Test Bank for Auditing IT Infrastructures for Compliance 3rd Edition by Johnson, Weiss, Solomon

ISBN: 9781284236606

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284236606, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. An IT security assessment is a key activity that involves the management of:
A) compliance with federal regulations.
B) risk.
C) IT governance.
D) controls.
Ans: B
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: An IT security assessment is a key activity that involves the management of risk, an uncertainty that might lead to a loss.
Taxonomy: Understand

2. Which of the following is *not* true of information security and information systems?
A) An IT security assessment is a key activity that involves the management of risk.
B) Loss is an uncertainty that might lead to a risk.
C) A risk-based approach to security includes identifying and categorizing information and information systems.
D) Monitoring security controls is a continual cycle as organizations evolve.
Ans: B
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Risk is an uncertainty that might lead to a loss.
Taxonomy: Understand

3. Security controls include the physical, procedural, and technical mechanisms to safeguard systems. When assessing security controls, what is the best indicator that the controls are functioning as expected?
A) Whether the controls are appropriately designed
B) Whether the controls are appropriately implemented
C) Whether controls are producing the required results
D) Whether the controls align to the policy of an organization
Ans: C
Complexity: Hard
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Analyze

4. Carl is an IT auditor. He is evaluating system security controls, one of which locks users out of a system after too many unsuccessful access attempts. Carl consults National Institute of Standards and Technology (NIST) Special Publication 800-53 (NIST 2013) and finds the following statement: “Determine if the system enforces the defined threshold of consecutive invalid access attempts.” The statement is an example of:
A) an assessment objective.
B) an assessment method.
C) a control.
D) an assessment object.
Ans: A
Complexity: Hard
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Analyze

5. An auditor can use several methods to conduct an assessment of IT security controls. Which of the following is *not* a typical assessment method?
A) Examination
B) Interview
C) Install
D) Test
Ans: C
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: IT security control assessments typically involve examination, interviews, and/or testing.
Taxonomy: Remember

6. Which of the following is best described as an assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker?
A) Risk management

B) Attack vector
C) Risk assessment
D) Penetration test
Ans: D
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

7. What is the best definition of an audit?
A) A key activity that involves the management of risk
B) An independent, objective assurance and consulting activity designed to add value and improve an organization's operations
C) An organization's ability to follow its own rules, which are typically based on defined policies and standards
D) An assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker
Ans: B
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

8. What ensures that only authorized users can read data?
A) Confidentiality
B) Integrity
C) Availability
D) Accountability
Ans: A
Complexity: Easy
Ahead: What Is the Confidentiality, Integrity, and Availability (C-I-A) Triad?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Remember

9. What ensures that only authorized users can modify data?
A) Confidentiality
B) Integrity
C) Availability
D) Accountability
Ans: B
Complexity: Easy
Ahead: What Is the Confidentiality, Integrity, and Availability (C-I-A) Triad?
Subject: Chapter 1

Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Remember

10. What is a control that maintains the integrity of data?
A) Limiting access to authorized users through the use of IDs and passwords
B) Enabling failover to a backup server in real time
C) Enabling failover to a backup server
D) Ensuring a message reaches its destination
Ans: A
Complexity: Medium
Ahead: What Is the Confidentiality, Integrity, and Availability (C-I-A) Triad?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

11. What is the act or process of doing what you have been asked or ordered to do?
A) Compliance
B) Accountability
C) Auditing
D) Assurance
Ans: A
Complexity: Easy
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

12. What refers to the need or desire for an organization to follow rules and guidelines set forth by external organizations and initiatives?
A) Internal compliance
B) Compliance with an organization's control objectives
C) Compliance with an organization's security policy
D) External compliance
Ans: D
Complexity: Medium
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Internal compliance refers to an organization's ability to follow its own rules; external compliance refers to the need or desire for an organization to follow rules and guidelines set forth by external organizations and initiatives.
Taxonomy: Remember

13. Compliance rules for organizations typically do *not* come from:

A) laws.
B) regulations.
C) social engineering.
D) an organization's policies.
Ans: C
Complexity: Easy
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Social engineering is something that might be audited but is not typically a source of compliance rules.
Taxonomy: Remember

14. Which of the following is *not* true of compliance, risk, and governance?
A) Compliance is closely related to risk management and governance at the technical, procedural, and strategic levels.
B) Assurance seeks to mitigate risk through controls.
C) Compliance helps risk management by verifying that the desired controls are in place.
D) Governance seeks to better run an organization using complete and accurate information and management processes or controls.
Ans: B
Complexity: Hard
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Risk management seeks to mitigate risk through controls.
Taxonomy: Analyze

15. Which of the following is a general step to meeting regulatory compliance?
A) Interpret the regulation and how it applies to the federal government.
B) Identify accountability at the governance, department, and executive levels of the regulatory body.
C) Identify any gaps in controls or determine where the organization stands with the compliance mandate.
D) Ensure management devises a plan to maintain any gaps in controls.
Ans: C
Complexity: Hard
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Analyze

16. An organization's ability to follow its own rules, which are typically based on defined policies, is called:
A) regulatory compliance.
B) internal compliance.
C) meeting contractual obligations.
D) external compliance.
Ans: B
Complexity: Easy
Ahead: What Is Compliance?

Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Remember

17. Regulatory compliance benefits:
A) organizations and shareholders only.
B) IT auditors, IT departments, and public confidence.
C) organizations, consumers, and shareholders.
D) IT departments and consumers only.
Ans: C
Complexity: Hard
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Regulatory compliance benefits organizations, consumers, and shareholders. Regulatory compliance protects an organization's reputation and integrity. It considers the interests of the consumer and shareholders.
Taxonomy: Analyze

18. _____ by itself does not reduce _____; it must be implemented and maintained.
A) Accountability; attack vectors
B) Risk; compliance gaps
C) A policy; risk
D) A risk; accountability
Ans: C
Complexity: Medium
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Analyze

19. A policy requiring enhanced security measures is not effective unless it is fully implemented. During a compliance audit, which of the following is *least* likely to ensure that policies are enforced?
A) Documentation of the compliance governance structure and ensuring that it is understood
B) Incentive structures that create a conflict of interest
C) Measurement and timely reporting on policy outcomes
D) Clear accountability
Ans: B
Complexity: Medium
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

20. An organization that does not comply with compliance laws faces the threat of fines and imprisonment. What other negative effect might an organization experience, especially if noncompliance causes an incident that goes public?
A) Legal fees resulting from infringements contained within many regulations
B) Increased revenue
C) Increase in stock price
D) Decreases in the cost of capital
Ans: A
Complexity: Easy
Ahead: What If an Organization Does Not Comply with Compliance Laws?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: Understand

True/False

1. True or False? Information systems typically refer to the IT infrastructure components (hardware and software) that collect, store, and process data.
Ans: True
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

2. True or False? Assurances are actions or changes to be applied to systems to reduce weaknesses or potential losses.
Ans: False
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Security controls are actions or changes to be applied to systems to reduce weaknesses or potential losses.
Taxonomy:

3. True or False? Security controls include the physical, procedural, and technical mechanisms to safeguard systems.
Ans: True
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

4. True or False? National Institute of Standards and Technology (NIST) Special Publication 800-53 (NIST 2013) defines a recommended assessment procedure.
Ans: True
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

5. True or False? IT security assessments must be comprehensive to cover all security controls in a target organization.
Ans: False
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Not all IT security assessments need to be comprehensive to cover all security controls or even all information systems.
Taxonomy:

6. True or False? Penetration tests simulate the process a real adversary may take while avoiding any business disruptions or outages.
Ans: True
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

7. True or False? Types of audits may include network security architecture and physical security.
Ans: True
Complexity: Easy
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

8. True or False? If an audit determines a control is poorly designed, further tests are needed to determine if the control is effective.
Ans: False
Complexity: Hard

Ahead: What Is the Difference Between Information System and Information Security Compliance
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: If an audit determines a control is poorly designed, then typically there is no need to test if the control is effective.
Taxonomy:

9. True or False? Governance aims to ensure that a sound security policy and comprehensive procedures are in place to implement policies.
Ans: True
Complexity: Medium
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

10. True or False? In terms of auditing, assurance describes a very formal audit.
Ans: True
Complexity: Medium
Ahead: What Is the Difference Between Information System and Information Security Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

11. True or False? Where external compliance refers to an organization's ability to follow its own rules, internal compliance refers to the need and desire for an organization to follow rules and guidelines set forth by outside organizations and authorities.
Ans: False
Complexity: Medium
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Internal compliance refers to an organization's ability to follow its own rules. External compliance refers to the need and desire for an organization to follow rules and guidelines set forth by external organizations and authorities.
Taxonomy:

12. True or False? In terms of compliance, regulations do not provide specifics and are open for interpretation.
Ans: True
Complexity: Easy
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:

Taxonomy:

13. True or False? Compliance frameworks such as Control Objectives for Information and Related Technology (COBIT), and standards put forth by the National Institute of Standards and Technology (NIST), help organizations interpret how to comply with regulations.
Ans: True
Complexity: Medium
Ahead: What Is Compliance?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

14. True or False? Compliance audits must include a detailed assessment of the various governance forums that ensure policies are in place and appropriately implemented.
Ans: True
Complexity: Medium
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

15. True or False? Risk management requires that every risk be mitigated.
Ans: False
Complexity: Medium
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Risk management means deeming some risks acceptable so a company may accomplish its business goals.
Taxonomy:

16. True or False? Unenforced policies do not reduce risk.
Ans: True
Complexity: Easy
Ahead: Why Are Governance and Compliance Important?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

17. True or False? Noncompliance with regulations can result in significant fines and jail time.
Ans: True
Complexity: Easy

Ahead: What If an Organization Does Not Comply with Compliance Laws?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

18. True or False? In terms of regulations, strict liability means even if there was not intent, government agencies can levy fines on organizations and some individuals can spend time in prison.
Ans: True
Complexity: Medium
Ahead: What If an Organization Does Not Comply with Compliance Laws?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy:

19. True or False? Regulators may never perform their own audits of an organization to ensure compliance with applicable laws.
Ans: False
Complexity: Medium
Ahead: What If an Organization Does Not Comply with Compliance Laws?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback: Regulators are typically charged with performing their own audits of an organization to ensure compliance with applicable laws.
Taxonomy:

20. True or False? The Payment Card Industry Data Security Standard (PCI DSS) is an industry-created standard that applies to organizations that process payment cards.
Ans: True
Complexity: Medium
Ahead: What If an Organization Does Not Comply with Compliance Laws?
Subject: Chapter 1
Title: The Need for Information Systems Compliance
Feedback:
Taxonomy: