation are useful in making hiring decisions.

**D.** Gender, race, and religious affiliation listed in social media profiles should not be relied upon as they may be false.

**10. Under the Fair Credit Reporting Act (FCRA), which of the following statements is true?**

**A.** Employers cannot request a copy of an employee's credit report under any circumstances.

**B.** Em plo yers m ust get the candidate 's co nsent to request a credit report.

**C.** Employers cannot use credit information to deny a job.

**D.** Employers are required to conduct credit checks on all applicants.

**11. Candidate and employee NPPI must be protected. NPPI does not include which of the following?**

**A.** Social security number

**B.** Credit card number

**C.** Published telephone number

**D.** Driver's license number

**12. Which of the following statements best describes the purpose of completing Department of Homeland**

Security/U.S. Citizenship and Immigration Services Form I-9 and providing supporting documentation?

**A.** The purpose is to establish identity and employment authorization.

**B.** The purpose is to determine tax identification and withholding.

**C.** The purpose is to document educational achievements.

**D.** The purpose is to verify criminal records.

**13. The permissions and access rights a user is granted should match their role and responsibilities. Who is responsible for defining to whom access should be granted?**

**A.** The information user

**B.** The information owner

**C.** The information custodian

**D.** The information author

**14. Network administrators and help desk personnel often have elevated privileges. They are examples of which of the following roles?**

**A.** The information owners

**B.** The information custodians

**C.** The information authors

**D.** The information sellers

**15. Which of the following statements is not true of confidentiality agreements?**

**A.** Confidentiality/non-disclosure agreements are legal protection against unauthorized use of information.

**B.** Confidentiality/non-disclosure agreements are generally considered a condition of work.

**C.** Confidentiality/non-disclosure agreements are legally binding contracts.

**D.** Confidentiality agreements should only be required of top-level executives.

**16. Which of the following elements would you expect to find in an acceptable use agreement?**

**A.** Handling standards

**B.** A lunch and break schedule

**C.** A job description

**D.** An evacuation plan

**17. Which of the following statements best describes when acceptable use agreements should be reviewed, updated, and distributed?**

**A.** Acceptable use agreements should be reviewed, updated, and distributed only when there are organizational changes.

**B.** Acceptable use agreements should be reviewed, updated, and distributed annually.

**C.** Acceptable use agreements should be reviewed, updated, and distributed only during the merger and acquisition due diligence phase.

**D.** Acceptable use agreements should be reviewed, updated, and distributed at the discretion of senior management.

**18. Which of the following terms best describes the SETA acronym?**

**A.** Security Education Teaches Awareness
**B.** Security Education Training Awareness
**C.** Security Education Teaches Acceptance
**D.** Security Education Training Acceptance

**19. Posters are placed throughout the workplace reminding users to log off when leaving their workstations unattended. This is an example of which of the following programs?**

**A.** A security education program

**B.** A security training program

**C.** A security awareness program

**D.** None of the above

**20. A network engineer attends a one-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?**

**A.** A security education program

**B.** A security training program

**C.** A security awareness program

**D.** None of the above

**21. The Board of Directors has a presentation on the latest trends in security management. This is an example of which of the following programs?**

**A.** A security education program

**B.** A security training program

**C.** A security awareness program

**D.** None of the above

**22. Companies have the legal right to perform which of the following activities?**

**A.** Monitor user Internet access from the workplace

**B.** Place cameras in locker rooms where employees change clothes

**C.** Conduct a search of an employee's home

**D.** None of the above

**23. Sanctions for policy violations should be included in which of the following documents?**

**A.** The employee handbook

**B.** A confidentiality/non-disclosure agreement

**C.** An acceptable use agreement

**D.** All of the above

**24. Studies often cite_____ as the weakest link in information security.**

**A.** policies

**B.** people

**C.** technology

**D.** regulations

**25. Which of the following terms best describes the impact of security education?**

**A.** Long-term

**B.** Short-term

**C.** Intermediate

**D.** Forever

**26. Which of the following privacy regulations stipulates that schools must have written permission in order to release any information from a student's education record?**

**A.** Sarbanes-Oxley Act (SOX)

**B.** HIPAA

**C.** Gramm-Leach-Bliley Act (GLBA)

**D.** FERPA

**27. Which of the following regulations specifically stipulates that employees should be trained on password management?**

**A.** FERPA
**B.** HIPAA
**C.** DPPA **D.**
FISMA

**28. Best practices dictate that employment applications should not ask prospective employees to provide which of the following information?**

**A.** Last grade completed

**B.** Current address

**C.** Social security number

**D.** Email address

**29. After a new employee's retention period has expired, completed paper employment applications should be_____.**

**A.** cross-cut shredded

**B.** recycled

**C.** put in the trash

**D.** stored indefinitely

**30. Intruders might find job posting information useful for which of the following attacks?**

**A.** A distributed denial of service attack (DDoS) attack

**B.** A social engineering attack

**C.** A man-in-the-middle attack

**D.** An SQL injection attack

A. Discussion Question 1

Why does the U.S. Government require both a level of security clearance (at least equal to the classification of the information) and an appropriate “need to know” the information before information is released to an individual?
Answer: Student answers will vary. Merely having a certain level of security clearance does not authorize an individual to access all information so classified. Information must be closely held to be protected, so requiring both

an equivalent security clearance and an authorized “need to know” restricts access appropriately. Background checks are more stringent for higher security clearance levels.

B. Discussion Question 2

What should be included in an acceptable use agreement?

Answer: Student answers will vary, but at a minimum the following components should be included in an acceptable use agreement: introduction, data classifications, applicable policy statement, handling standards, contacts, violations section, and acknowledgment

## CHAPTER 7

**1. Which of the following groups should be assigned responsibility for physical and environmental security?**

A. Facilities management
B. Information security management
C. Building security
D. A team of experts including facilities, information security, and building security

**2. Physical and environmental security control decisions should be driven by a(n) _____.**

A. educated guess
B. industry survey
C. risk assessment
D. risk management

**3. Which of the following terms best describes CPTED?**

A. Crime prevention through environmental design
B. Crime prevention through environmental designation
C. Criminal prevention through energy distribution
D. Criminal prosecution through environmental design

**4. Which of the following is a CPTED strategy?**

A. Natural surveillance.
B. Territorial reinforcement.
C. Natural access control.
D. All of the above are CPTED strategies.

**5. Which of the following models is known as the construct that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities?**

A. Layered defense model
B. Perimeter defense model
C. Physical defense model

D. Security defense model

**6. Which of the following is a location-based threat?**

A. Flight path
B. Volcano
C. Political stability
D. All of the above

**7. Best practices dictate that data centers should be _____.**

A. well marked
B. located in urban areas
C. inconspicuous and unremarkable
D. built on one level

**8. Which of the following would be considered a "detection" control?**

A. Lighting
B. Berms
C. Motion sensors
D. Bollards

**9. Badging or an equivalent system at a secure facility should be used to identify _____.**

A. everyone who enters the building
B. employees
C. vendors
D. visitors

**10. Which of the following statements best describes the concept of shoulder surfing?**

A. Shoulder surfing is the use of a keylogger to capture data entry.
B. Shoulder surfing is the act of looking over someone's shoulder to see what is on a computer screen.
C. Shoulder surfing is the act of positioning one's shoulders to prevent fatigue.
D. None of the above.

**11. The term BYOD is used to refer to devices owned by Company employees.**

**12. Which of the following statements is not true about reducing power consumption?**

A. Reducing power consumption saves energy.
B. Reducing power consumption saves money.
C. Reducing power consumption creates less pollution.
D. Reducing power consumption increases CO2 emissions.

**13. The United States government Energy Star certification indicates which of the following?**

A. The product is a good value.
B. The product was made in the United States.
C. The product has met energy efficiency standards.
D. The product is used by the government.

**14. Which of the following actions contribute to reducing daily power consumption?**

A. Turning off computers when not in use
B. Turning off monitors when not in use
C. Turning off printers when not in use
D. All of the above

**15. Which of the following terms best describes a prolonged increase in voltage?**

A. Power spike
B. Power surge
C. Power hit
D. Power fault

**16. Common causes of voltage variations include _____.**

A. lightning, storm damage, and electric demand
B. using a power conditioner
C. turning on and off computers
D. using an uninterruptable power supply

**17. Adhering to building and construction codes, using flame-retardant materials, and properly grounding equipment are examples of which of the following controls?**

A. Fire detection controls
B. Fire containment controls
C. Fire prevention controls
D. Fire suppression controls

**18. A Class C fire indicates the presence of which of the following items?**

A. Electrical equipment
B. Flammable liquids
C. Combustible materials
D. Fire extinguishers

**19. Classified data can reside on which of the following items?**

A. Smartphones
B. Cameras
C. Scanners
D. All of the above

**20. Which of the following data types includes details about a file or document?**

A. Apparent data
B. Hidden data
C. Metadata
D. Cache data

**21. URL history, search history, form history, and download history are stored by the device_____.**

A. operating system
B. browser
C. BIOS
D. None of the above

**22. Which of the following statements about formatting a drive is not true?**

A. Formatting a drive creates a bootable partition.
B. Formatting a drive overwrites data.
C. Formatting a drive fixes bad sectors.
D. Formatting a drive permanently deletes files.

**23. Disk wiping works reliably on which of the following media?**

A. USB thumb drives
B. Conventional hard drives
C. SD cards
D. Solid-state hard drive

**24. The United States Department of Defense (DoD) medium security disk-wiping standard specifies which of the following actions?**

A. Three iterations to completely overwrite a hard drive six times
B. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive
C. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive, plus a read-verify process
D. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive, plus a magnetic swipe

**25. Which of the following terms best describes the process of using a realigning and resetting particle to erase data?**

A. Deleting
B. Degaussing
C. Destroying
D. Debunking

**26. Which of the following terms best describes the shredding technique that reduces material to fine, confetti-like pieces?**

A. Cross-cut
B. Strip-cut
C. Security-cut
D. Camel-cut

**27. A certificate of destruction is evidence that _____.**

A. the media has be destroyed by a third party
B. the media has been destroyed internally
C. the media has been destroyed by its owner
D. the media has been destroyed

**28. Which of the following amounts represents the average per-record cost of a data breach in the United States?**

A. $1
B. $18
C. $188
D. $1,188

**29. Which of the following controls includes remote lock, remote wipe, and remote location?**

A. Work-at-home controls
B. Mobile device antitheft controls
C. GPS controls
D. Find-my-car controls

**30. In an environmental disaster, priority should be given to _____.**

A. protecting human life
B. saving key documents
C. data center continuity
D. first responder safety

## CHAPTER 8

**1. Which of the following is true about documenting SOPs?**

A. It promotes business continuity.
B. The documentation should be approved before publication and distribution.
C. Both A and B.
D. Neither A nor B.

**2. Which two factors influence the type of SOP used?**

A. Cost and complexity
B. Number of decisions and number of steps
C. Language and age of the workforce
D. Number of warnings and number of exceptions

**3. Which of the following formats should be used when an SOP includes multiple decision making steps?**

A. Simple
B. Hierarchical
C. Graphic
D. Flowchart

**4. The change control process starts with which of the following?**

A. Budget
B. RFC submission
C. Vendor solicitation
D. Supervisor authorization

**5. What is the most important message to share with the workforce about "change"?**

A. The reason for the change
B. The cost of the change
C. Who approved the change
D. Management's opinion of the change

**6. Which of the following statements best describes the action that should occur prior to implementing a change that has the potential to impact business processing?**

A. The impact should be communicated.
B. The change should be thoroughly tested.
C. A rollback or recovery plan should be developed.
D. All of the above.

**7. Which of the following is not a part of a malware defense-in-depth strategy?**

A. Security awareness
B. Prevention controls
C. Reverse engineering
D. Detection controls

**8. Which of the following statements best describes a security patch?**

A. A security patch is designed to fix a security vulnerability.
B. A security patch is designed to add security features.
C. A security patch is designed to add security warnings.
D. A security patch is designed to fix code functionality.

**9. Which of the following is a component of an AV application?**

A. Definition files
B. Handler
C. Patch
D. Virus

**10. Which of the following statements best describes the testing of security patches?**

A. Security patches should never be tested because waiting to deploy is dangerous.
B. Security patches should be tested prior to deployment, if possible.
C. Security patches should be tested one month after deployment.
D. Security patches should never be tested because they are tested by the vendor.

**11. Which of the following operating systems are vulnerable to malware?**

A. Apple OS only.
B. Android OS only.
C. Microsoft Windows OS only.
D. Malware is operating system agnostic.

**12. Which of the following terms best describes malware that is specifically designed to hide in the background and gather info over an extended period of time?**

A. Trojan
B. APT
C. Ransomware
D. Zero-day exploit

**13. A _____ can spread from one computer to another without requiring a host file**

to infect.
A. virus
B. Trojan
C. worm
D. rootkit

**14. _____ wait for remote instructions and are often used in DDoS attacks.**

A. APTs
B. Bots
C. DATs
D. None of the above

**15. Which of the following statements best describes a blended threat?**

A. A blended threat is designed to be difficult to detect.
B. A blended threat is designed to be difficult to contain.
C. A blended threat is designed to be difficult to eradicate.
D. All of the above.

**16. Which of the following statements best describes data replication?**

A. Replicated data needs to be restored from tape.
B. Only administrators have access to replicated data.
C. Replicated data is generally available in near or real time.
D. Replication is expensive.

**17. Organizations that are considering storing legally protected data in "the cloud" should_____.**

A. contractually obligate the service provider to protect the data
B. assume that the appropriate security controls are in place
C. give their customers an option as to where data is stored
D. only use cloud storage for data replication

**18. Which of the following actions best describes the task that should be completed once backup media such as tape is no longer in rotation?**

A. It should be erased and reused.
B. It should be recycled.
C. It should physically be destroyed.
D. It should be labeled as old and put in a supply closet.

**19. Which of the following terms best describes the Department of Defense project to develop a set of communications protocols to transparently connect computing resources in various geographical locations?**

A. DoDNet
B. ARPANET
C. EDUNET
D. USANET

**20. Which of the following terms best describes the message transport protocol used for sending email messages?**

A. SMTP
B. SMNP
C. POP3
D. MIME

**21. In its native form, email is transmitted in _____.**

A. cipher text
B. clear text
C. hypertext
D. meta text

**22. Which of the following statements best describes how users should be trained to manage their email?**

A. Users should click embedded email hyperlinks.
B. Users should open unexpected email attachments.
C. Users should access personal email from the office.
D. Users should delete unsolicited or unrecognized emails.

**23. Open email relay service can be used to do which of the following?**

A. Secure messages
B. Ensure message delivery
C. Misappropriate resources
D. Create blacklists

**24. Which of the following statements best describes a system log?**

A. A system log is a record of allowed and denied events.
B. A system log is a record of problem events only.
C. A system log is a record of user productivity.
D. A system log is a record of system codes.

**25. Which of the following statements best describes trend analysis?**

A. Trend analysis is used to tie individual log entries together based on related information.
B. Trend analysis is used to examine activity based on patterns.
C. Trend analysis is used to compare log data to known bad activity.
D. Trend analysis is used to identify activity over time.

**26. Which of the following statements best describes authentication server logs?**

A. Authentication server logs capture user, group, and administrative activity.
B. Authentication server logs capture bad HTML code.
C. Authentication server logs capture SQL injection attempts.
D. Authentication server logs capture web traffic.

**27. Which of the following terms best describes the process of assessing a service provider's reputation, financial statements, internal controls, and insurance coverage?**

A. Downstream investigation
B. Standard of care
C. Due diligence
D. Outsource audit

**28. SSAE16 audits must be attested to by a _____.**

A. Certified Information System Auditor (CISA)
B. Certified Public Accountant (CPA)
C. Certified Information Systems Manager (CISM)
D. Certified Information System Security Professional (CISSP)

**29. Service providers should be required to provide notification of which of the following types of incidents?**

A. Confirmed incidents
B. Confirmed incidents by known criminals
C. Confirmed incidents that have been reported to law enforcement
D. Confirmed and suspected incidents

**30. Which of the following reasons best describes why independent security testing is recommended?**

A. Independent security testing is recommended because of the objectivity of the tester.
B. Independent security testing is recommended because of the expertise of the tester.
C. Independent security testing is recommended because of the experience of the tester.
D. All of the above.

## CHAPTER 9

**1. Which of the following terms best describes access controls that are security features that govern how users and processes interact?**

A. Objects
B. Resources
C. Processes
D. All of the above

**2. Which of the following terms best describes the process of verifying the identity of a subject?**

A. Accountability
B. Authorization
C. Access model
D. Authentication

**3. Which of the following terms best describes the process of assigning authenticated subjects permission to carry out a specific operation?**

A. Accountability
B. Authorization
C. Access model
D. Authentication

**4. Which of the following terms best describes the active entity that requests access to an object or data?**

A. Subject
B. Object
C. Resource
D. Factor

**5. Which of the following security principles is best described as giving users the minimum access required to do their jobs?**

A. Least access
B. Less protocol
C. Least privilege
D. Least process

**6. Which of the following security principles is best described as prohibiting access to information not required for one's work?**

A. Access need security principle
B. Need-to-monitor security principle
C. Need-to-know security principle
D. Required information process security principle

**7. Which type of access is allowed by the security principle of default deny?**

A. Basic access is allowed.
B. Access that is not explicitly forbidden is permitted.
C. Access that is not explicitly permitted is forbidden.
D. None of the above.

**8. Which of the following statements best describes the access rights of a user who has been granted Top Secret clearance at an organization that is using the mandatory access control (MAC) model?**

A. The user can automatically access all Top Secret information.
B. The user can access only Top Secret information.
C. The user can access specific categories of Top Secret information.
D. The user can only access information up to the Top Secret level.

**9. Who is responsible for DAC decisions?**

A. Data owners
B. Data administrators
C. Data custodians
D. Data users

**10. Which of the following terms best describes the control that is used when the SOP for user provisioning requires the actions of two systems administrators—one who can create and delete accounts and the other who assigns access permissions?**

A. Least privilege
B. Segregation of duties
C. Need to know
D. Default deny all

**11. Which of the following types of network, operating system, or application access controls is user agnostic and relies on specific criteria such as source IP address, time of day, and geographic location?**

A. Mandatory
B. Role-based
C. Rule-based
D. Discretionary

**12. Which of the following is not considered an authentication factor?**

A. Knowledge
B. Inheritance
C. Possession
D. Biometric

**13. Which of the following terms best describes authentication that requires two or more factors?**

A. Dual control
B. Multifactor
C. Multiple-factor
D. Multilayer

**14. Which of the following statements best describes reasons to change a password?**

A. Passwords should be changed in order to increase the complexity of the password.

B. Passwords should be changed when there is a suspicion that the password has been compromised.
C. Passwords should be changed in order to create a unique password after a user initially logs on to a system using a default or basic password.
D. All of the above.

**15. Which of the following terms best describes a type of password that is a form of knowledge based authentication that requires a user to answer a question based on something familiar to them?**

A. Categorical
B. Cognitive
C. Complex
D. Credential

**16. Which of the following types of authentication requires two distinct and separate channels to authenticate?**

A. In-band authentication
B. Mobile authentication
C. Out-of-band authentication
D. Out-of-wallet authentication

**17. Which of the following terms best describes the internal network that is accessible to authorized users?**

A. Trusted network
B. DMZ
C. The Internet
D. Semi-trusted network

**18. Rules related to source and destination IP address, port, and protocol are used by a(n) _____to determine access.**

A. firewall
B. IPS
C. IDS
D. VPN

**19. Which of the following statements is true of an intrusion detection system (IDS)?**

A. An IDS can disable a connection.
B. An IDS can respond to identified threats.
C. An IDS uses signature-based detection and/or anomaly-based detection techniques.
D. An IDS can delete malicious content.

**20. Which of the following terms best describes a VPN?**

A. A VPN provides a secure tunnel for transmitting data through a untrusted network.
B. A VPN is a cost-effective solution for securing remote access.
C. Both A and B.
D. Neither A nor B.

**21. Which of the following statements best describes mutual authentication?**

A. Mutual authentication is used to auto-save passwords.
B. Mutual authentication is used to verify the legitimacy of the server before providing access credentials.
C. Mutual authentication is used to eliminate the need for multifactor authentication.
D. Mutual authentication is used to authorize access.

**22. Network access controls (NAC) systems are used to “check” a remote device for which of the following?**

A. Operating system version
B. Patch status
C. Wireless configuration

D. All of the above

**23. Which of the following statements best describes teleworking?**

A. An employee who talks on the telephone
B. An employee who uses his cell phone to access the Internet
C. An employee who works from a remote location on a scheduled basis
D. An employee who uses a mobile device to check email

**24. Which of the following statements is not true of monitoring access?**

A. Monitoring access mitigates the risks associated with misuse of privileges.
B. Monitoring access is illegal.
C. Monitoring access can identify user issues.
D. Monitoring access can provide oversight of administrative activities.

**25. The objective of user access controls is to ensure that authorized users are able to access information and resources and that _____.**

A. authorized users are able to work uninterrupted
B. unauthorized users are prevented from accessing information resources
C. authorized users can access the Internet
D. unauthorized activity is logged

**26. Which of the following statements best describes whitelists?**

A. Whitelists are IP addresses or Internet domain names of sites that are allowed.
B. Whitelists are IP addresses or Internet domain names of frequently used sites.
C. Whitelists are IP addresses or Internet domain names of known malware sites.
D. Whitelists are IP addresses or Internet domain names of sites that should be blocked.

**27. Which of the following passwords is the strongest?**

A. PetNameBob
B. PetN@meB0b
C. 8579377
D. H8djwk!!j4

**28. Which type of information about user access should be logged and analyzed?**

A. Successful access
B. Failed access
C. Privileged operations
D. All of the above

**29. Which of the following types of authentication requires a user to enter a password and answer a question?**

A. Single-factor authentication
B. Multifactor authentication
C. Multi-layer authentication
D. Out-of-band authentication

**30. Access logs should be reviewed _____.**

A. daily
B. annually
C. when there is a suspicion of malicious activity
D. only by law enforcement personnel

## CHAPTER 10

**1. When is the best time to think about security when building an application?**

A. Build the application first and then add a layer of security.
B. At inception.
C. Start the application development phase, and when you reach the halfway point, you have enough of a basis to look at to decide where and how to set up the security

elements.
D. No security needs to be developed inside of the code itself. It will be handled at the operating system level.

**2. Which of the following statements best describes the purpose of the systems development lifecycle (SDLC)?**

A. The purpose of the SDLC is to provide a framework for system development efforts.
B. The purpose of the SDLC is to provide a standardized process for system development efforts.
C. The purpose of the SDLC is to assign responsibility.
D. All of the above.

**3. In which phase of the SDLC is the need for a system expressed and the purpose of the system documented?**

A. The initiation phase
B. The implementation phase
C. The operational phase
D. The disposal phase

**4. During which phase of the SDLC is the system accepted?**

A. The initiation phase
B. The implementation phase
C. The operational phase
D. The disposal phase

**5. Which of the following statements is true?**

A. Retrofitting security controls to an application system after implementation is normal; this is when security controls should be added.
B. Retrofitting security controls to an application system after implementation is sometimes necessary based on testing and assessment results.
C. Retrofitting security controls to an application system after implementation is always a bad idea.
D. Retrofitting security controls to an application system after implementation is not necessary because security is handled at the operating system level.

**6. Which phase of software release indicates that the software is feature complete?**

A. Alpha
B. Beta
C. Release candidate
D. General availability

**7. Which phase of software release is the initial release of software for testing?**

A. Alpha
B. Beta
C. Release candidate
D. General availability

**8. Which of the following statements best describes the difference between a security patch and an update?**

A. Patches provide enhancements; updates fix security vulnerabilities.
B. Patches should be tested; updates do not need to be tested.
C. Patches fix security vulnerabilities; updates add features and functionality.
D. Patches cost money; updates are free.

**9. The purpose of a rollback strategy is to _____.**

A. make backing up easier
B. return to a previous stable state in case problems occur
C. add functionality
D. protect data

**10. Which of the following statements is true?**

A. A test environment should always be the exact same as the live environment.
B. A test environment should be as cheap as possible no matter what.
C. A test environment should be as close to the live environment as possible.
D. A test environment should include live data for true emulation of the real-world setup.

**11. Which of the following statements best describes when dummy data should be used?**

A. Dummy data should be used in the production environment.
B. Dummy data should be used in the testing environment.
C. Dummy data should be used in both test and production environments.
D. Dummy data should not be used in either test or production environments.

**12. Which of the following terms best describes the process of removing information that would identify the source or subject?**

A. Detoxification
B. Dumbing down
C. Development
D. De-identification

**13. Which of the following terms best describes the open framework designed to help organizations implement a strategy for secure software development?**

A. OWASP
B. SAMM
C. NIST
D. ISO

**14. Which of the following statements best describes an injection attack?**

A. An injection attack occurs when untrusted data is sent to an interpreter as part of a command.
B. An injection attack occurs when trusted data is sent to an interpreter as part of a query.
C. An injection attack occurs when untrusted email is sent to a known third party.
D. An injection attack occurs when untrusted data is encapsulated.

**15. Input validation is the process of _____.**

A. masking data
B. verifying data syntax
C. hashing input
D. trusting data

**16. Which of the following types of data changes as updates become available?**

A. Moving data
B. Mobile data
C. Dynamic data
D. Delta data

**17. The act of limiting the characters that can be entered in a web form is known as _____.**

A. output validation
B. input validation
C. output testing
D. input testing

**18. Which statement best describes a distinguishing feature of cipher text?**

A. Cipher text is unreadable by a human.
B. Cipher text is unreadable by a machine.
C. Both A and B.
D. Neither A nor B.

**19. Which term best describes the process of transforming plain text to cipher text?**

A. Decryption
B. Hashing
C. Validating
D. Encryption

**20. Which of the following statements is true?**

A. Digital signatures guarantee confidentiality only.
B. Digital signatures guarantee integrity only.
C. Digital signatures guarantee integrity and nonrepudiation.
D. Digital signatures guarantee nonrepudiation only.

**21. Hashing is used to ensure message integrity by _____.**

A. comparing hash values
B. encrypting data
C. encapsulating data
D. comparing algorithms and keys

**22. When unauthorized data modification occurs, which of the following tenets of security is directly being threatened?**

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

**23. Which of the following statements about encryption is true?**

A. All encryption methods are equal: Just choose one and implement it.
B. The security of the encryption relies on the key.
C. Encryption is not needed for internal applications.
D. Encryption guarantees integrity and availability, but not confidentiality.

**24. Which of the following statements about a hash function is true?**

A. A hash function takes a variable-length input and turns it into a fixed-length output.
B. A hash function takes a variable-length input and turns it into a variable-length output.
C. A hash function takes a fixed-length input and turns it into a fixed-length output.
D. A hash function takes a fixed-length input and turns it into a variable-length output.

**25. Which of the following values represents the number of available values in a 256-bit keyspace?**

A. $2 \times 2256$
B. $2 \times 256$
C. 2562
D. 2256

**26. Which of the following statements is not true about a symmetric key algorithm?**

A. Only one key is used.
B. It is computationally efficient.
C. The key must be publicly known.
D. 3DES is widely used.

**27. The contents of a _____ include the issuer, subject, valid dates, and public key.**

A. digital document
B. digital identity
C. digital thumbprint
D. digital certificate

**28. Two different but mathematically related keys are referred to as _____.**

A. public and private keys
B. secret keys
C. shared keys

D. symmetric keys

**29. In cryptography, which of the following is not publicly available?**

A. Algorithm
B. Public key
C. Digital certificate
D. Symmetric key

**30. A hash value that has been encrypted with the sender's private key is known as a _____.**

A. message digest
B. digital signature
C. digital certificate
D. cipher text

## CHAPTER 11

**1. Which of the following statements best defines incident management?**

A. Incident management is risk minimization.
B. Incident management is a consistent approach to responding to and resolving issues.
C. Incident management is problem resolution.
D. Incident management is forensic containment.

**2. Which of the following statements is true of security-related incidents?**

A. Over time, security-related incidents have become less prevalent and less damaging.
B. Over time, security-related incidents have become more prevalent and more disruptive.
C. Over time, security-related incidents have become less prevalent and more damaging.
D. Over time, security-related incidents have become more numerous and less disruptive.

**3. Minimizing the number of incidents is a function of which of the following?**

A. Incident response testing
B. Forensic analysis
C. Risk management
D. Security investments

**4. An information security incident can _____.**

A. compromise business security
B. disrupt operations
C. impact customer trust
D. All of the above

**5. Which of the following statements is true when an information security–related incident occurs at a business partner or vendor who hosts or processes legally protected data on behalf of an organization?**

A. The organization does not need to do anything.
B. The organization must be notified and respond accordingly.
C. The organization is not responsible.
D. The organization must report the incident to local law enforcement.

**6. Which of the following attack types best describes a targeted attack that successfully obstructs functionality?**

A. Spam attack
B. Malware attack
C. DDoS attack
D. Killer attack

**7. A celebrity is admitted to the hospital. If an employee accesses the celebrity's patient record just out of curiosity, the action is referred to as _____.**

A. inappropriate usage
B. unauthorized access

C. unacceptable behavior
D. undue care

**8. Employees who report incidents should be _____.**

A. prepared to assign a severity level
B. praised for their actions
C. provided compensation
D. None of the above

**9. Which of the following statements is true of an incident response plan?**

A. An incident response plan should be updated and authorized annually.
B. An incident response plan should be documented.
C. An incident response plan should be stress tested.
D. All of the above

**10. Which of the following terms best describes a signal or warning that an incident may occur in the future?**

A. A sign
B. A precursor
C. An indicator
D. Forensic evidence

**11. Which of the following terms best describes the process of taking steps to prevent the incident from spreading?**

A. Detection
B. Containment
C. Eradication
D. Recovery

**12. Which of the following terms best describes the addressing of the vulnerabilities related to the exploit or compromise and restoring normal operations?**

A. Detection
B. Containment
C. Testing
D. Recovery

**13. Which of the following terms best describes the eliminating of the components of the incident?**

A. Investigation
B. Containment
C. Eradication
D. Recovery

**14. Which of the following terms best describes the substantive or corroborating evidence that an incident may have occurred or may be occurring now?**

A. Indicator of compromise
B. Forensic proof
C. Heresy
D. Diligence

**15. Which of the following is not generally an incident response team responsibility?**

A. Incident impact analysis
B. Incident communications
C. Incident plan auditing
D. Incident management

**16. Incident response activity logs should not include which of the following?**

A. Date
B. Time

C. Decisions made
D. Cost of the activity

**17. The decision to contact law enforcement should be made _____.**

A. early in the incident lifecycle
B. once an incident has been verified
C. after evidence has been collected
D. only if there is a loss of funds

**18. Which of the following agencies' investigative responsibilities include financial fraud, money laundering, and identity theft?**

A. FBI
B. Department of Homeland Security
C. Secret Service
D. State Police

**19. Documentation of the transfer of evidence is known as a _____.**

A. chain of evidence
B. chain of custody
C. chain of command
D. chain of investigation

**20. Data breach notification laws pertain to which of the following?**

A. Intellectual property
B. Patents
C. PII
D. Products

**21. Federal breach notification laws apply to _____.**

A. specific sectors such as financial and healthcare
B. all United States citizens
C. any disclosure of a Social Security number
D. None of the above

**22. HIPAA/HITECH requires _____ within 60 days of the discovery of a breach.**

A. notification be sent to affected parties
B. notification be sent to law enforcement
C. notification be sent to Department of Health and Human Services
D. notification be sent to all employees

**23. With the exception of the _____, all federal agencies are required to act in accordance with OMB M-07-16: "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" guidance.**

A. Department of Health and Human Services
B. Federal Reserve
C. Internal Revenue Service
D. Veterans Administration

**24. Which of the following statements is true of state breach notification laws?**

A. Notification requirements are the same in every state.
B. State laws exist because there is no comparable federal law.
C. Every state has a state breach notification law.
D. The laws only apply to verified breaches.

**25. Which of the following states was the first state to enact a security breach notification law?**

A. Massachusetts
B. Puerto Rico

C. California
D. Alabama

**26. Which of the following statements is true concerning the Texas security breach notification law?**

A. The Texas security breach notification law includes requirements that in-state businesses provide notice to residents of all states.
B. The Texas security breach notification law includes requirements that in-state businesses only provide notice to residents of Texas.
C. The Texas security breach notification law includes requirements that in-state businesses are exempt from notification requirements.
D. The Texas security breach notification law includes requirements that in-state businesses provide notice internationally.

**27. Consumers are most concerned about compromise of their _____.**

A. password/PIN and SSN
B. email address
C. checking account number
D. address and date of birth

**28. Which of the following statements is true?**

A. Consumers want to be notified of a data breach and they overwhelmingly expect to be compensated.
B. Consumers want to be notified of a data breach and they overwhelmingly expect to be provided as much detail as possible.
C. Consumers want to be notified of a data breach and they overwhelmingly expect to be told when the criminal is apprehended.
D. Consumers want to be notified of a data breach and they overwhelmingly expect to be interviewed by investigators.

**29. Incident response plans and procedures should be tested _____.**

A. during development
B. upon publication
C. on an ongoing basis
D. only when there are changes

**30. The Board of Directors (or equivalent body) is responsible for _____.**

A. the cost of notification
B. contacting regulators
C. managing response efforts
D. authorizing incident response policies

## CHAPTER 12

**1. Which of the following terms best describes the primary objective of business continuity?**

A. Assurance
B. Availability
C. Accounting
D. Authentication

**2. Which of the following statements best describes a disaster?**

A. A disaster is a planned activity.
B. A disaster is an isolated incident.
C. A disaster is a significant disruption of normal business functions.
D. A disaster is a change in management structure.

**3. Flood, fire, and wind are examples of which type of threat?**

A. Malicious act

B. Environmental
C. Logistical
D. Technical

**4. Which of the following terms best describes the process of identifying viable threats and likelihood of occurrence?**

A. Risk assessment
B. Threat assessment
C. Likelihood assessment
D. Impact assessment

**5. Which of the following terms best describes the process of evaluating the sufficiency of controls?**

A. Risk assessment
B. Threat assessment
C. Likelihood assessment
D. Impact assessment

**6. Which of the following statements best describes the outcome of a BIA?**

A. A BIA generates RTOs.
B. A BIA produces an organizational agreement on essential processes and services.
C. A BIA identifies the gap between current and desired recovery capabilities.
D. All of the above

**7. An acceptable length of time a business function or process can be unavailable is known as_____.**

A. maximum unavailability (MU)
B. total acceptable time (TAT)
C. maximum tolerable downtime (MTD)
D. recovery time objective (RTO)

**8. The recovery point objective (RPO) represents _____.**

A. acceptable data loss
B. acceptable processing time loss
C. acceptable downtime
D. None of the above

**9. Recovery time objectives relate to which of the following?**

A. Business services
B. Data restoration
C. Information systems
D. None of the above

**10. Which of the following plans are included in a BCP?**

A. Resumption plans
B. Response plans
C. Contingency plans
D. All of the above

**11. Legal and regulatory accountability for an organization's preparedness is assigned to_____.**

A. the BCT
B. regulators
C. the Board of Directors or organizational equivalent
D. service providers

**12. The authority to declare an emergency and activate the plan is owned by _____.**

A. the BCT
B. executive management
C. the Board of Directors or organizational equivalent
D. service providers

**13. Which of the following plans include evacuation and in-shelter procedures?**

A. The fire drill plan
B. The occupant emergency plan
C. The business contingency plan
D. A FEMA directive

**14. Which of the following entities is responsible for the ongoing command of operations in the event of a disaster?**

A. First responders
B. The BCT
C. The Chairman of the Board
D. The Information Security Officer

**15. The designated location for the BCT operations is referred to as the _____.**

A. BCT office
B. hot site
C. command and control center
D. conference room

**16. Contingency and recovery procedures should include a level of detail appropriate for which of the following entities?**

A. New hires or temporary employees
B. Cross-trained personnel or service providers familiar with the organization
C. Auditors
D. Examiners

**17. The BCT is tasked with all of the following activities except _____.**

A. testing the plan
B. managing the plan
C. reporting to the command and control center
D. auditing the plan

**18. Which type of alternate data-processing facility is fully equipped with all resources required to maintain operations?**

A. Hot site
B. Warm site
C. Cold site
D. Off site

**19. Which type of alternate data-processing facility has power and HVAC but not equipment?**

A. Hot site
B. Warm site
C. Cold site
D. Off site

**20. Which of the following statements is true of the IT department's responsibilities?**

A. The IT department is responsible for restocking supplies.
B. The IT department is responsible for recovery and resumption related to the information system and supporting infrastructure.
C. The IT department is responsible for rebuilding facilities.
D. The IT department is responsible for the release of updates to the press.

**21. Which of the following statements best describes the primary objective of an organization's contingency plan?**

A. The primary objective of an organization's contingency plan is for the organization to become fully operational.
B. The primary objective of an organization's contingency plan is for the organization to recover systems.
C. The primary objective of an organization's contingency plan is for the organization to notify authorities.
D. The primary objective of an organization's contingency plan is for the organization to continue to provide services.

**22. Which of the following entities is responsible for developing, validating, and training personnel on operational contingency plans?**

A. Business process owners
B. BCT
C. Business managers
D. Business associates

**23. Validation and deactivation activities are part of _____.**

A. response
B. contingency
C. recovery
D. resumption

**24. Which of the following should not be included in service provider agreements?**

A. Response time
B. Replacement equipment
C. Priority of service
D. Emergency passcodes

**25. Plan maintenance includes which of the following?**

A. Testing and auditing
B. Departmental review
C. Updating and distribution
D. All of the above

**26. Structured walkthrough exercises are designed to validate _____.**

A. procedures
B. strategy
C. resources
D. readiness

**27. Tabletop simulation exercises are designed to validate _____.**

A. procedures
B. strategy
C. resources
D. readiness

**28. Which of the following entities should conduct BCP audits?**

A. The IT department
B. The Office of Information Security
C. Independent auditors

D. The BCT

**29. Which of the following organizations is the federal agency whose primary responsibility is to respond to disasters and assist with business recovery?**

A. Department of Homeland Security (DHS)
B. American Red Cross (ARC)
C. Federal Emergency Management Agency (FEMA)
D. National Guard

**30. Which term best describes organizations that have the ability to quickly adapt and recover from known or unknown changes to the environment?**

A. Accountable
B. Resilient
C. Compliant
D. Vulnerable

## CHAPTER 13

**1. Which of the following statements best defines the type of organizations that are subject to GLBA regulations?**

A. GLBA applies only to banks and credit unions.
B. GLBA applies only to check cashing businesses.
C. GLBA applies to any business engaged in financial services.
D. GLBA applies only to institutions licensed to offer depository services.

**2. The Financial Modernization Act of 1999 _____.**

A. deregulated financial services
B. mandated use of computers
C. required banks and credit unions to merge
D. prohibited banks from controlling a nonbanking company

**3. The GLBA requires financial institutions to protect which of the following?**

A. The privacy of customer NPPI
B. The security of customer NPPI
C. The privacy and the security of customer NPPI
D. None of the above

**4. Which of the following is not considered NPPI?**

A. SSN
B. Name
C. Checking account number
D. PIN or password associated with a financial account or payment card

**5. The Interagency Guidelines Establishing Standards for Safeguarding Customer Information was jointly developed by the _____.**

A. Federal Deposit Insurance Corporation (FDIC)
B. Office of the Comptroller of the Currency (OCC), Federal Reserve System (FRS),FDIC, and Office of Thrift Supervision (OTS)
C. Securities and Exchange Commission (SEC) and FDIC
D. National Credit Union Administration (NCUA) and FDIC

**6. Which of the following entities developed, published, and enforced the Safeguards Act?**

A. Federal Reserve System (FRS)
B. Securities and Exchange Commission (SEC)
C. Federal Trade Commission (FTC)
D. Federal Deposit Insurance Corporation (FDIC)

**7. Which of the following statements is false?**

A. The Safeguards Act applies to all federally insured institutions.

B. Compliance with the Safeguards Act is not proactively audited.
C. The Interagency Guidelines are more stringent than the Safeguards Act.
D. Enforcement of the Safeguards Act begins with a complaint.

**8. The Interagency Guidelines require a written security program that includes all of the following except _____.**

A. legal safeguards
B. physical safeguards
C. technical safeguards
D. administrative safeguards

**9. Financial institutions can be fined up to _____ per violation.**

A. $100
B. $1,000
C. $10,000
D. $100,000

**10. Financial institutions are expected to take a _____ approach to information security.**

A. threat-based
B. risk-based
C. audit-based
D. management-based

**11. Which of the following terms describes a potential danger that has the capacity to cause harm?**

A. Risk
B. Threat
C. Variable
D. Vulnerability

**12. Which of the following statements best describes a threat assessment?**

A. A threat assessment identifies the types of threats that may affect the institution or customers.
B. A threat assessment is a systematic rating of threats based on level of impact and likelihood.
C. A threat assessment is an audit report.
D. A threat assessment is a determination of inherent risk.

**13. Which of the following risk types is defined as a level of risk after controls and safeguards have been implemented?**

A. Ongoing risk
B. Residual risk
C. Acceptable risk
D. Inherent risk

**14. Which of the following risk management frameworks is recommended by the FFIEC?**

A. Basil
B. COBIT
C. NIST
D. FDIC

**15. Which of the following statements is true?**

A. Strategic risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.
B. Reputational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

C. Transactional risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.
D. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

**16. The risk arising from problems with service or product delivery is known as _____.**

A. strategic risk
B. reputational risk
C. transactional risk
D. operational risk

**17. At a minimum, financial institutions are expected to deliver user-focused information security training _____.**

A. quarterly
B. semi-annually
C. annually
D. bi-annually

**18. A security awareness and training program is considered which type of control?**

A. Administrative control
B. Physical control
C. Technical control
D. Contractual control

**19. Which of the following statements best describes independent testing?**

A. Independent testing is testing performed by a contractor.
B. Independent testing is testing performed by personnel not associated with the target system.
C. Independent testing is testing performed by personnel with security clearance.
D. Independent testing is testing performed by certified professionals.

**20. Which of the following test methodologies is a privileged inspection to determine condition, locate weakness or vulnerabilities, and identify corrective actions?**

A. Audit
B. Assessment
C. White box
D. Black box

**21. The statement, "An institution can outsource a task, but it cannot outsource the responsibility,"applies to an organization's relationship with _____.**

A. regulators
B. employees
C. directors
D. service providers

**22. Per the Interagency Guidance, which of the following entities is responsible for oversight of a financial institution's Information Security Program?**

A. Chief Executive Officer (CEO)
B. Information Security Officer
C. Board of Directors
D. Regulatory Agencies

**23. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it must notify _____.**

A. its regulatory agency
B. affected customers
C. Board of Directors
D. All of the above

**24. Which of the following statements is not true about financial institution regulatory examination?**

A. All institutions are subject to a three-year examination schedule.
B. A rating scale of 1 to 5 is used to represent supervisory concern.
C. Institutions found not in compliance can be subject to closure.
D. Results are presented to the Board of Directors.

**25. Which of the following statements best defines a corporate account takeover attack?**

A. Personal information is used to apply for a loan.
B. Users are denied access to online banking.
C. Fraudulent ACH and wire transfers are initiated from a commercial account.
D. Corporate logos are used in phishing emails.

**26. Which of the following is an example of multifactor authentication?**

A. Password and PIN
B. Password and picture
C. Password and challenge question
D. Password and out-of-band code

**27. Which of the following terms best describes the Supplemental Authentication Guidance requirement of layered defense?**

A. Dual control
B. Separation of duties
C. Defense in depth
D. Need-to-know

**28. Which of the following statements is true?**

A. When a financial institution chooses to outsource a banking function, it must conduct a due-diligence investigation.
B. When a financial institution chooses to outsource a banking function, it must report the relationship to its regulatory agency.
C. When a financial institution chooses to outsource a banking function, it must require the service provider to have appropriate controls and safeguards.
D. All of the above.

**29. Which of the following agencies is responsible for investigating consumer security–related complaints about a university financial aid office?**

A. FTC
B. Department of Education
C. FDIC
D. Sallie Mae

**30. Banks have customers; credit unions have _____.**

A. members
B. supporters
C. constituents
D. incorporators

## CHAPTER 14

**1. Which of the following statements best describes the intent of the initial HIPAA legislation adopted in 1996?**

A. The intent of the initial HIPAA legislation was to simplify and standardize the healthcare administrative process.
B. The intent of the initial HIPAA legislation was to lower healthcare costs.
C. The intent of the initial HIPAA legislation was to encourage electronic record sharing between healthcare providers.
D. The intent of the initial HIPAA legislation was to promote the continued use of paperbased

patient records.

**2. Which of the following statements best describes the intent of the Security Rule published in 2003?**

A. The intent of the Security Rule was to detail privacy practices.
B. The intent of the Security Rule was to establish breach notification procedures.
C. The intent of the Security Rule was to publish standards to protect ePHI.
D. The intent of the Security Rule was to assign enforcement responsibilities.

**3. In addition to healthcare providers, HIPAA/HITECH regulations apply to _____.**

A. medical insurance companies
B. pharmacies
C. business associates
D. All of the above

**4. Which of the following statements is not true?**

A. HIPAA is technology neutral.
B. HIPAA is vendor specific.
C. HIPAA documentation must be saved for six years.
D. HIPAA is scalable.

**5. Which of the following federal agencies is responsible for HIPAA/HITECH administration,oversight, and enforcement?**

A. Department of Health and Human Services
B. Department of Energy
C. Department of Commerce
D. Department of Education

**6. Which of the following is not a HIPAA/HITECH Security Rule category?**

A. Documentation
B. Compliance
C. Physical
D. Technical

**7. Which of the following statements is true?**

A. All implementation specifications are required.
B. All implementation specifications are optional.
C. Implementation specifications are either required or addressable.
D. Addressable specifications are optional.

**8. Which of the following statements best defines a business associate?**

A. A business associate is a person or organization that creates, stores, processes, accesses,
or transmits data on behalf of the CE.
B. A business associate is a healthcare provider with whom patient information is shared in the course of treatment.
C. A business associate is an employee who creates, stores, processes, or transmits data on
behalf of the CE.
D. A business associate is a person or organization that provides any service to the CE.

**9. In the context of HIPAA/HITECH, which of the following is not a factor to be considered in the determination of “reasonable and appropriate” security measures?**

A. Size of the CE
B. Level of risk
C. Geographic location of the CE
D. Complexity of implementation

**10. The Security Rule does not dictate a specific risk assessment methodology; however, the Department of Health and Human Services implementation and training guidance references which of the following methodologies?**

A. NIST 800-30: Risk Management Guide for Information Technology Systems
B. OCTAVE
C. FAIR
D. ISO 27002:2013

**11. Which of the following statements is true of the role of a HIPAA Security Officer?**

A. The role of a HIPAA Security Officer is optional.
B. The role of a HIPAA Security Officer can be performed by a committee.
C. The role of a HIPAA Security Officer is accountable by law for compliance.
D. The role of a HIPAA Security Officer must be assigned to a designated individual.

**12. Which of the following statements best defines authorization?**

A. Authorization is the process of positively identifying a user or system.
B. Authorization is the process of granting users or systems a predetermined level of access to information resources.
C. Authorization is the process of determining who accessed a specific record.
D. Authorization is the process of logging the access and usage of information resources.

**13. Which of the following statements is false?**

A. Identity-based access is granted by username.
B. Role-based access is granted by job or function.
C. Group-based access is granted by membership
D. Clinical-based access is granted by patient name.

**14. Which of the following would be considered an optional topic for workforce security training?**

A. Malware protection
B. Login procedures
C. Organizational HIPAA compliance penalties
D. Password management

**15. Users should be trained to recognize and _____ a potential security incident.**

A. report
B. contain
C. recover from
D. eradicate

**16. Which of the following statements is true of HIPAA compliance?**

A. HIPAA certification is granted by DHHS.
B. HIPAA accreditation is granted by the Joint Commissions for Hospital Accreditation (JCAHO).
C. There is no formal HIPAA/HITECH certification or accreditation process.
D. CEs must complete an annual self-assessment and submit it to the Centers for Medicare and Medicaid Services (CMS).

**17. Which of the following statements is true of a business associate's HIPAA/HITECH compliance requirements?**

A. A business associate's HIPAA/HITECH compliance requirements are the same as a healthcare provider.
B. A business associate's HIPAA/HITECH compliance requirements are limited to what is in the BA agreement.
C. A business associate's HIPAA/HITECH compliance requirements are not as stringent as those of a healthcare provider.
D. A business associate's HIPAA/HITECH compliance requirements are exempt if the organization's annual gross revenue is less than $500,000.

**18. According to the workstation security standard, when users leave their workstation unattended, they should _____.**

A. do nothing
B. lock the workstation
C. log out
D. turn off their monitor

**19. Which of the following is not an acceptable end-of-life disposal process for media that contains ePHI?**

A. Permanently wipe it
B. Shred it
C. Recycle it
D. Crush it

**20. Granting the minimal amount of permissions necessary to do a job reflects the security principle of _____.**

A. Need-to-know
B. Deny all
C. Allow some
D. Least privilege

**21. Both the HITECH Act and the Omnibus Rule refer to "unsecure data," which means data_____.**

A. in motion
B. with weak access controls
C. that is unencrypted
D. stored in the cloud

**22. Which of the following protocols/mechanisms cannot be used for transmitting ePHI?**

A. SSL
B. SFTP
C. Encrypted email
D. HTTP

**23. HIPAA-related documentation must be retained for a period of _____ years from the date of creation or the date it was last in effect, whichever is later.**

A. two
B. four
C. six
D. eight

**24. Which of the following changes was not introduced by the Omnibus Rule?**

A. The Omnibus Rule expanded the definition of a business associate.
B. The Omnibus Rule explicitly denied enforcement authority to State Attorneys General.
C. The Omnibus Rule increased violation penalties.
D. The Omnibus Rule defined breach notification requirements.

**25. Effective September 2013, subcontractors of business associates _____.**

A. are considered business associates
B. are granted limited liability
C. are not considered a covered entity
D. are exempt from HIPAA/HITECH regulations if they are considered a small business

**26. Which of the following is not a Security Rule violation category?**

A. Did not know
B. Did not cause
C. Willful neglect – corrected
D. Willful neglect – not corrected

**27. The “safe harbor” provision applies to _____.**

A. encrypted data
B. key management
C. dual control
D. de-identified data

**28. Which of the following is not required to be included in a breach notification?**

A. A description of the breach
B. The type of ePHI involved
C. Contact information for questions pertaining to the incident
D. Who was responsible for the breach

**29. A HIPAA standard defines what a covered entity must do; implementation specifications_____.**

A. describe the technology that must be used
B. describe how it must be done and/or what it must achieve
C. describe who must do it
D. describe the tools that must be used

**30. Subsequent legislation increased the maximum fines for HIPAA/HITECH violations to_____.**

A. up to $50,000 annually per violation category
B. up to $100,000 annually per violation category
C. up to $1,000,000 annually per violation category
D. up to $1,500,000 annually per violation category

## CHAPTER 15

**1. The majority of payment card fraud is borne by _____.**

A. consumers
B. banks, merchants, and card processors
C. Visa and MasterCard
D. All of the above

**2. Which of the following statements best describes the objective of the PCI Security Standards Council?**

A. The objective of the PCI Security Standards Council is to create a single enforcement body.
B. The objective of the PCI Security Standards Council is to create a common penalty structure.
C. The objective of the PCI Security Standards Council is to create a single payment card security standard.
D. The objective of the PCI Security Standards Council is to consolidate all payment card rules and regulations.

**3. A skimmer can be used to read _____.**

A. the cardholder data
B. sensitive authentication data
C. the associated PIN
D. All of the above

**4. According to PCI DDS, which of the following is true of the primary account number (PAN)?**

A. It must never be stored.
B. It can only be stored in an unreadable (encrypted) format.
C. It should be indexed.
D. It can be stored in plain text.

**5. Which of the following statements best describes sensitive authentication data?**

A. Sensitive authentication data must never be stored, ever.
B. Sensitive authentication data can be stored indefinitely in an unreadable (encrypted) format.
C. Sensitive authentication data should be masked.
D. Sensitive authentication data may never be stored post-authorization.

**6. Which of the following tasks is the PCI Security Standards Council not responsible for?**

A. Creating a standard framework
B. Certifying ASVs and QSAs
C. Providing training and educational materials
D. Enforcing PCI compliance

**7. Which of the following statements best describes PCI DSS Version 3?**

A. PCI DSS Version 3 is a departure from earlier versions because the core principles have changed.
B. PCI DSS Version 3 is a departure from earlier versions because it promotes a risk-based approach.
C. PC I DSS Version 3 is a departure from earlier versions because the penalties have increased.
D. PC I DSS Version 3 is a departure from earlier versions because it shifts the compliance obligation to service providers.

**8. Which of the following statements best describes the "cardholder data environment"?**

A. The "cardholder data environment" includes the people that handle cardholder data or sensitive authentication data.
B. The "cardholder data environment" includes the processes that handle cardholder data or sensitive authentication data.
C. The "cardholder data environment" includes the technology that handles cardholder data or sensitive authentication data.
D. All of the above.

**9. Sensitive authentication data does not include which of the following?**

A. PINs
B. Card expiration date
C. CVV2
D. Mag stripe or chip data

**10. Which of the following statements best describes the PAN?**

A. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements do not apply.
B. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements apply only to e-commerce merchants.
C. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements apply only to Level 1 merchants.
D. None of the above.

**11. Which of the following statements is true?**

A. When a debit or ATM card is lost or stolen, the cardholder liability is limited to $50.
B. When a debit or ATM card is lost or stolen, the cardholder is responsible for all charges.
C. When a debit or ATM card is lost or stolen, the cardholder liability depends on when the loss or theft is reported.
D. When a debit or ATM card is lost or stolen, the cardholder is never responsible for the charges.

**12. The terms CVV2, CID, CVC2, and CVV2 all refer to the _____.**

A. authentication data
B. security code

C. expiration date
D. account number

**13. There are 12 categories of PCI standards. In order to be considered compliant, an entity must comply with or document compensating controls for _____.**

A. All of the requirements
B. 90% of the requirements
C. 80% of the requirements
D. 70% of the requirements

**14. Which of the following is not considered a basic firewall function?**
**A. Ingress filtering**

B. Packet encryption
C. Egress filtering
D. Perimeter protection

**15. Which of the following is considered a secure transmission technology?**

A. FTP
B. HTTP
C. Telnet
D. SFTP

**16. Which of the following statements best describes key management?**

A. Key management refers to the generation, storage, and protection of encryption keys.
B. Key management refers to the generation, storage, and protection of server room keys.
C. Key management refers to the generation, storage, and protection of access control list keys.
D. Key management refers to the generation, storage, and protection of card manufacturing keys.

**17. Which of the following methods is an acceptable manner in which a merchant can transmit a PAN?**

A. Using cellular texting
B. Using an HTTPS/SSL session
C. Using instant messaging
D. Using email

**18. Which of the following statements is true?**

A. The PCI requirement to protect all systems against malware requires that merchants select a malware solution commensurate with the level of protection required.
B. The PCI requirement to protect all systems against malware requires that merchants select a PCI-certified anti-malware solution.
C. The PCI requirement to protect all systems against malware requires that merchants select a PCI-compliant anti-malware solution.
D. The PCI requirement to protect all systems against malware requires that merchants select a malware solution that can be disabled if necessary.

**19. Which of the following documents lists injection flaws, broken authentication, and cross-site scripting as the top three application security flaws?**

A. ISACA Top Ten
B. NIST Top Ten

C. OWASP Top Ten
D. ISO Top Ten

**20. Which of the following security principles is best described as the assigning of the minimum required permissions?**

A. Need-to-know
B. Deny all
C. Least privilege
D. Separation of duties

**21. Which of the following is an example of two-factor authentication?**

A. Username and password
B. Password and challenge question
C. Username and token
D. Token and PIN

**22. Skimmers can be installed and used to read cardholder data enter at _____.**

A. point-of-sale systems
B. ATMs
C. gas pumps
D. All of the above

**23. Which of the following best describes log data?**

A. Log data can be used to identify indicators of compromise.
B. Log data can be used to identify primary account numbers.
C. Log data can be used to identify sensitive authentication data.
D. Log data can be used to identify cardholder location.

**24. Quarterly external network scans must be performed by a _____.**

A. managed service provider
B. Authorized Scanning Vendor
C. Qualified Security Assessor
D. independent third party

**25. In keeping with the best practices set forth by the PCI standard, how often should information security policies be reviewed, updated, and authorized?**

A. Once
B. Semi-annually
C. Annually
D. Bi-annually

26. Which of the following is true of PCI requirements?

A. PCI requirements augment regulatory requirements.
B. PCI requirements supersede regulatory requirements.
C. PCI requirements invalidate regulatory requirements.
D. None of the above.

**27. The difference between a Level 1 merchant and Levels 2–4 merchants is that _____**

A. Level 1 merchants must have 100% compliance with PCI standards.
B. Level 1 merchants must complete an annual onsite compliance assessment.
C. Level 1 merchants must have quarterly external vulnerabilities scans.
D. Level 1 merchants must complete a self-assessment questionnaire.

**28. Which of the following statements is true of entities that experience a cardholder data breach?**

A. They must pay a minimum $50,000 fine.
B. They may be reassigned as a Level 1 merchant.
C. They will no longer be permitted to process credit cards.
D. They must report the breach to a federal regulatory agency.

**29. Which of the following statements best describes the reason different versions of the SAQ are necessary?**

A. The number of questions vary by payment card channel and scope of environment.
B. The number of questions vary by geographic location.
C. The number of questions vary by card brand.
D. The number of questions vary by dollar value of transactions.

**30. Which of the following statements is true of an entity that determines it is not compliant?**

A. The entity does not need to submit an SAQ.
B. The entity should notify customers.
C. The entity should submit an action plan along with its SAQ.
D. The entity should do nothing