# ChAPTER 7 REVIEW/Answers to test your skills

## Multiple Choice

**1.** Which of the following groups should be assigned responsibility for physical and environmental 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) \_\_\_\_\_\_\_\_\_\_\_.

**C.** Risk assessment

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

**A.** Crime prevention through environmental design

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

**D.** All 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

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

**D.** All the above

**7.** Best practices dictate that data centers should be \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**C.** Inconspicuous and unremarkable

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

**C.** Motion sensors

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

**A.** Everyone who enters the building

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

**B.** Shoulder surfing is the act of looking over someone’s shoulder to see what is on a computer screen.

**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?

**D.** Reducing power consumption increases CO2 emissions.

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

**C.** The product has met energy efficiency standards.

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

**D.** All the above

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

**B.** Power surge

**16.** Common causes of voltage variations include \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Lightning, storm damage, and electric demand

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

**C.** Fire prevention controls

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

**A.** Electrical equipment

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

**D.** All the above

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

**C.** Metadata

**21.** URL history, search history, form history, and download history are stored by the device \_\_\_\_\_\_\_\_\_\_\_.

**B.** Browser

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

**D.** Formatting a drive permanently deletes files.

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

**B.** Conventional hard drives

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

**C.** Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive, plus a read-verify process

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

**B.** Degaussing

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

**A.** Cross-cut

**27.** A certificate of destruction is evidence that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**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?

**C.** $188

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

**B.** Mobile device antitheft controls

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

**A.** Protecting human life

# ChAPTER 8 REVIEW/Answers to test your skills

## Multiple Choice

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

**C.** Both A and B.

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

**B.** Number of decisions and number of steps

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

**D.** Flowchart

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

**B.** RFC submission

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

**A.** The reason for 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?

**D.** All of the above.

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

**C.** Reverse engineering

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

**A.** A security patch is designed to fix security vulnerability.

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

**A.** Definition files

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

**B.** Security patches should be tested prior to deployment, if possible.

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

**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?

**B.** APT

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

**C.** worm

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

**B.** Bots

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

**D.** All of the above.

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

**C.** Replicated data is generally available in near or real time.

**17.** Organizations that are considering storing legally protected data in “the cloud” should \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** contractually obligate the service provider to protect the data

**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?

**C.** It should physically be destroyed.

**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?

**B.** ARPANET

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

**A.** SMTP

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

**B.** clear text

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

**D.** Users should delete unsolicited or unrecognized emails.

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

**C.** Misappropriate resources

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

**A.** A system log is a record of allowed and denied events.

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

**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.

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

**C.** Due diligence

**28.** SSAE16 audits must be attested to by a \_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Certified Public Accountant (CPA)

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

**D.** Confirmed and suspected incidents

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

**D.** All the above.

# ChAPTER 9 REVIEW/Answers to test your skills

## Multiple Choice

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

**D.** All the above

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

**D.** Authentication

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

**B.** Authorization

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

**A.** Subject

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

**C.** Least privilege

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

**C.** Need-to-know security principle

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

**C.** Access that is not explicitly permitted is forbidden.

**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?

**C.** The user can access specific categories of Top Secret information.

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

**A.** Data owners

**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?

**B.** Segregation of duties

**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?

**C.** Rule-based

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

**B.** Inheritance

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

**B.** Multifactor

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

**D.** All the above.

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

**B.** Cognitive

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

**C.** Out-of-band authentication

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

**A.** Trusted network

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

**A.** Firewall

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

**C.** An IDS uses signature-based detection and/or anomaly-based detection techniques.

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

**C.** Both A and B.

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

**B.** Mutual authentication is used to verify the legitimacy of the server before providing access credentials.

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

**D.** All the above

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

**C.** An employee who works from a remote location on a scheduled basis

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

**B.** Monitoring access is illegal.

**25.** The objective of user access controls is to ensure that authorized users can access information and resources and that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Unauthorized users are prevented from accessing information resources

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

**A.** Whitelists are IP addresses or Internet domain names of sites that are allowed.

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

**D.** H8djwk!!j4

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

**D.** All the above

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

**C.** Multilayer authentication

**30.** Access logs should be reviewed \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Daily

# ChAPTER 10 REVIEW/Answers to test your skills

## Multiple Choice

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

**B.** At inception.

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

**D.** All 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

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

**B.** The implementation phase

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

**B.** Retrofitting security controls to an application system after implementation is sometimes necessary based on testing and assessment results.

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

**B.** Beta

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

**A.** Alpha

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

**C.** Patches fix security vulnerabilities; updates add features and functionality.

**9.** The purpose of a rollback strategy is to \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Return to a previous stable state in case problems occur

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

**C.** A test environment should be as close to the live environment as possible.

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

**B.** Dummy data should be used in the testing environment.

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

**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?

**B.** SAMM

**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.

**15.** Input validation is the process of \_\_\_\_\_\_\_\_\_\_\_.

**B.** Verifying data syntax

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

**C.** Dynamic data

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

**B.** Input validation

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

**C.** Both A and B.

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

**D.** Encryption

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

**C.** Digital signatures guarantee integrity and nonrepudiation.

**21.** Hashing is used to ensure message integrity by \_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Comparing hash values

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

**B.** Integrity

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

**B.** The security of the encryption relies on the key.

**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.

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

**D.** 2256

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

**C.** The key must be publicly known.

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

**D.** Digital certificate

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

**A.** Public and private keys

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

**D.** Symmetric key

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

**B.** Digital signature

# ChAPTER 11 REVIEW/Answers to test your skills

## Multiple Choice

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

**B.** Incident management is a consistent approach to responding to and resolving issues.

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

**B.** Over time, security-related incidents have become more prevalent and more disruptive.

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

**C.** Risk management

**4.** An information security incident can \_\_\_\_\_\_\_\_\_\_\_.

A. Compromise business security

B. Disrupt operations

C. Impact customer trust

**D.** All 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?

**B.** The organization must be notified and respond accordingly.

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

**C.** DDoS 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

**8.** Employees who report incidents should be \_\_\_\_\_\_\_\_\_\_\_.

**B.** Praised for their actions

**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 the above.

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

**B.** A precursor

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

**B.** Containment

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

**D.** Recovery

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

**C.** Eradication

**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

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

**C.** Incident plan auditing

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

**D.** Cost of the activity

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

**A.** Early in the incident lifecycle

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

**C.** Secret Service

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

**B.** Chain of custody

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

**C.** PII

**21.** Federal breach notification laws apply to \_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Specific sectors such as financial and healthcare

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

**A.** Notification be sent to affected parties

**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.

**D.** Veterans Administration

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

**B.** State laws exist because there is no comparable federal law.

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

**C.** California

**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.

**27.** Consumers are most concerned about compromise of their \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Password/PIN and SSN

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

**B.** Consumers want to be notified of a data breach and they overwhelmingly expect to be provided as much detail as possible.

**29.** Incident response plans and procedures should be tested \_\_\_\_\_\_\_\_\_\_\_\_.

**C.** On an ongoing basis

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

**D.** Authorizing incident response policies

# ChAPTER 12 REVIEW/Answers to test your skills

## Multiple Choice

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

**B.** Availability

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

**C.** A disaster is a significant disruption of normal business functions.

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

**B.** Environmental

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

**B.** Threat assessment

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

**A.** Risk assessment

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

**D.** All the above

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

**C.** Maximum tolerable downtime (MTD)

**8.** The recovery point objective (RPO) represents \_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Acceptable data loss

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

**C.** Information systems

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

**D.** All the above

**11.** Legal and regulatory accountability for an organization’s preparedness is assigned to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**C.** The Board of Directors or organizational equivalent

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

**B.** Executive management

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

**B.** The occupant emergency plan

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

**B.** The BCT

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

**C.** Command and control center

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

**B.** Cross-trained personnel or service providers familiar with the organization

**17.** The BCT is tasked with all the following activities *except* \_\_\_\_\_\_\_\_\_\_\_.

**D.** Auditing the plan

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

**A.** Hot site

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

**C.** Cold site

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

**B.** The IT department is responsible for recovery and resumption related to the information system and supporting infrastructure.

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

**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

**23.** Validation and deactivation activities are part of \_\_\_\_\_\_\_\_\_\_.

**D.** Resumption

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

**D.** Emergency passcodes

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

**D.** All the above

**26.** Structured walkthrough exercises are designed to validate \_\_\_\_\_\_\_\_\_.

**A.** Procedures

**27.** Tabletop simulation exercises are designed to validate \_\_\_\_\_\_\_\_\_\_.

**D.** Readiness

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

**C.** Independent auditors

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

**C.** Federal Emergency Management Agency (FEMA)

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

**B.** Resilient

# ChAPTER 13 REVIEW/Answers to test your skills

## Multiple Choice

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

**C.** GLBA applies to any business engaged in financial services.

**2.** The Financial Modernization Act of 1999 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Deregulated financial services

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

**C.** The privacy and the security of customer NPPI

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

**B.** Name

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

**B.** Office of the Comptroller of the Currency (OCC), Federal Reserve System (FRS), FDIC, and Office of Thrift Supervision (OTS)

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

**C.** Federal Trade Commission (FTC)

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

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

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

**A.** Legal safeguards

**9.** Financial institutions can be fined up to \_\_\_\_\_ per violation.

**D.** $100,000

**10.** Financial institutions are expected to take a \_\_\_\_\_\_\_\_\_ approach to information security.

**B.** Risk-based

**11.** Which of the following terms describes a potential danger that has the capacity to cause harm?

**B.** Threat

**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.

**13.** Which of the following risk types is defined as a level of risk after controls and safeguards have been implemented?

**B.** Residual risk

**14.** Which of the following risk management frameworks is recommended by the FFIEC?

**C.** NIST

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

**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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**C.** Transactional risk

**17.** At a minimum, financial institutions are expected to deliver user-focused information security training \_\_\_\_\_\_\_\_\_.

**C.** Annually

**18.** A security awareness and training program is considered which type of control?

**A.** Administrative control

**19.** Which of the following statements best describes independent testing?

**B.** Independent testing is testing performed by personnel not associated with the target system.

**20.** Which of the following test methodologies is a privileged inspection to determine condition, locate weakness or vulnerabilities, and identify corrective actions?

**B.** Assessment

**21.** The statement, “An institution can outsource a task, but it cannot outsource the responsibility,” applies to an organization’s relationship with \_\_\_\_\_\_\_\_.

**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?

**C.** Board of Directors

**23.** If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it must notify \_\_\_\_\_\_\_\_\_\_\_\_.

**D.** All the above

**24.** Which of the following statements is *not* true about financial institution regulatory examination?

**A.** All institutions are subject to a 3-year examination schedule.

**25.** Which of the following statements best defines a corporate account takeover attack?

**C.** Fraudulent ACH and wire transfers are initiated from a commercial account.

**26.** Which of the following is an example of multifactor authentication?

**D.** Password and out-of-band code

**27.** Which of the following terms best describes the Supplemental Authentication Guidance requirement of layered defense?

**C.** Defense in depth

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

**D.** All the above.

**29.** Which of the following agencies is responsible for investigating consumer security-related complaints about a university financial aid office?

**A.** FTC

**30.** Banks have customers; credit unions have \_\_\_\_\_\_\_\_.

**A.** members

# ChAPTER 14 REVIEW/Answers to test your skills

## Multiple Choice

**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.

**2.** Which of the following statements best describes the intent of the Security Rule published in 2003?

**C.** The intent of the Security Rule was to publish standards to protect ePHI.

**3.** In addition to healthcare providers, HIPAA/HITECH regulations apply to \_\_\_\_\_\_\_\_\_\_.

**D.** All the above

**4.** Which of the following statements is *not* true?

**B.** HIPAA is vendor-specific.

**5.** Which of the following federal agencies is responsible for HIPAA/HITECH administration, oversight, and enforcement?

**A.** Department of Health and Human Services

**6.** Which of the following is *not* a HIPAA/HITECH Security Rule category?

**B.** Compliance

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

**C.** Implementation specifications are either required or addressable.

**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.

**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?

**C.** Geographic location of the CE

**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

**11.** Which of the following statements is true of the role of a HIPAA Security Officer?

**D.** The role of a HIPAA Security Officer must be assigned to a designated individual.

**12.** Which of the following statements best defines authorization?

**B.** Authorization is the process of granting users or systems a predetermined level of access to information resources.

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

**D.** Clinical-based access is granted by patient name.

**14.** Which of the following would be considered an optional topic for workforce security training?

**C.** Organizational HIPAA compliance penalties

**15.** Users should be trained to recognize and \_\_\_\_\_\_\_\_\_ a potential security incident.

**A.** Report

**16.** Which of the following statements is true of HIPAA compliance?

**C.** There is no formal HIPAA/HITECH certification or accreditation process.

**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.

**18.** According to the workstation security standard, when users leave their workstation unattended, they should \_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Lock the workstation

**19.** Which of the following is *not* an acceptable end-of-life disposal process for media that contains ePHI?

**C.** Recycle it.

**20.** Granting the minimal amount of permissions necessary to do a job reflects the security principle of \_\_\_\_\_\_\_\_\_\_\_.

**D.** Least privilege

**21.** Both the HITECH Act and the Omnibus Rule refer to “unsecure data,” which means data \_\_\_\_\_\_\_\_\_\_.

**C.** That is unencrypted

**22.** Which of the following protocols/mechanisms cannot be used for transmitting ePHI?

**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.

**C.** six

**24.** Which of the following changes was *not* introduced by the Omnibus Rule?

**B.** The Omnibus Rule explicitly denied enforcement authority to the State Attorney’s General.

**25.** Effective September 2013, subcontractors of business associates \_\_\_\_\_\_\_\_\_\_\_\_\_.

**A.** Are considered business associates

**26.** Which of the following is *not* a Security Rule violation category?

**B.** Did not cause

**27.** The “safe harbor” provision applies to \_\_\_\_\_\_\_\_\_\_.

**A.** Encrypted data

**28.** Which of the following is *not* required to be included in a breach notification?

**D.** Who was responsible for the breach

**29.** A HIPAA standard defines what a covered entity must do; implementation specifications \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Describe how it must be done and/or what it must achieve

**30.** Subsequent legislation increased the maximum fines for HIPAA/HITECH violations to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**D.** Up to $1,500,000 annually per violation category

# ChAPTER15 REVIEW/Answers to test your skills

## Multiple Choice

**1.** The majority of payment card fraud is borne by \_\_\_\_\_\_\_\_\_\_.

**B.** Banks, merchants, and card processors

**2.** Which of the following statements best describes the objective of the PCI Security Standards Council?

**C.** The objective of the PCI Security Standards Council is to create a single payment card security standard.

**3.** A skimmer can be used to read \_\_\_\_\_\_\_\_\_\_\_\_.

**C.** The associated PIN

**4.** According to PCI DDS, which of the following is true of the primary account number (PAN)?

**B.** It can be stored only in an unreadable (encrypted) format.

**5.** Which of the following statements best describes sensitive authentication data?

**A.** Sensitive authentication data must never be stored, ever.

**6.** Which of the following tasks is the PCI Security Standards Council *not* responsible for?

**D.** Enforcing PCI compliance

**7.** Which of the following statements best describes PCI DSS Version 3?

**B.** PCI DSS Version 3 is a departure from earlier versions because it promotes a risk-based approach.

**8.** Which of the following statements best describes the “cardholder data environment”?

**D.** All the above.

**9.** Sensitive authentication data does *not* include which of the following?

**B.** Card expiration date

**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.

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

**C.** When a debit or ATM card is lost or stolen, the cardholder liability depends on when the loss or theft is reported.

**12.** The terms CVV2, CID, CVC2, and CVV2 all refer to the \_\_\_\_\_\_\_\_\_\_\_.

**B.** Security code

**13.** There are 12 categories of PCI standards. To be considered compliant, an entity must comply with or document compensating controls for \_\_\_\_\_\_\_\_\_.

**A.** All the requirements

**14.** Which of the following is *not* considered a basic firewall function?

**B.** Packet encryption

**15.** Which of the following is considered a secure transmission technology?

**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.

**17.** Which of the following methods is an acceptable manner in which a merchant can transmit a PAN?

**B.** Using an HTTPS/SSL session

**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.

**19.** Which of the following documents lists injection flaws, broken authentication, and cross-site scripting as the top three application security flaws?

**C.** OWASP Top Ten

**20.** Which of the following security principles is best described as the assigning of the minimum required permissions?

**C.** Least privilege

**21.** Which of the following is an example of two-factor authentication?

**D.** Token and PIN

**22.** Skimmers can be installed and used to read cardholder data entered at \_\_\_\_\_\_\_\_.

**D.** All the above

**23.** Which of the following best describes log data?

**A.** Log data can be used to identify indicators of compromise.

**24.** Quarterly external network scans must be performed by a \_\_\_\_\_\_\_\_\_\_.

**B.** Authorized Scanning Vendor

**25.** In keeping with the best practices set forth by the PCI standard, how often should information security policies be reviewed, updated, and authorized?

**C.** Annually

**26.** Which of the following is true of PCI requirements?

**A.** PCI requirements augment regulatory requirements.

**27.** The difference between a Level 1 merchant and Levels 2–4 merchants is that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Level 1 merchants must complete an annual onsite compliance assessment.

**28.** Which of the following statements is true of entities that experience a cardholder data breach?

**B.** They may be reassigned as a Level 1 merchant.

**29.** Which of the following statements best describes the reason different versions of the SAQ are necessary?

**A.** The number of questions varies by payment card channel and scope of environment.

**30.** Which of the following statements is true of an entity that determines it is not compliant?

**C.** The entity should submit an action plan along with its SAQ.