# ChAPTER1 REVIEW/Answers to test your skills

## Multiple Choice

1. Policies define which of the following?

 D. All the above

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

 A. Chaos

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

 B. A fundamental philosophy or belief

4. Which of the following best describes corporate culture?

 A. Shared attitudes, values, and goals

5. Which of the following is a true statement?

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

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

 D. All the above

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

 C. How an organization protects information assets and systems

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

 D. Building graffiti

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

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

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

 D. Management

11. Who should always be exempt from policy requirements?

 C. No one

12. “Attainable” means that the policy \_\_\_\_\_\_\_\_\_\_\_.

 A. Can be successfully implemented

13. Which of the following statements is always true?

 C. Policies should be adaptable.

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

 A. Meaningless

15. Who must approve the retirement of a policy?

 C. Executive management or the Board of Directors

16. Which of the following sectors is not considered part of the “critical infrastructure”? D. Chemical industry

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

 C. Regulation

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

 A. Financial and medical records

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

 D. California

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

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

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

 D. Policy lifecycle

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

 C. Personnel throughout the company

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

 B. Enforcement

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

 D. All the above

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

 C. The policy becomes expected behavior; all others being deviant.

26. How often should policies be reviewed?

 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

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

 C. Being a careful steward of information in your care

29. Who should authorize policies?

 A. Directors or executive management

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

 D. To protect information and information systems from authorized users

# ChAPTER2 REVIEW/Answers to test your skills

## Multiple Choice

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

 B. Guiding principles, standards, guidelines, and procedures

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

 C. To dictate mandatory requirements

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

 D. To make suggestions

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

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

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

**C.** Procedure

**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

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

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

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

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

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

**B.** False

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

**D.** All the above

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

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

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

**B.** Policy Heading

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

**C.** Policy goals and objectives

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

**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.

**B.** Policy statement

**16.** A policy should be considered \_\_\_\_\_.

**A.** Mandatory

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

**A.** A glossary of terms used

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

**C.** Policy enforcement clause

**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.”

**D.** The policy statement

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

**A.** Introduction

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

**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

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

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

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

**B.** Clear and concise

**25.** Readers prefer “plain language” because it \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**D.** All the above

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

**C.** Technical jargon

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

**A.** Must

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

**B.** Employees

**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?

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

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

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

# ChAPTER3 REVIEW/Answers to test your skills

## Multiple Choice

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

**C.** Confidentiality, integrity, availability

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

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

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

**A.** Disaster recovery site

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

**A.** Protection from unauthorized access

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

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

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

**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

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

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

**C.** Accounting

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

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

**10.** An information owner is responsible for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

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

**B.** International Organization for Standardization

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

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

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

**B.** Political

**14.** The greater the criminal work factor, the \_\_\_\_\_

**A.** More time it takes

**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?

**C.** Denial of service

**16.** Information custodians are responsible for \_\_\_\_\_

**E.** Implementing safeguards

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

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

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

**D.** All the above

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

**C.** ISO/IEC 27000

**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?

**D.** Risk assessment

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

**B.** Asset management

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

**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

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

**B.** Compliance

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

**C.** Incident Management

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

**C.** Availability

**27.** The \_\_\_\_\_\_\_\_\_\_\_\_ can be held legally responsible for the safeguarding of legally protected information.

**B.** Information owner

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

**C.** Human Resources

**29.** Defining organizational roles, responsibilities, and authority relate to the \_\_\_\_\_\_\_\_\_\_ domain.

**C.** Governance

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

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

**Chapter4 REVIEW/Answers to test your skills**

## Multiple Choice

1. When an information security program is said to be “strategically aligned,” this indicates that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**D.** All of the above

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

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

**3.** Information security policies should be authorized by \_\_\_\_\_\_\_\_\_\_\_\_.

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

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

**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?

**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.

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

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

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

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

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

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

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

**A.** Average

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

**D.** Purchasing

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

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

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

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

**14.** Defining protection requirements is the responsibility of \_\_\_\_\_\_\_\_\_\_\_\_.

**C.** Data owners

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

**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?

**B.** Risk

**17.** Inherent risk is the state before \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**B.** security measures have been implemented

**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?

**C.** Threat

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

**B.** Threat source

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

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

**B.** risk tolerance

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

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

**23.** A control is a security measure that is designed to \_\_\_\_\_\_\_ a threat source.

**D.** All the above

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

**A.** Risk acceptance

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

**C.** Residual risk

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

**B.** Risk transfer

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

**C.** Reputation risk

**28.** Compliance risk as it relates to federal and state regulations can never be \_\_\_\_\_\_\_\_\_\_\_\_.

**B.** Transferred

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

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

**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.

# ChAPTER5 REVIEW/Answers to test your skills

## Multiple Choice

**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?

**B.** Information asset

**2.** Information systems \_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_, and \_\_\_\_\_\_\_\_\_\_ information.

**C.** Store, process, and transmit

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

**A.** Classifying information

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

**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

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

**D.** All 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.

**C.** Confidentiality

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

**B.** Top Secret

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

**B.** Unclassified

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

**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?

**B.** Integrity

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

**D.** No.

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

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

**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?

**C.** Nonpublic personal information

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

**C.** Users who have a “need to know”

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

**D.** All 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

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

**A.** Declassification

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

**C.** Reclassification

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

**B.** Availability

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

**A.** Server

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

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

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

**C.** An IP address

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

**A.** Software assets

**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?

**B.** Derivative classification

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

**D.** Home address

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

**B.** Encrypted

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

**D.** All the above.

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

**C.** A logical address

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

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

# ChAPTER6 REVIEW/Answers to test your skills

## Multiple Choice

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

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

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

**C.** Recruitment

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

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

**4.** Data submitted by potential candidates must be \_\_\_\_\_\_\_\_\_\_\_\_.

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

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

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

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

**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

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

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

**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?

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

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

**B.** Employers must get the candidate’s consent to request a credit report.

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

**C.** Published telephone number

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

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

**B.** The information owner

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

**B.** The information custodians

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

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

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

**A.** Handling standards

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

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

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

**B.** Security Education Training Awareness

**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?

**C.** A security awareness program

**20.** A network engineer attends a 1-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?

**B.** A security training program

**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

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

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

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

**D.** All the above

**24.** Studies often cite \_\_\_\_\_\_\_\_\_\_\_\_ as the weakest link in information security.

**B.** People

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

**A.** Long-term

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

**D.** FERPA

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

**B.** HIPAA

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

**C.** Social Security number

**29.** After a new employee’s retention period has expired, completed paper employment applications should be \_\_\_\_\_\_\_\_\_\_\_.

**A.** Cross-cut shredded

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

**B.** A social engineering attack