Study Guide

Access Controls for Certified in CybersecuritySM

# Checklist of Exam Objectives: Areas to Study

3.1 Understand physical access controls

* Physical security controls (e.g., badge systems, gate entry, environmental design)
* Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
* Authorized versus unauthorized personnel

3.2 Understand logical access controls

* Principle of least privilege
* Segregation of duties
* Discretionary Access Control (DAC)
* Mandatory Access Control (MAC)
* Role

# **Exam Essentials: What you need to know**

Remember that access control is about letting the ‘right’ entities (people, processes) to be able to perform the ‘right’ tasks; not just about keeping people out.

Access controls pertain to both logical (technical) and physical controls.

Know the Identity Management lifecycle – especially termination of access

Be familiar with the IAAA – the function of each step.

Single Sign On has benefits and disadvantages – know how to implement and manage the risk of single sign on.

Most access control implementations are based on discretionary access control. This is where the asset owner makes the decision on who gets access and what level of access they get. Mandatory Access Control requires compliance with policy as well as the owner’s consent. In MAC the owner’s decision enforces need-to-know.

Be familiar with the implementations of Federated Identity Management.

RBAC (Role Based Access Control) is based on personnel with similar or identical access requirements, in this way it may violate the principle of least privilege.

# Important Terminology

Identity Management Lifecycle: The need to actively manage identities throughout the identity lifecycle – from provision to maintenance to de-provisioning

Authentication – to verify or validate the identity

Authorization – the rights or privileges granted to an authorized user

Accounting or Auditing (as part of identity and access management) – the tracking and recording of all activity on a system. Establishes a link between activities and the unique identifier of the entity that executed the activity.

Multifactor Authentication (MFA) – the use of more than one factor to authenticate an identity. The factors are based on: what you know; what you have; and what you are. Standards often require the use of two different factors in order to be considered MFA.

RBAC – Role based access control – access permissions based on a defined job role. A job role may include entities (persons or processes) with identical or similar access requirements.

Rule based access control – access permissions based on explicit rules that may permit or deny access.

Mandatory Access Control (MAC) – access that is mandated by policy and provides a more stringent level of access than discretionary access control. Enforces separation of duties and requires labeling of assets and users. Requires consent of asset owner and compliance with policy before access is granted.

Discretionary Access Control (DAC) - The majority of systems in the world are based on DAC. In DAC the owner of the asset determines what level of access is granted, and to whom the access is granted. The system just enforces the access decision made by the owner.

Privileged Access Accounts – a higher risk to the organization since the higher levels of access can be misused. Requires compensating controls – more supervision; monitoring of actions, removal of access when no longer required, etc.

Federated Identity Management – ‘single sign on for the web’ use of an identity provider to review the login of a subject (client, relaying party) and provide proof of authentication (security assertion) to a relying party (merchant)

# **Sample Questions**

1. The organization has a policy to change the administrator password on all servers whenever an IT administrator leaves the organization even though all employees have unique UserIDs and the organization uses Multi-factor Authentication. Is this a reasonable policy?
   1. No. It is a lot of work with little associated risk
   2. Yes, because the former employee may know another user’s password.
   3. No, because knowledge of the password will not permit access due to MFA
   4. Yes, because the policy requires it.
2. A recent audit found many UserIDs on the system that were not being used. The auditor stated that this was an unacceptable risk. Why is this a risk?
   1. Because UserIDs may be used by someone else if they are not in regular use
   2. Because this is a violation of least privilege
   3. Because there is no way to track misuse of such UserIDs
   4. Because each UserID has a licensing cost that is wasted
3. How can an organization avoid the risk of having unused UserIDs?
   1. Encourage the use of shared IDs
   2. Force all passwords to change every 30 days
   3. Have each supervisory manager perform scheduled reviews
   4. Terminate all user accounts annually and require re-enrollment
4. User access is restricted according to groupings of their job responsibilities. Which access model is this based on?
   1. Role based access control
   2. Rule based access control
   3. Mandatory Access Control
   4. Attribute based Access Control
5. Which control can be used to prevent the highjacking of an existing remote logon session?
   1. Periodic authentication
   2. Multi-factor Authentication
   3. Strong password policies
   4. Continuous authentication
6. PKI can be used to manage access based on which principle?
   1. MFA
   2. RBAC
   3. Credential Management
   4. Symmetric encryption
7. What term is used to indicate the correct level of access to be enforced associated with a building?
   1. Clearance
   2. Object
   3. Classification
   4. Mandatory
8. An offensive email was sent but the user claims that they did not send it. Which security principle is in question here?
   1. Non-repudiation
   2. Authentication
   3. Integrity
   4. Confidentiality
9. What is commonly used to create a dynamic password?
   1. Fingerprint
   2. Iris scan
   3. Smartcard
   4. Passport
10. What can be used to substitute sensitive data with a non-sensitive value in an e-commerce credit card transaction?
    1. Masking
    2. Tokenization
    3. Obfuscation
    4. Transposition
11. A user account was used to send an email when the user left their workstation unattended and logged in. What control should be used to address this risk?
    1. Session timeout
    2. Policy
    3. MFA
    4. Non-repudiation
12. Which type of access control uses geographic location to determine access permissions?
    1. Attribute
    2. Mandatory
    3. Discretionary
    4. Role Based
13. Which control is used to prevent errors or fraud?
    1. Logging
    2. Least privilege
    3. Separation of duties
    4. Collusion
14. A merchant does not want to manage user accounts for their internet-based customers and decides to use a solution based on OpenID. What is this an example of?
    1. Single Sign On
    2. Kerberos
    3. Active Directory
    4. XML
15. Which form of access control permits delegation of authority?
    1. DAC
    2. MAC
    3. RBAC
    4. Rule-based

Answers:

1. This is a difficult question – intended to make you think and do analysis. The best answer is probably C. But it is good to review and think about this – what are the considerations that you would see factoring into your answer. A is incorrect since these are admin accounts and do represent a higher level of risk than other accounts. B is incorrect though it may be true. Use of MFA reduces the risk of a compromised password. D is incorrect – if a policy is wrong then steps should be taken to change the policy
2. Another think-about-it question. What is the risk? How does a security-minded person respond to such an audit in an appropriate manner? What action should be taken, if any? B is correct but also possibly wrong – least privilege states that only the minimal level of access should be provided and only for the time required. But these could be authorized users that may only need access occasionally. Requiring them to apply for access each time they need it would be unreasonable. C is incorrect – you should still be able to log the activity associated with a UserID. D is partially correct since it can be a waste of money to pay for unused IDs. A is probably the best answer (or B) because it is a risk is a UserID starts to be used by someone else and the real owner is not aware of it since they are not using it.
3. C is the best answer. Each manager should have to review the access permissions for their direct reports and correct any access permission errors. A is wrong – we should not encourage shared IDs that removes accountability. B is incorrect, a password change will disable unused IDs but not remove them. D is incorrect since terminating accounts would be an extraordinary expense and may interrupt business operations.
4. A – this is an example of RBAC – role based access control groups users with identical or similar job functions. B is not the best answer since rules are not necessarily related to job role. C refers to access control theorems and role based access control may be based on either MAC or DAC. D is incorrect since ABAC is a granular form of access control entitlement based on specific conditions (attributes).
5. A is correct but not the best answer – periodic authentication will prevent extended use of a highjacked session but will not prevent it like D – continuous authentication will. B and C are more relevant to establishing a secure session.
6. C is the best answer. PKI supports credential management. MFA uses two factors and PKI may only be one of those. RBAC may use certificates but is not the best answer. PKI is based on asymmetric encryption not symmetric.
7. C - A building is an object and therefore has a classification that indicates its level of security. A user or subject has clearance. Mandatory is an access control theorem.
8. A – the user is repudiating sending the email so this is a breach of the principle of non-repudiation. Authentication is also in question – was someone else able to log into the user’s account or did the user leave their workstation unattended but logged in? Did the user share their password? This is what the investigator must determine. Integrity and Confidentiality are not the concepts being breached here.
9. C is the best answer – smartcard is commonly used to create a one time (dynamic) password. The other answers refer to biometrics and ownership with a static value.
10. B – Tokenization is used to substitute a credit card number with a token value. The other answers may hide a credit card number from view but not substitute it.
11. B – this is a violation of policy and that needs to be the primary control to ensure that a user does not leave a workstation logged in and unattended and to ensure that staff knows that to send an email from another person’s account is a strict violation of policy. A is a compensating control that may help after a few minutes if the workstation is left logged in but it will only help after a few minutes. MFA would not apply to a session already logged in. D is
12. A is the most correct answer. Location is an attribute. This access may be based on the concepts of MAC, DAC and perhaps even on RBAC. But this is an example of ABAC
13. C – separation or segregation of duties is designed to catch fraud or prevent errors – collusion is where people work together to bypass separation of duties. Logging may detect fraud but not prevent it. Least privilege is a good answer since limiting access may prevent unauthorized activity – but it is not the best answer
14. A – this is an example of Federated Identity Management (FIM) – which is a type of single sign on for the internet. Kerberos is an example of Single Sign On but usually for within an organization not for internet customers. Active Directory is a commonly used access control method but not specific to this question. XML defines the structure of communications – often between organizations but not applicable here with the question presented
15. A - DAC allows the delegation of authority. MAC does not permit delegation, RBAC and rule-based may be based on either DAC or MAC.