Access Control and Identity Management 4th edition Gregory Test Bank

SKU: 9781284315080-TEST-BANK

Access Control and Identity Management, Fourth Edition
Peter H. Gregory
Test Bank

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: A-head
Information Field: Subject
Information Field: Title
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284324259

Chapter: Chapter 01 - Quiz

Multiple Choice

1. Which of the following best describes access?
A) The ability to overcome restrictions or barriers to information
B) The ability of a subject and an object to interact
C) The ability of a computer and a database to interact
D) The formulation of rules allowing or denying access
Ans: B
Complexity: Easy
Ahead: Access and Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Fundamentally, access refers to the ability of a subject and an object to interact. Access can be defined in terms of social rules, physical barriers, or informational restrictions.
Taxonomy: Understand

2. Access control defines allowable interactions based upon which of the following?
A) Granting rights to a subject with respect to the object
B) Granting rights to an object with respect to the subject
C) Denying privileges to a subject with respect to an element
D) Denying privileges to an element with respect to the subject
Ans: A
Complexity: Easy
Ahead: Access and Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Access control is the formalization of those rules for allowing or denying access. Access controls define the allowable interactions between subjects and objects. It is based on the granting of rights, or privileges, to a subject with respect to an object.
Taxonomy: Understand

3. Of the three principal components of any access control scenario, which of the following is defined as resources, such as databases, files, and printers, to which a subject requires access?
A) Policies

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

B) Subjects
C) Objects
D) Tools
Ans: C
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Objects are defined as resources to which the subject desires access, such as files, databases, printers, and physical facilities.
Taxonomy: Remember

4. Which access control subject has *not* presented authenticated credentials?
A) Authorized
B) Unauthorized
C) Accounted
D) Unknown
Ans: D
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Unknown access control subjects are those who have not presented authenticated credentials; therefore, their identities are unknown.
Taxonomy: Remember

5. The access control process by which a decision is made to allow or deny access to an object is called:
A) authentication.
B) authorization.
C) identification.
D) information exchange.
Ans: B
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Authorization is the decision to allow or deny access to an object.
Taxonomy: Remember

6. Which of the following best describes the concept of trust in the identification access control process?
A) The access control process can trust that the labels "Beth" and "Elizabeth" correctly identify the same subject.
B) Subjects and objects can mutually trust each other when more than one label is applied to each subject or object.
C) The subject must trust that the system stores credentials securely, but the system must always test to determine if the subject has falsified its credentials.
D) The subject must trust that the system stores credentials securely, and the system must trust that the subject has not falsified its credentials.
Ans: D
Complexity: Difficult

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Control and Identity Management 4th edition Gregory Test Bank

Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Trust is a two-way street. The system must trust that a subject has not falsified their credentials, but at the same time, the subject must be confident that the system will securely store those credentials. If a system stores usernames and passwords insecurely, they can be stolen and used to impersonate legitimate users. This insecure storage destroys the integrity of the entire access control system.
Taxonomy: Analyze

7. Authorization is a set of rights defined for a subject and an object. The rights are based on the subject's:
A) identity.
B) purpose.
C) relationship to the object.
D) label in the system.
Ans: A
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Authorization is a set of rights defined for a subject and an object. The rights are based on the subject's identity. For example, a manager in the human resources department might be authorized to view personnel records but not authorized to edit the year-end financial report.
Taxonomy: Understand

8. Logical access controls for subjects can be based on one or more criteria. Which criteria type is defined by the context of the access request?
A) How
B) What
C) Who
D) Why
Ans: A
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework
Feedback: The How criterion is the context of the access request, meaning, by what method a subject intends to access an object.
Taxonomy: Remember

9. When designing a set of access controls, what question must you consider every time?
A) How does the user need to access this resource?
B) When does the user need access to this resource?
C) Where does the user need access to this resource?
D) Why does the user need to access this resource?
Ans: D
Complexity: Difficult
Ahead: Logical Access Controls
Subject: Chapter 1

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Title: Access Control Framework
Feedback: You should determine why a user needs access to a specific resource every time you design a set of access controls. Every user should have a well-defined purpose related to their job function to gain access to resources.
Taxonomy: Analyze

10. Logical access controls for objects can be defined at many levels. Which of the following is defined as the lowest level of granularity for information-based assets?
A) Application
B) Database
C) Data element
D) System
Ans: C
Complexity: Medium
Ahead: Logical Access Controls for Objects
Subject: Chapter 1
Title: Access Control Framework
Feedback: The data element is the lowest level of granularity for information-based assets. For example, if a database table contains a Social Security number, you may need to place special restrictions on that data element.
Taxonomy: Remember

11. Which of the following is an authentication factor that is represented by a retinal scan?
A) Something you are
B) Something you have
C) Something you know
D) Something you wear
Ans: A
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework
Feedback: The unique physical characteristics of a person, such as those detectable by a retinal or iris scan, a fingerprint scan, or voice analysis, are examples of “something you are.”
Taxonomy: Understand

12. The biometric method of access control that depends on what a person does is called:
A) behavioral characteristics.
B) facial recognition.
C) fingerprinting.
D) behavioral profiling.
Ans: A
Complexity: Medium
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework
Feedback: Behavioral characteristics may include typing tempo or speed (or keystroke dynamics), writing rhythms, and voice recognition.
Taxonomy: Understand

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

13. Which of the following best defines identity management?
A) The formalization of rules for allowing or denying access
B) The category of objects to be protected by access controls
C) The technical methods used to enforce policies
D) The process of creating, maintaining, and revoking user accounts
Ans: D
Complexity: Medium
Ahead: Access and Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Identity management is the process of creating, maintaining, and revoking user accounts, and of providing mechanisms for user authentication.
Taxonomy: Understand

14. Organizations typically use which two elements to enforce policies?
A) Objects and tools
B) Subjects and procedures
C) Procedures and tools
D) Subjects and objects
Ans: C
Complexity: Medium
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Organizations typically use procedures and tools together to enforce policies. For example, most companies have strict policies to determine who has access to personnel records.
Taxonomy: Analyze

15. Which of the following is true about group-based access controls?
A) An individual can be assigned to only one group.
B) Belonging to a group absolves the individual of any security accountability.
C) Differing groups can have differing permissions, such as one group having read and another having read and write.
D) Individuals in a group are not required to log in with a username and password.
Ans: C
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework
Feedback: You can assign individuals to several groups. For example, every person within an enterprise may be a member of the Employees group, with read access to the company intranet and an account on the timecard system. A manager might also be a member of the Managers group and have write access to their department’s intranet page, as well as read access to each of their group’s timecard reports.
Taxonomy: Understand

16. A user needs to modify a data file stored on a network file server. The user logs into the operating system and requests access to the file server. The system layer on the file server checks the user's

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Control and Identity Management 4th edition Gregory Test Bank

credentials against its rules to determine whether the user has no access, read-only access, read/write access, or administrative access to the requested data file. What is this process called?
A) Logical access control
B) Physical access control
C) Group-based access control
D) Identity management
Ans: A
Complexity: Medium
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework
Feedback: The scenario is an example of logical access control.
Taxonomy: Understand

17. A user needs to modify a data file stored on a network file server. The user logs into the operating system and requests access to the file server. The system layer on the file server checks the user's credentials against its rules to determine whether the user has no access, read-only access, read/write access, or administrative access to the requested data file. What is the file server in this scenario?
A) Subject
B) Object
C) Access control
D) Token
Ans: B
Complexity: Medium
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework
Feedback: The file server is one of several objects.
Taxonomy: Understand

18. Miriam is responsible for implementing network authentication. Which of the following should she *not* choose for performing authentication of a network user?
A) Fingerprint scan
B) Password
C) Smart card
D) Driver's license number
Ans: D
Complexity: Medium
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Fingerprint scans, passwords, and smart cards are valid authentication techniques. Driver's license numbers are not secret.
Taxonomy: Apply

19. Lin works for the U.S. military in a Sensitive Compartmented Information Facility (SCIF). SCIF security prevents outside surveillance, enabling people to view and discuss sensitive information. Lin's job is to design the strongest security possible to protect the facility. Which of the following is the strongest combination of authentication for entering the facility?
A) A retinal scan, swiping an ID badge, and typing in a PIN

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

B) Swiping an ID badge and voice recognition
C) A fingerprint scan and entering a code from a token
D) A hand (palm) scan and entering a code from a token
Ans: A
Complexity: Medium
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Three authentication factors — a retinal scan, swiping an ID badge, and entering a PIN — would be the strongest form.
Taxonomy: Analyze

20. The following are true of biometrics, *except*:
A) Biometrics is the study of physical human characteristics.
B) Physical biometrics read physical characteristics, such as retinal scans and facial recognition.
C) Behavioral characteristics, which may include voice recognition, are more subject to error than physical characteristics.
D) The code provided by an authenticator app is an example of something you know.
Ans: D
Complexity: Difficult
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: The code provided by an authenticator app is an example of something you have.
Taxonomy: Understand

True/False

1. True or False? Regarding access controls, an object is the resource to which the subject desires access.
Ans: True
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework

2. True or False? Regarding access controls, the subject is the user, network, process, or application requesting access to a resource.
Ans: True
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework

3. True or False? Organizations typically use procedures and tools together to enforce policies.
Ans: True

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework

4. True or False? In an access control system, authentication is the process of maintaining records of the actions performed by authorized users.
Ans: False
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework
Feedback: Authentication ensures users are who they claim to be.

5. True or False? Physical security is the process of ensuring that only authorized personnel can access physical resources, including hardware and facilities.
Ans: True
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework

6. True or False? A “backdoor” enables a system administrator to take control of a compromised server.
Ans: True
Complexity: Easy
Ahead: Principal Components of Access Control
Subject: Chapter 1
Title: Access Control Framework

7. True or False? Authentication builds upon identification by requiring that the subject provide proof of identity.
Ans: True
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework

8. True or False? Confidence in any authentication system can be measured by two components: the confidence in the accuracy of the authentication mechanisms and the number of authentication factors.
Ans: True
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

9. True or False? Authorization rules are always complex.
Ans: False
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework
Feedback: Authorization rules can be simple or complex, depending on the value of the protected resources.

10. True or False? Authorization rules are defined depending on business needs and the sensitivity of the resources.
Ans: True
Complexity: Easy
Ahead: Access Control Process
Subject: Chapter 1
Title: Access Control Framework

11. True or False? Logical access controls can be based on one or more criteria, including who, what, where, when, and how.
Ans: True
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework

12. True or False? Access controls are often more efficiently managed through role-based groups.
Ans: True
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework

13. True or False? Group access rights for a system or application simplify permissions management.
Ans: True
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework

14. True or False? In an access control system, an object is active, which acts upon a passive subject.
Ans: True
Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Control and Identity Management 4th edition Gregory Test Bank

Feedback: A subject is active, which acts upon a passive object.

15. True or False? The primary authentication factors are something you know, something you have, and something you are.
Ans: True
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework

16. True or False? Regarding authentication factors, a U.S. government Common Access Card (CAC) is an example of something you know.
Ans: False
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework
Feedback: A CAC is an example of something you have.

17. True or False? Regarding authentication factors, a password is an example of something you know.
Ans: True
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework

18. True or False? Regarding authentication factors, voice analysis is an example of something you are.
Ans: True
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework

19. True or False? Biometrics are used to provide authentication factors for “something you know.”
Ans: False
Complexity: Easy
Ahead: Authentication Factors
Subject: Chapter 1
Title: Access Control Framework
Feedback: Biometrics are used to provide authentication factors for “something you are.”

20. True or False? Granting access to a system by groups rather than by individuals reduces individual accountability for activities.
Ans: False

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Control and Identity Management 4th edition Gregory Test Bank

Complexity: Easy
Ahead: Logical Access Controls
Subject: Chapter 1
Title: Access Control Framework
Feedback: Granting access by groups rather than individuals does not reduce individual accountability for activities. An individual still needs to log in with a unique username and password, and the log files are cataloged by username, not by group.

Copyright © 2027 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Control and Identity Management 4th edition Gregory Test Bank