Test Bank for Security Policies and Implementation Issues 3rd Johnson

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Information Field: Objective
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 97812841899840, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple-Choice

1. _____ is the act of protecting information and the systems that store and process it.
A) Information systems security
B) Continuous improvement
C) Change management
D) Availability
Ans: A
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Information systems security (ISS) is the act of protecting information and the systems that store and process it. This protection is against risks that would lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information.
Taxonomy: Remember

2. _____ is a widely accepted international best practices framework for implementing information systems security.
A) Information Systems Audit and Control Association (ISACA)
B) Control Objectives for Information and related Technology (COBIT)
C) Capability Maturity Model Integration (CMMI)
D) Information assurance (IA)
Ans: B
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: COBIT is a widely accepted international best practices framework for implementing information systems security.
Taxonomy: Remember

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

3. Which of the following is *not* one of the four domains that collectively represents a conceptual information systems security management life cycle?
A) Align, Plan, and Organize
B) Build, Acquire, and Implement
C) Deliver, Service, and Support
D) Evaluate, Assess, and Recover
Ans: D
Complexity: Difficult
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: The last of the four domains is Monitor, Evaluate, and Assess.
Taxonomy: Analyze

4. The COBIT Align, Plan, and Organize domain includes basic details of an organization's requirements and goals. This domain answers which of the following questions?
A) What are the areas of vulnerability?
B) Where is there room to build?
C) What are the processes for quality assurance?
D) What do you want to do?
Ans: D
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: The COBIT Align, Plan, and Organize domain is where an organization determines how a project will be managed. This domain answers the questions "What do you want to do?" and "How do you want to get there?"
Taxonomy: Analyze

5. When writing a _____ , one could state how often a supplier will provide a service or how quickly a firm will respond. For managed services, this document often covers system availability and acceptable performance measures.
A) policy framework
B) policy
C) service level agreement
D) standard
Ans: C
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A service level agreement is a stated commitment to provide a specific service level. A contract is a separate document, and policies and standards are used internally in organizations.
Taxonomy: Apply

6. A _____ would be a misconfiguration of a system that allows the hacker to gain unauthorized access, whereas a _____ is a combination of the likelihood that such a misconfiguration could happen, a hacker's exploitation of it, and the impact if the event occurred.

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

A) vulnerability, risk
B) risk, vulnerability
C) threat, risk
D) risk, threat
Ans: A
Complexity: Difficult
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A vulnerability would be a misconfiguration of a system that allows the hacker to gain unauthorized access, whereas a risk is a combination of the likelihood that such a misconfiguration could happen, a hacker's exploitation of it, and the impact if the event occurred. A threat is a human-caused or natural event that could impact the system.
Taxonomy: Analyze

7. During the COBIT _____ domain phase, the service level agreement (SLA) plays a significant role because it determines the type of solutions that will be selected. Additionally, change management is critical to this phase.
A) Align, Plan, and Organize
B) Build, Acquire, and Implement
C) Deliver, Service, and Support
D) Monitor, Evaluate, and Assess
Ans: B
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: SLAs and change management are important in the COBIT Build, Acquire, and Implement phase.
Taxonomy: Remember

8. During the COBIT _____ domain phase, you analyze data from the prior phase and compare it with day-to-day operations, and then apply lessons learned to improve operations.
A) Align, Plan, and Organize
B) Build, Acquire, and Implement
C) Deliver, Service, and Support
D) Monitor, Evaluate, and Assess
Ans: C
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: During the Deliver, Service, and Support phase, you analyze data from the Build, Acquire, and Implement phase and compare it with day-to-day operations, and then apply lessons learned to improve operations.
Taxonomy: Remember

9. Internal and external audits are most likely to take place during the COBIT _____ domain phase.
A) Align, Plan, and Organize
B) Build, Acquire, and Implement

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

C) Deliver, Service, and Support
D) Monitor, Evaluate, and Assess
Ans: D
Complexity: Medium
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Audits are most likely to take place during the COBIT Monitor, Evaluate, and Assess domain phase.
Taxonomy: Remember

10. A policy definitions document is most similar to a:
A) guideline.
B) policy framework.
C) dictionary.
D) baseline.
Ans: C
Complexity: Medium
Ahead: What Are Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A policy definitions document is most similar to a dictionary.
Taxonomy: Understand

11. Which of the following is *not* one of the five pillars of the information assurance (IA) model?
A) Confidentiality
B) Integrity
C) Availability
D) Assurance
Ans: D
Complexity: Medium
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Assurance is not one of the five pillars of the IA model.
Taxonomy: Remember

12. Carl is a security professional. He is reviewing his organization's security policies and related documents. One document contains general rules, a description of the organizations' core values, as well as a description of areas in which there is zero tolerance for transgressions. What type of document is Carl reviewing?
A) Policy principles
B) Policy definitions
C) Standard
D) Guideline
Ans: A
Complexity: Easy
Ahead: What Are Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Feedback: A policy principles document communicates general rules that cut across the entire organization. Principles are written in plain English and focus on key risks or behaviors. When reading security principles, think of them as senior executives expressing their goals and objectives. They express core values of the organization that often include the areas where there will be zero tolerance for transgression.
Taxonomy Apply

13. Which of the following situations best illustrates the process of authentication?
A) A website that requires use of a strong password
B) Using an electronic signature on official documentation
C) When an application sets a limit on the amount of payment a user can approve
D) When a service is made unavailable to a user due to a server crash
Ans: A
Complexity: Difficult
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Authentication is the ability to verify the identity of a user or device. There is a lot involved in maintaining good authentication processes, such as forcing users to change their passwords periodically and forcing rules on how complicated passwords should be.
Taxonomy: Analyze

14. _____ functions as a preventive control designed to prevent mistakes from happening. _____ functions as a detective control intended to improve the quality over time by affording opportunities to learn from past mistakes.
A) Quality control; Quality assurance
B) Governance; Nonrepudiation
C) Quality assurance; Quality control
D) Quality control; Governance
Ans: C
Complexity: Medium
Ahead: What Is Governance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Quality assurance (QA) functions act as a preventive control. When QA works well, it prevents mistakes from happening. Quality control (QC) functions act as a detective control. When QC works well, it improves the quality over time by affording opportunities to learn from past mistakes.
Taxonomy: Analyze

15. Maria is a security professional. She has been looking for ways to streamline some processes in the IT environment. She recently determined the most efficient way to spin up a new server. She is documenting the steps that should be taken by anyone spinning up a server in the future. What kind of document is Maria creating?
A) Procedure
B) Policy
C) Guideline
D) Standard
Ans: A
Complexity: Difficult
Ahead: What Are Information Systems Security Policies?

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A procedure is a written statement describing the steps required to implement a process. Procedures describe how to accomplish specific tasks. Procedures are not written just for humans to follow. Well-written procedures are often used to document requirements for automated processes.
Taxonomy: Apply

16. Which of the following statements most clearly contrasts the difference between policies and procedures?
A) Policies are requirements placed on processes, whereas procedures are the technical steps taken to achieve those policy goals.
B) Policies implement controls on a system to make it compliant to a standard, whereas procedures influence the creation of policies.
C) Policies set the parameters within which a procedure can be used, whereas procedures influence the creation of policies.
D) Policies are often approved by lower-level management responsible for the implementation of policies, whereas procedures are often approved by the most senior levels of management.
Ans: A
Complexity: Difficult
Ahead: What Are Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Policies are requirements placed on processes. Procedures are the technical steps taken to achieve those policy goals. A policy is often approved by the most senior levels of management. A procedure or guideline is often approved by lower-level management responsible for the implementation of policies
Taxonomy: Analyze

17. Which of the following is *not* one of the foundational reasons for using and enforcing security policies?
A) To enable continuous improvement of systems
B) To protect systems from the insider threat
C) To protect information at rest and in transit
D) To control changes to the IT infrastructure
Ans: A
Complexity: Difficult
Ahead: Why Information Systems Security Policies Are Important
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: The last of the four foundational reason for using and enforcing security policies is "defending the business."
Taxonomy: Understand

18. The following are all true of governance, *except*:
A) good governance provides assurance and confidence that rules are being followed.
B) regulators look at the governance structure for assurance that risks to shareholders, customers, and the public are being properly managed.
C) effective governance embraces quality assurance and quality control as part of the culture.
D) generally, the more confidence regulators have that a company has strong governance, the more regulatory oversight is used.
Ans: D

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Complexity: Medium
Ahead: Why Is Governance Important?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Generally, the more confidence regulators have that a company has strong governance, the less regulatory oversight is used.
Taxonomy: Analyze

19. During which phase of business process reengineering (BPR) are new policies written or current ones are updated?
A) Phase 1: Plan
B) Phase 2: Create/refine process baseline
C) Phase 3: Research and benchmarking
D) Phase 4: Develop the future process
Ans: D
Complexity: Easy
Ahead: When Do You Need Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Policies are written or current ones updated during the "develop the future process" phase of BPR.
Taxonomy Understand

20. There are many barriers to policy acceptance and enforcement. Which of the following is *not* one the challenges to policy acceptance?
A) Organizational support at all levels
B) Giving employees a stake
C) Policy awareness and understanding
D) Failure to report infractions
Ans: D
Complexity: Medium
Ahead: Why Enforcing and Winning Acceptance for Policies Is Challenging
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: It is more challenging to reward, recognize, and show employees good examples to model their behavior than it is to discipline them.
Taxonomy: Understand

True/False

1. True or False? A failure in one COBIT phase (or domain) can lead to a weakness or vulnerability downstream.
Ans: True
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

2. True or False? A vulnerability is a human-caused or natural event that could impact a system.
Ans: False
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A threat is a human-caused or natural event that could impact a system, whereas a vulnerability is a weakness in a system that can be exploited.

3. True or False? A risk is the likelihood or probability of an event and its impact.
Ans: True
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

4. True or False? The concept of independent audits (or assessments) is that the further one is away from the actual transaction, the more unbiased and independent the opinion that can be obtained.
Ans: True
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

5. True or False? Integrity ensures that only authorized individuals are able to access information.
Ans: False
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Confidentiality is the goal of ensuring that only authorized individuals are able to access information, whereas integrity ensures that information has not been improperly changed.

6. True or False? The legal concept of nonrepudiation provides assurance that an individual cannot deny having digitally signed a document or been party to a transaction.
Ans: True
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management

7. True or False? A more detailed written procedure produces a more error-free result.
Ans: True
Complexity: Easy

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

8. True or False? A policy is a process or a method for implementing a solution.
Ans: False
Complexity: Easy
Ahead: What Are Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A standard is a process or a method for implementing a solution, and often becomes the measuring stick by which an organization is evaluated for compliance.

9. True or False? One of the foundational reasons for using and enforcing security policies is to protect systems from insider threats.
Ans: True
Complexity: Easy
Ahead: Why Information Systems Security Policies Are Important
Subject: Chapter 1
Title: Information Systems Security Policy Management

10. True or False? Business process reengineering (BPR) should include information systems security concerns and updated those policies and procedures as needed.
Ans: True
Complexity: Easy
Ahead: When Do You Need Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management

11. True or False? Control Objectives for Information and related Technology (COBIT) is a widely accepted international best practices framework.
Ans: True
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

12. True or False? The COBIT Monitor, Evaluate, and Assess domain phase looks at specific business requirements and strategic direction and determines if the system still meets these objectives.
Ans: True
Complexity: Easy
Ahead: What Is Information Systems Security?
Subject: Chapter 1
Title: Information Systems Security Policy Management

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

13. True or False? ISO 38500 provides guidance for managing IT governance.
Ans: True
Complexity: Easy
Ahead: ISO/IEC 38500
Subject: Chapter 1
Title: Information Systems Security Policy Management

14. True or False? The process of authentication, in which an identity is verified, explicitly applies to human users.
Ans: False
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Computers often exchange information or process transactions on humans' behalf and thus need to be authenticated.

15. True or False? The term "entitlement" is related to restricting the type of access a user has.
Ans: True
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management

16. True or False? Availability ensures information is available to authorized users and devices.
Ans: True
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management

17. True or False? Encryption ensures integrity as well as availability.
Ans: False
Complexity: Easy
Ahead: What Is Information Assurance?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Encryption ensures integrity as well as confidentiality.

18. True or False? Data exists generally in one of two states: data at rest, such as on a backup tape, or data in transit, such as when traveling across a network.
Ans: True
Complexity: Easy
Ahead: Why Information Systems Security Policies Are Important
Subject: Chapter 1

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson

Title: Information Systems Security Policy Management

19. True or False? An organization can set up a sound policy framework that can prevent any issues from occurring in information systems security (ISS).
Ans: False
Complexity: Easy
Ahead: When Do You Need Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: Even with a sound policy framework, issues will occur. Depending on the criticality of the issue, policy implementation or change can occur at any time in the process.

20. True or False? Regarding policy framework documents, a policy is optional.
Ans: False
Complexity: Easy
Ahead: What Are Information Systems Security Policies?
Subject: Chapter 1
Title: Information Systems Security Policy Management
Feedback: A guideline is optional.

Access Complete Test Bank for Security Policies and Implementation Issues 3rd Johnson